



Junos[®] Space

Connectivity Services Director User Guide

Release
2.2R1



Modified: 2019-04-05

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Junos® Space Connectivity Services Director User Guide

2.2R1

Copyright © 2019 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	lv
	Documentation and Release Notes	lv
	Documentation Conventions	lv
	Documentation Feedback	lvii
	Requesting Technical Support	lviii
	Self-Help Online Tools and Resources	lviii
	Creating a Service Request with JTAC	lix
Part 1	Overview	
Chapter 1	Working with Connectivity Services Director	3
	Connectivity Services Overview	3
	Understanding the Need for Connectivity Services Director for Managing Services	4
	Benefits of a Unified User Interface for Routing and Tunnel Services with Connectivity Services Director	6
	Connectivity Services Director Overview	8
	Understanding the Connectivity Services Director User Interface	10
	Connectivity Services Director Banner	10
	View Pane	12
	Displaying Devices Using Various Network Views	12
	Filtering the Network Tree	13
	Expanding or Collapsing Nodes in the Network Tree	14
	Searching the Network Tree	15
	Tasks Pane	15
	Alarms	16
	Main Window or Workspace	16
	Tables in Connectivity Services Director	16
	Moving and Resizing Columns	16
	Navigating Pages	16
	Displaying the Column Drop-Down Menu	17
	Sorting on a Column	17
	Hiding and Exposing Columns	18
	Searching Table Contents	18
	Filtering Table Contents	20
	Understanding the Usage and Layout of Connectivity Services Director Views and Tasks	21
	Understanding the Management Lifecycle Modes in Connectivity Services Director	22

	Understanding Connectivity Services Director User Administration	24
	Logging In to Connectivity Services Director	25
	Accessing the Services Activation Director GUI	27
	Changing Your Password for Connectivity Services Director	28
	Logging Out of Connectivity Services Director	30
	Getting Started Assistant Overview in Services Activation Director	31
Chapter 2	Service View Tasks and Lifecycle Modes	33
	Understanding the Service View Tasks Pane in Build Mode	33
	Understanding the Service View Tasks Pane in Deploy Mode	36
	Understanding the Service View Tasks Pane in Monitor Mode	38
	Understanding the Service View Tasks Pane in Fault Mode	40
	About Build Mode in Service View of Connectivity Services Director	41
	Manage Service Definitions	42
	Prestage Devices	42
	Prestage Services	42
	Manage Threshold Alarm Profiles	43
	Service Definition Operations	43
	Audit and Troubleshooting of Services	43
	About Deploy Mode in Service View of Connectivity Services Director	43
	Manage Network Services	44
	Manage Deployment of Service Orders	44
	About Fault Mode in All Views of Connectivity Services Director	45
	About Monitor Mode in Service View of Connectivity Services Director	45
	Quick Access to Important Troubleshooting Details	46
	Performance Monitoring	46
	View and Clear Interface Information	46
	View Interface Status	47
	View Routing Table	47
	View MAC Table	47
	Traceroute for an MPLS LSP	47
	MPLS Ping	47
Chapter 3	Network Services Overview	49
	Getting Started with Connectivity Services Director	50
	Prestaging Devices Overview	53
	Junos Space Layer 2 Services Overview	55
	Point-to-Point Services	56
	Port-to-Port Service	56
	Single VLAN Service Using 802.1Q Interfaces	57
	All Traffic Service Using Q-in-Q Interface	58
	Range of VLANs Service with Q-in-Q Interfaces	58
	VPLS Services	59
	Service Autodiscovery	61
	VPLS and Normalization	62
	Junos Space Layer 3 Services Overview	64
	Overview	64
	Layer 3 VPN Platform Support	64
	Layer 3 VPN Attributes	64
	Device Configuration for a Layer 3 VPN	65

Provisioning Process Overview	65
Network Operator Tasks—Provisioning Prerequisites	66
Service Designer Tasks	67
Service Provisioner Tasks	67
Seamless MPLS Support in Junos Space Overview	69
Service Attributes Overview	71
General Attributes	71
Service Type	72
Signaling	72
Comments	72
Service Template	72
Threshold Alarm Profile	72
Interface Type	72
Enabling Additional Features	72
Customer	73
Enable QoS	73
UNI Settings	73
Ethernet Options	74
Interface	74
MTU	74
Customer Traffic Type	74
Customer VLAN ID	75
Service VLAN ID and VLAN ID Range	75
Physical Encapsulation	75
Logical Encapsulation	76
Rate Limiting and Bandwidth	77
UNI Settings for TDM Interfaces	77
UNI Settings for ATM Interfaces	77
Connectivity Settings	77
Virtual Private LAN Service Identifier (VPLS ID)	78
Auto Discovery	78
Virtual Circuit Identifier (VCID) (Point-to-Point Services Only)	78
Route Targets and Route Distinguishers	78
Normalized VLAN (Multipoint Services Only)	78
MAC Learning	79
Advanced Settings	80
Tunnel Services	80
Local Switching	80
Fast Reroute Priority	80
Label Block Size	81
Connectivity Type	81
Node Settings	81
Static Routes	82
PIM Settings	82
MVPN Settings	84
MAC Settings	85
Topology Settings	85

Service Order States and Service States Overview	86
Service Order States	86
Service States	87
Understanding VLAN Manipulation (Normalization and VLAN Mapping) on	
Ethernet Services	88
VLAN Translation (Normalization) for VPLS Services	89
VLAN Mapping for VPLS Services	89
Sample VLAN Configuration on MX Series and M Series PE Routers	91
VLAN Pool Profiles Overview	93
Redundant Pseudowires for Layer 2 Circuits and VPLS	94
Types of Redundant Pseudowire Configurations	94
Pseudowire Failure Detection	95
VPLS over GRE Overview	95
Junos Space Network Topology Overview	96
Service Recovery Overview	97
Multicast L3VPN Overview	98
Multi-Chassis Automatic Protection Switching Overview	99
Inverse Multiplexing for ATM Overview	100
Rendezvous Point	101
Understanding Multicast Rendezvous Points, Shared Trees, and	
Rendezvous-Point Trees	101
Understanding PIM Sparse Mode	103
Rendezvous Point	104
RP Mapping Options	105
Configuring Shared-Tree Data Distribution Across Provider Cores for Providers	
of MBGP MVPNs	106
Configuring SPT-Only Mode for Multiprotocol BGP-Based Multicast VPNs	107
Configuring VRF Route Targets for Routing Instances for an MBGP MVPN	109
Static Pseudowire Provisioning for VPLS Services	110

Part 2

Chapter 4

Getting Started With Connectivity Services Director

Understanding Connectivity Services Director System Administration and Preferences	115
Understanding Connectivity Services Director User Administration	115
Understanding the System Tasks Pane	117
Audit Logs Overview	117
Viewing Audit Logs From Connectivity Services Director	117
Managing Jobs	118
Collecting Logs for Troubleshooting	120
Setting Up User and System Preferences	122
Accessing the Preferences page	122
Choosing Server Time or Local Time	123
Specifying Search Preferences	123
Retaining Connectivity Services Director Reports	123
Modifying Services Activation Parameter Settings	123

	Specifying Topology Preferences	128
	Changing Monitor Mode Settings	129
	Disabling Data Collection for Monitors	129
	Changing the Polling Interval	130
	Specifying Database History Retention	131
	Changing Alarm Settings	131
	Configuring Global Alarm Notifications	132
	Retaining Alarm History	132
	Specifying Event History	132
	Enabling Alarms	132
	Changing the Severity of Individual Alarms	152
	Configuring Threshold Alarms	152
	Configuring Individual Alarm Notifications	152
	Disabling Optical Performance Monitoring	153
Part 3	Working with the Dashboard	
Chapter 5	About the Dashboard	157
	Understanding the Dashboard	157
Chapter 6	Using the Dashboard	159
	Using Dashboard Widgets	159
Chapter 7	Dashboard Widget Reference	161
	Device Alarms Widget	161
	Service Alarms by Severity Widget	162
	Config Deployment Jobs Status Widget	162
	Config Deployment Jobs Status Widget Summary	162
	Config Deployment Jobs Status Widget Details	163
	Device & Port Utilization Heatmap Widget	163
	Using the Global Controls	163
	Interacting with the Heat Maps	163
	Viewing Active Flows on a Port	164
	Flow Analysis Details Window	165
	Port Status - Physical Widget	166
	Port Status - Physical Widget Summary	167
	Port Status - Physical Widget Details	167
Part 4	Working in Build Mode	
Chapter 8	About Build Mode	171
	Understanding Build Mode in Views Other than Service View of Connectivity	
	Services Director	171
	Discovering Devices	171
	Building the Custom View	172
	Configuring Devices	172
	Deploying Device Configurations	173
	Importing Device Configurations	173
	Out-of-Band Configuration Changes	173

	Managing Devices	174
	Understanding the Build Mode Tasks Pane in Views Other than Service View . .	174
Chapter 9	Discovering Devices	177
	Discovering Devices in a Physical Network	177
	Preparing MX Series Devices for Discovery	178
	Specifying the Target Devices	178
	Specifying the Discovery Options	180
	Specifying the Schedule Options	182
	Reviewing the Device Discovery Options	182
	Viewing the Discovery Status	182
	Troubleshooting Device Discovery Error Messages	184
	Viewing the Brownfield Job	185
Chapter 10	Creating Custom Device Groups	187
	Understanding Custom Device Groups	187
	Where Is the Custom Group Function Located in Connectivity Services Director?	187
	How Do Custom Group Rules Work?	188
	What Happens When I Edit a Custom Group Rule?	188
	When Are Rules Executed?	188
	Creating Custom Device Groups	188
	Creating Custom Groups	189
	Creating a Custom Group	189
Chapter 11	Configuring Quick Templates	193
	Understanding Quick Templates	193
	Configuring and Managing Quick Templates	194
	Creating a Quick Template	196
	Applying Templates to Devices	197
	Editing a Quick Template	198
	Deleting a Quick Template	198
	Cloning a Quick Template	198
	Using the Quick Template Details Window	198
	Viewing Deployed Quick Templates	199
Chapter 12	Configuring Device Settings	201
	Understanding Device Common Settings Profiles	201
	Creating and Managing Device Common Settings	201
	Managing Device Common Settings	202
	Creating a Device Common Settings Profile	203
	Specifying Basic Settings for Device Common Settings	205
	Specifying Management Settings for Routing Device Common Settings . .	208
	Specifying Protocol Settings for Routing Device Common Settings	211
	Reviewing and Saving a Device Common Settings Configuration	213
	What to Do Next	214
	Assigning Device Common Settings to Devices	214
	Assigning Device Common Settings	214
	Editing the Assignments of the Device Common Setting	216

Chapter 13	Configuring Class of Service (CoS)	219
	Understanding Class of Service (CoS) Profiles	219
	How Would I Use CoS (also known as QoS)?	219
	How Do I Create CoS Groups?	220
	How Is CoS Different From QoS?	220
	How Does CoS Work?	220
	What Wireless Network Traffic Aspects Can I Control Using CoS?	221
	What CoS Parameters Can I Control?	222
	What Are the Default CoS Traffic Types?	222
	Data Center Switching CoS Configuration	223
	How Do I Implement Class of Service?	223
	Editing Discovered CoS Profiles	223
	Creating and Managing Wired CoS Profiles	224
	Managing Wired CoS Profiles	225
	Using the Default CoS Profiles for Routers	226
	Using the Default CoS Profiles for Campus Switching ELS with Hierarchical Port Scheduling	226
	Using the Default CoS Profiles for Data Center Switching	226
	Creating a Wired CoS Profile	227
	Specifying Settings for a Routing, Switching, and Campus Switching ELS CoS Profile	228
	Specifying Settings for a Campus Switching ELS CoS Profile with Hierarchical Port Scheduling (ETS)	232
	Specifying Settings for a Data Center Switching CoS Profile	236
	What to Do Next	243
Chapter 14	Configuring Link Aggregation Groups (LAGs)	245
	Understanding Link Aggregation	245
	Managing and Creating a Link Aggregation Group	245
	Link Aggregation Group Options	246
	Creating a Link Aggregation Group	247
	What To Do Next	249
Chapter 15	Managing Network Devices	251
	Viewing the Device Inventory Page in Device View of Connectivity Services Director	252
	Viewing the Physical Inventory of Devices	253
	Viewing Licenses With Connectivity Services Director	254
	Viewing a Device's Current Configuration from Connectivity Services Director	255
	Accessing a Device's CLI from Connectivity Services Director	256
	Accessing a Device's Web-Based Interface from Connectivity Services Director	257
	Deleting Devices	258
	Rebooting Devices	258

Part 5	Building a Topology View of the Network	
Chapter 16	Downloading and Installing CSD-Topology	261
	CSD-Topology Installation and Configuration Overview	261
	Installation Prerequisites	262
	Installing the CSD-Topology Software Using the RPM Bundle	262
	Minimum Hardware and Software Requirements for Junos VM on VMWare	263
	Installing the JunosVM for CSD-Topology	264
	Setting Up the Datastore	265
	Creating VRR VMs	267
	Configuring the JunosVM	275
	Configuring the CSD-Topology Server with the JunosVM IP Address	276
	Verifying the Connectivity Between the CSD-Topology Server and JunosVM	277
	Verifying That the CSD-Topology Services Are Running	277
	Stopping Firewall on the CSD-Topology Server	278
	Configuring Peer Routers and Topology Acquisition on the JunosVM	278
	Specifying the Topology Details in the Connectivity Services Director GUI	280
	Connecting an x86 Server to the Network	281
	Interactive Method of Installing the RPM Image and CSD-Topology Software from a USB or DVD Drive	286
Chapter 17	Configuring Topology Acquisition and Connectivity Between the CSD-Topology and Path Computation Clients	289
	Configuring PCEP on a PE Router (from CLI)	289
	Configuring Connectivity for BGP-LS Topology Acquisition	291
	Configuring BGP-LS Topology Acquisition on the CSD-Topology	292
	Configuring Topology Acquisition on the PCC Routers	293
	Configuring Connectivity for OSPF Topology Acquisition	294
	Configuring OSPF on the CSD-Topology	294
	Configuring OSPF Over GRE on the CSD-Topology	295
	Configuring Connectivity for IS-IS Topology Acquisition	296
	Configuring IS-IS on the CSD-Topology	296
	Configuring IS-IS Over GRE on the CSD-Topology	297
Chapter 18	Accessing the Topology View of CSD-Topology	299
	Understanding the Network Topology in Connectivity Services Director	300
	Monitoring the Topology of Network Elements Managed by CSD-Topology	
	Overview	301
	Specifying Topology Preferences	302
	CSD-Topology Topology Map Window Overview	304
	Working with the Graphical Image in the Topology View Window	306
	Expanding and Collapsing Groups by Using the Topology Map Grouping Shortcut Menu	309
	Filtering Links, LSPs, and Services by Using the Topology Map Node Shortcut Menu	310
	Removing the Highlighted LSPs by Using the Topology Map LSPs Shortcut Menu	311
	Viewing the Service Path by Using the Topology Map Service Shortcut Menu	312

Filtering Devices, LSPs, and Services for Sorting and Segregating the Topology View	313
Segregating the Displayed Devices by Searching the Entire Topology View	314
Resynchronizing the Topology View	315
Viewing Device Details of a CSD-Topology for Examining Traffic Transmission	316
Viewing LSP Details of a CSD-Topology for Analyzing Network Changes	318
Viewing Link Details of a CSD-Topology for Determining the Operational Status	321
Viewing Service Details of a CSD-Topology for Monitoring and Troubleshooting Service Parameters	323
Viewing Topology Map Group Details in a Pop-Up Dialog Box	326
Viewing Topology Map Device Details in a Pop-Up Dialog Box	328
Viewing Topology Map Link Details in a Pop-Up Dialog Box	330
Viewing Topology Map LSP Details in a Pop-Up Dialog Box	332
Viewing Topology Map Service Details in a Pop-Up Dialog Box	334
Enabling the Collection of LSP and Service Association Details	336
Using Custom Grouping for Devices in a CSD Topology	336
Viewing Generated Alarms for Services in the Topology View	337
Viewing the Optical Link Details for Examining the Performance of Optical Links	338

Part 6

Chapter 19

Prestaging

Prestaging Devices Overview	343
Prestaging Devices Process Overview	344
Prestaging Workflow in Connectivity Services Director	347
Auto-Discovery and Auto Prestaging of Devices	347
Parallel Prestaging Jobs	348
Auto Prestaging Jobs When a Manual Prestaging Job is Running	348
Manual Prestaging Jobs When an Auto Prestaging Job is Running	348
Multiple Auto Prestaging Jobs for a Device	349
Multiple Auto Prestaging Jobs for a Device	349
Scenarios With a Clustered Environment	349
Types of Prestaging	349
Prerequisites for Prestaging Devices in Connectivity Services Director	350
Discovering and Assigning All N-PE Devices	351
Discovering Device Roles	352
Assigning Device Roles	352
Discovering and Assigning N-PE Devices with Exceptions	353
Including Interfaces in UNI Role Assignments	354
Committing Your Prestaging Choices	354
Prestaging ATM and TDM Pseudowire Devices	356
Discovering and Assigning Provider Role or LSP Role for Devices with Exceptions	359
Including Interfaces in UNI Role Assignments	360
Committing Your Prestaging Choices	361

	Discovering and Assigning All Provider or LSP Devices	362
	Discovering LSP Device Roles	362
	Assigning Provider Device Roles	363
	Prestaging Rules	364
	N-PE Device Classification Rules	364
	UNI Classification Rules	365
	VLAN Pool Profile Classification Rules	366
	Auto Discovery Only	366
Chapter 20	Prestaging: Managing Devices and Device Roles	369
	Discovering Tunnel Devices	369
	Adding a UNI	371
	Unassigning Device Roles	372
	Deleting UNIs	373
	Discovering Device Roles	374
	Excluding Devices from N-PE Role Assignment	375
	Excluding Interfaces from UNI Role Assignments	376
	Unassigning N-PE Devices	378
	Viewing N-PE Devices	378
	Viewing N-PE Devices in a Table	379
	Viewing Prestaging Statistics	381
	Viewing the Prestaged Device Details	381
	Viewing Services for Devices and Device Roles in a Graphical Form	382
	Viewing Prestaging Rules	383
	Viewing Prestaging Rules in a Table	384
	Managing Prestage Device Jobs	385
	Specifying the Wait and Idle Times for Prestaging Devices	387
Chapter 21	Prestaging: Managing IP Addresses	389
	Creating an IP Address Pool	389
	Managing Resources	391
	Specifying IPv4 Addressing Assignment in Layer 3 VPN Service Definitions	394
Chapter 22	Device Configuration Prerequisites to Prestaging Examples	397
	Example: Base Configuration for N-PE Device in a Multipoint Service	397
	Example: Base Configuration for N-PE Device in a Point-to-Point Ethernet (LDP) Service	399
	Example: Base Configuration for N-PE Device in a Point-to-Point Ethernet (LDP) Service	400
	Example: Base Configuration for a P Router	401
Chapter 23	Prestaging Services	405
	Creating and Handling a Service Recovery Request	406
	Selecting a Service Definition in the Wizard for Creating a Service Recovery Request	409
	Specifying Devices and Filters in the Wizard for Creating a Service Recovery Request	410
	Reviewing the Configured Settings in the Wizard for Creating a Service Recovery Request	413
	Viewing Service Recovery Report	415

Performing a Service Recovery on a Defined Service	416
Processing of Device Change Notifications Overview	417
XPath of Relevance to Connectivity Services Director	418
Processing of XPath Notifications for Out-of-Band Configuration	
Changes	419
Handling of Out-of-Band Notifications for Service Recovery	420
Viewing Service Recovery Instance Details	421
Managing Out-of-Band Notifications for Recovered Services	425
Viewing Details of an Out-of-Band Notification for Recovered Services	427
Viewing Services Rejected During a Service Recovery	429
Viewing Service Recovery Jobs	431
Performing a Configuration Audit for Recovered Services	434
Viewing Configuration Audit Results of Recovered Services	437
Recovering Modifications and Deletions Performed for Existing Endpoints	441
Recovering Parameters for Point-to-Point Services	441
Recovering Parameters for Layer 3 VPN Services	442
Recovering Parameters for VPLS Services	443
Recovering Endpoint Deletions from a Service	444
REST API Changes in Connectivity Services Director for Service Recovery	445
Sample XPath Notifications Received on Devices for Deleted Endpoints	446
Sample XPath Notifications Received on Devices for a Modified VPLS	
Service	449
Sample XPath Notifications Received on Devices for a Created VPLS Service ..	453
Sample XPath Notifications Received on Devices for a Created Layer 3 VPN	
Service	457
Sample XPath Notifications Received on Devices for a Created Point-to-Point	
Service	458
Sample XPath Notifications Received on Devices for CFM Profiles Associated	
with a P2P Service	459
Sample XPath Notifications Received on Devices for CoS Profiles Associated	
with a P2P Service	461

Part 7

Chapter 24

Service Design: Working with Service Definitions

Service Design: Predefined Service Definitions	465
Predefined Service Definitions	465
Ethernet Point-to-Point Predefined Service Definitions	465
ELine-Dot1q-SingleVLAN	468
ELine-Dot1q-SingleVLAN-CCC	470
ELine-Dot1q-SingleVLAN-Ext-CCC	472
ELine-PortBased	474
ELine-QinQ-AllVLAN	476
ELine-QinQ-AllVLAN-CCC	479
ELine-QinQ-AllVLAN-Ext-CCC	481
ELine-QinQ-VLANRange	483
ELine-QinQ-VLANRange-CCC	485

ELine-QinQ-VLANRange-Ext-CCC	487
Multipoint-to-Multipoint Predefined Service Definitions	489
ELAN-BGP-Dot1q-Normalized-VLAN-None	492
ELAN-BGP-Dot1Q-SingleVLAN	496
ELAN-BGP-PortBased	499
ELAN-BGP-QinQ-AllVLAN	502
ELAN-BGP-QinQ-AllVLAN-Normalized-All	506
ELAN-BGP-QinQ-AllVLAN-Normalized-None	509
ELAN-BGP-QinQ-Range-Normalized-VLAN	512
Point-to-Multipoint Service Definitions	515
ELAN-Hub-Spoke-QinQ-AllVLAN	516
ELAN-Hub-Spoke-QinQ-AllVLAN-No	517
Predefined Point-to-Point Service Definitions	517
ELine-Dot1q-SingleVLAN Service Definition	522
Configuration on Endpoint A	522
Configuration on Endpoint Z	523
ELine-Dot1q-SingleVLAN-CCC Service Definition	524
Configuration on Endpoint A	524
Configuration on Endpoint Z	525
ELine-Dot1q-SingleVLAN-Ext-CCC Service Definition	526
Configuration on Endpoint A	526
Configuration on Endpoint Z	527
ELine-PortBased Service Definition	528
Configuration on Endpoint A	528
Configuration on Endpoint Z	529
ELine-QinQ-AllVLAN Service Definition	530
Configuration on Endpoint A	530
Configuration on Endpoint Z	531
ELine-QinQ-AllVLAN-CCC Service Definition	532
Configuration on Endpoint A	533
Configuration on Endpoint Z	534
ELine-QinQ-AllVLAN-Ext-CCC Service Definition	535
Configuration on Endpoint A	535
Configuration on Endpoint Z	536
ELine-QinQ-VLANRange Service Definition	537
Configuration on Endpoint A	537
Configuration on Endpoint Z	538
ELine-QinQ-VLANRange-CCC Service Definition	539
Configuration on Endpoint A	539
Configuration on Endpoint Z	540
ELine-QinQ-VLANRange-Ext-CCC Service Definition	541
Configuration on Endpoint A	541
Configuration on Endpoint Z	542
ELine-BGP-Port-Based	543
Configuration on Endpoint A	543
Configuration on Endpoint Z	544
ELine-BGP-Dot1q-SingleVLAN	546
Configuration on Endpoint A	546
Configuration on Endpoint Z	547

Eline-BGP-QinQ-AllVLAN	548
Configuration on Endpoint A	548
Configuration on Endpoint Z	549
Predefined Multipoint-to-Multipoint Ethernet Service Definitions	551
ELAN-BGP-Dot1q-Normalized-VLAN-None Service Definition	553
Configuration on Endpoint A	554
Configuration on Endpoint B	555
Configuration on Endpoint Z	556
ELAN-BGP-Dot1Q-SingleVLAN Service Definition	557
Configuration on Endpoint A	557
Configuration on Endpoint B	558
Configuration on Endpoint Z	559
ELAN-BGP-PortBased Service Definition	560
Configuration on Endpoint A	560
Configuration on Endpoint B	561
Configuration on Endpoint Z	562
ELAN-BGP-QinQ-AllVLAN Service Definition	563
Configuration on Endpoint A	564
Configuration on Endpoint B	565
Configuration on Endpoint Z	566
ELAN-BGP-QinQ-AllVLAN-Normalized-All Service Definition	567
Configuration on Endpoint A	567
Configuration on Endpoint B	568
Configuration on Endpoint Z	569
ELAN-BGP-QinQ-AllVLAN-Normalized-None Service Definition	570
Configuration on Endpoint A	570
Configuration on Endpoint B	571
Configuration on Endpoint Z	572
ELAN-BGP-QinQ-Range-Normalized-VLAN Service Definition	573
Configuration on Endpoint A	574
Configuration on Endpoint Z	575
Predefined Point-to-Multipoint Ethernet Service Definitions	576
ELAN-Hub-Spoke-QinQ-AllVLAN-Normalized-All Service Definition	577
Configuration on Endpoint A	578
Configuration on Endpoint B	580
Configuration on Endpoint Z	581
ELAN-Hub-Spoke-QinQ-AllVLAN Service Definition	583
Configuration on Endpoint A	584
Configuration on Endpoint B	586
Configuration on Endpoint Z	587
Predefined Full Mesh Layer 3 VPN Service Definitions	589
Predefined Hub-and Spoke Layer 3 VPN Service Definitions	590

Chapter 25	Service Design: Managing Point-to-Point Service Definitions	593
	Choosing a Predefined Service Definition or Creating a New Service Definition	593
	Choosing a Predefined Service Definition	593
	Creating a Point-to-Point Ethernet Service Definition	599
	Specifying General Information	600
	Specifying UNI Settings	603
	Specifying Connectivity Information When Signaling Is LDP	614
	Specifying Connectivity Information When Signaling Is BGP	615
	Reviewing the Configured Settings	617
	Creating a Point-to-Point ATM or TDM Pseudowire Service Definition	618
	Specifying General Information for the ATM or TDM Service	619
	Specifying UNI Settings for ATM and TDM Service Definitions	621
	Specifying UNI Settings for ATM Interfaces	621
	Specifying UNI Settings for TDM Interfaces	621
	Specifying Connectivity Information for an ATM or a TDM Service	622
	Reviewing the Configured Settings	624
	Creating a Point-to-Point Ethernet Service Definition	625
	Specifying General Information	625
	Specifying UNI Settings	628
	Specifying UNI Settings for Port-to-Port Services	628
	Specifying UNI Settings for Services with 802.1Q Interface Types	631
	Specifying UNI Settings for Services with Q-in-Q Interface Types	634
	UNI Settings for Services with Flexible VLAN Tagging (Asymmetric Interface Types)	637
	Specifying Connectivity Information When Signaling Is LDP	640
	Specifying Connectivity Information When Signaling Is BGP	643
	Modifying a Custom Service Definition	646
	Publishing a Custom Service Definition	647
	Unpublishing a Custom Service Definition	648
	Deleting a Customized Service Definition	649
	Viewing Service Definitions	650
	Tabular View	650
	Searching for Service Definitions	651
	Viewing Service Definition Details	651
	Performing Actions on Service Definitions	652
Chapter 26	Service Design: Managing VPLS Service Definitions	653
	Creating a Multipoint-to-Multipoint VPLS Service Definition	653
	Specifying General Information for Multipoint-to-Multipoint VPLS Service Definitions	654
	Specifying Advanced Settings	657
	Specifying Site Settings for Multipoint-to-Multipoint VPLS Service Definitions	660
	UNI or Site Settings for Port-to-Port Interfaces in VPLS Services	660
	UNI or Site Settings for 802.1Q Interfaces in VPLS Services	664
	UNI or Site Settings for Q-in-Q Interfaces in VPLS Services	668
	UNI Settings for Services with Flexible VLAN Tagging (Asymmetric Interface Types)	672

	Reviewing the Configured Settings	677
	Creating a Point-to-Multipoint VPLS Service Definition	678
	Specifying General Information for Point-to-Multipoint VPLS Service	
	Definitions	679
	Specifying Advanced Settings	684
	Specifying UNI or Site Settings for Point-to-Multipoint VPLS Service	
	Definitions	686
	UNI or Site Settings for Port-to-Port Interfaces in VPLS Services	686
	UNI or Site Settings for 802.1Q Interfaces in VPLS Services	689
	UNI or Site Settings for Q-in-Q Interfaces in VPLS Services	694
	UNI or Site Settings for Services with Flexible VLAN Tagging (Asymmetric	
	Interface Types)	699
	Reviewing the Configured Settings	704
	Creating a Service Definition for VPLS Access into Layer 3 Networks	705
Chapter 27	Service Design: Managing Layer 3 VPN Service Definitions	709
	Creating a Full-Mesh Layer 3 VPN Service Definition	709
	Specifying General Settings Information	709
	Specifying Site or UNI Settings	712
	Reviewing the Configured Settings	718
	Creating a Hub-and-Spoke (One Interface) Layer 3 VPN Service Definition	719
	Specifying General Information	721
	Specifying UNI or Site Settings	723
	Reviewing the Configured Settings	729
	Creating a Service Definition for Point-to-Point Pseudowire Access into a Layer	
	3 VPN	730
	Creating a Multicast VPN Service Definition	732
Part 8	Service Provisioning: Working with Customers	
Chapter 28	Service Provisioning: Managing Customers	737
	Adding a New Customer	737
	Deleting Customers	738
	Modifying an Existing Customer	739
	Viewing Customer Details	740
Part 9	Working in Deploy Mode	
Chapter 29	About Deploy Mode	745
	Understanding Deploy Mode in Views Other than Service View of Connectivity	
	Services Director	745
	Deploying Configuration Changes	745
	Managing Software Images	747
	Managing Devices	747
	Managing Device Configuration Files	747
	Managing Baseline Configuration	747
	Understanding the Deploy Mode Tasks Pane in Views Other than Service	
	View	748

Chapter 30	Deploying and Managing Device Configurations	751
	Deploying Configuration to Devices	751
	Selecting Configuration Deployment Options	752
	Using the Change Request Details Page	755
	Creating a Change Request	756
	Validating Configuration	756
	Discarding the Pending Configurations	757
	Viewing Pending Configuration Changes	757
	Using the Pending Changes Window	758
	Using the Configuration or Pending Configuration Window	758
	Using the Deploy Configuration Errors/Warnings Window	758
	Using the Configuration Validation Window	759
	Deploying Configuration Changes to Devices Immediately	759
	Scheduling Configuration Deployment	759
	Specifying Configuration Deployment Scheduling Options	760
	Editing Change Requests	760
	Deleting Change Request	761
	Resubmitting a Change Request	761
	Performing a Rollback	762
	Managing Configuration Deployment Jobs	762
	Selecting Configuration Deployment Job Options	763
	Viewing Configuration Deployment Job Details	764
	Canceling Configuration Deployment Jobs	764
	Deploy Configuration Window	764
	Approving Change Requests	765
	Enabling SNMP Categories and Setting Trap Destinations	767
	Viewing Eligible Devices for Trap Forwarding	767
	Enabling Trap Forwarding	768
	Deploying SNMP Trap Configurations	769
	Understanding Resynchronization of Device Configuration	773
	The Resynchronize Device Configuration Task	774
	How Resynchronization Works in NSOR Mode	774
	How Resynchronization Works in SSOR Mode	776
	How Connectivity Services Director Resynchronizes the Build Mode Configuration	778
	Resynchronizing Device Configuration	778
	The Resynchronize Device Configuration List of Devices	779
	Resynchronizing Devices When Junos Space Is in NSOR Mode	780
	Resynchronizing Devices When Junos Space Is in SSOR Mode	781
	Resynchronizing Devices in Manual Approval Mode	782
	Viewing the Network Changes	782
	Viewing Resynchronization Job Status	782
	Managing Device Configuration Files	783
	Selecting Device Configuration File Management Options	783
	Backing Up Device Configuration Files	784
	Restoring Device Configuration Files	785
	Viewing Device Configuration Files	785
	Comparing Device Configuration Files	786
	Deleting Device Configuration Files	786

	Managing Device Configuration File Management Jobs	786
	Enabling or Disabling Network Ports on Routers	787
Chapter 31	Deploying and Managing Software Images	789
	Managing Software Images	789
	Selecting Software Image Management Options	789
	Adding Software Images to the Repository	790
	Using the Device Image Upload Window	790
	Viewing Software Image Details	791
	Using the Device Image Summary Window	791
	Deleting Software Images	791
	Deploying Software Images	791
	Specifying Software Deployment Job Options	792
	Selecting Software Images To Deploy	793
	Selecting Options for Software Deployment	794
	Summary of Software Deployment	795
	Managing Software Image Deployment Jobs	795
	Selecting Software Image Management Options	796
	Viewing Software Image Job Details	797
	Using the Device Image Staging Window	797
	Canceling Software Image Jobs	798
Part 10	Service Provisioning: Working with Service Orders	
Chapter 32	Service Provisioning: Viewing the Configured Services and Service Orders	801
	Viewing Service Orders	801
	Viewing Service Orders in a Table	801
	Viewing Service Order and Service Details	803
	Viewing Services	807
	Viewing Services in a Table	807
	Viewing the Configured Point-to-Point, L3VPN, and VPLS Services	809
	Viewing the Configuration Details of VPN Services	812
Chapter 33	Service Provisioning: Managing Point-to-Point Service Orders	815
	Creating a Service Order	815
	Creating a Point-to-Point ATM or TDM Pseudowire Service Order	816
	Selecting the Service Definition	816
	Entering General/Connectivity Settings Information	818
	Specifying Endpoint Information	820
	Specifying Template Settings	826
	Reviewing the Configured Settings	828
	Deploying the New Service	828
	Creating a Point-to-Point Service Order	829
	Selecting the Service Type	830
	Entering General Settings Information	832
	Specifying the Connectivity	833
	Specifying QoS Settings	835
	Specifying OAM Settings	835
	Specifying Endpoint Information	836

	Specifying Template Settings	841
	Reviewing the Configured Settings	843
	Specifying Connectivity and Endpoint Information for Managing VLANs	844
	Deploying and Monitoring the Progress of the New Service	844
	Creating a Bulk-Provisioning Service Order for Pseudowire Services	845
	Creating an Inverse Multiplexing for ATM Service Order	849
	Provisioning a Single-Ended Point-to-Point Service	853
	Selecting Specific LSPs for Connectivity Services	855
	Associating an LSP with a Point-to-Point Service	855
	Viewing LSP Details in a Service Order	856
	Viewing LSP Details in a Service	857
	Viewing LSP Configuration Details	857
	Stitching Two Point-to-Point Pseudowires	858
	Deactivating a Service	860
	Reactivating a Service	862
	Force-Deploying a Service	864
	Recovering a Service Definition through Force Upload	867
	Decommissioning a Service	868
	Viewing Alarms for a Service	871
	Inline Editing of VPLS and Layer 3 VPN Service Orders	872
	Interconnecting a Layer 3 VPN Service with a VPLS Service	876
	Changing the Logical Loopback Interface for Provisioning	878
Chapter 34	Service Provisioning: Managing VPLS Service Orders	881
	Creating a Multipoint-to-Multipoint VPLS Service Order	881
	Selecting the Service Definition	881
	Entering Service Parameters Information	884
	Specifying OAM Settings	890
	Selecting N-PE Devices	891
	Specifying Node Settings	893
	Setting Attributes for Nodes or Devices on a Service	893
	Setting Attributes for Nodes or Devices on a Service with Flexible VLAN Tagging	896
	Modifying Site Settings	896
	Specifying QoS Settings	902
	Specifying Template Settings	903
	Reviewing the Configured Settings	904
	Deploying the New Service	905
	Creating a Point-to-Multipoint VPLS Service Order	905
	Selecting the Service Definition	906
	Entering Service Parameters Information	909
	Specifying OAM Settings	915
	Selecting N-PE Devices	916
	Specifying Node Settings	918
	Setting Attributes for Nodes or Devices on a Service	918
	Setting Attributes for Nodes or Devices on a Service with Flexible VLAN Tagging	922
	Modifying Site Settings	922
	Specifying QoS Settings	927

	Specifying Template Settings	928
	Reviewing the Configured Settings	929
	Deploying the New Service	930
	Creating a Service Order for VPLS Access into Layer 3 Networks	930
	Creating a VPLS Service Order with CFM	933
	Interconnecting a VPLS Service with a Layer 3 VPN Service	936
Chapter 35	Service Provisioning: Managing Layer 3 VPN Service Orders	939
	Stitching a Pseudowire to an L3VPN Service	939
	Creating a Full Mesh Layer 3 VPN Ethernet Service Order	941
	Selecting the Service Definition	941
	Configuring Service Parameters Information	943
	Specifying General Settings	943
	Specifying PE-CE Settings Information	946
	Selecting N-PE Devices or Nodes	947
	Setting Attributes for Endpoints or Nodes	948
	Adding and Deleting UNI Interfaces	954
	Setting Attributes for UNIs or Sites	954
	Specifying QoS Settings	961
	Specifying Template Settings	961
	Reviewing the Configured Settings	963
	Deploying the New Service	963
	Creating a Hub-and-Spoke Layer 3 VPN Service Order	964
	Selecting the Service Definition	964
	Configuring Service Parameters Information	965
	Specifying General Settings	965
	Specifying PE-CE Settings Information	968
	Selecting N-PE Devices or Nodes	969
	Setting Attributes for Endpoints or Nodes	970
	Adding and Deleting UNI Interfaces	976
	Setting Attributes for UNIs or Sites	976
	Specifying QoS Settings	982
	Specifying Template Settings	983
	Reviewing the Configured Settings	984
	Deploying the New Service	985
	Selecting a Published L3VPN Service Definition for a Service Order	985
	Entering Layer 3 VPN Order Information	986
	Setting General Settings	986
	Entering VPN and Connectivity Settings Information	987
	Entering PE-CE Settings	988
	Selecting Endpoint PE Devices or Nodes	988
	Creating a Service Order Based on a Service Definition with a Template	990
	Deploying a Layer 3 VPN Service Order	993
	Creating a Multicast VPN Service Order	995
	Creating Policies for a Layer 3 VPN Service	998

Part 11

Chapter 36

Service Provisioning: Working with Services Deployment

Service Provisioning: Managing Deployed Services	1003
Managing Service Configuration Deployment Jobs	1003
Selecting Service Configuration Deployment Job Options	1004
Viewing Service Configuration Deployment Job Details	1005
Canceling Service Configuration Deployment Jobs	1005
Deploying Services Configuration to Devices	1005
Selecting Configuration Deployment Options	1007
Validating Configuration	1007
Deleting the Partial Service Configurations	1009
Discarding the Pending Configurations	1011
Deploying Configuration Changes to Devices Immediately	1012
Scheduling Configuration Deployment	1012
Specifying Configuration Deployment Scheduling Options	1012
Deploy Configuration Window	1013
Deleting a Partial Configuration of an LSP Service Order	1014
Deleting a Service Order	1015
Deploying a Service	1016
Validating the Pending Configuration of a Service Order	1018
Viewing the Configuration of a Pending Service Order	1020
Viewing Decommissioned Point-Point, VPLS, and L3VPN Service Orders	1022
Modifying a Point-to-Point Ethernet Service	1024
Modifying a Multipoint-to-Multipoint Ethernet Service	1026
Adding an Endpoint	1027
Adding a UNI Interface	1028
Deleting a UNI Interface and Deleting an Endpoint	1030
Changing the Endpoint Bandwidth	1031
Changing Advanced Settings for an Endpoint	1032
Modifying a Point-to-Multipoint Ethernet Service	1033
Adding a Spoke	1034
Adding a Hub	1035
Changing a Spoke to a Hub	1036
Changing a Hub to a Spoke	1037
Adding a UNI Interface	1038
Deleting a UNI Interface or Deleting an Endpoint	1039
Changing the Endpoint Bandwidth	1040
Changing Advanced Settings for an Endpoint	1041
Modifying a Hub-and-Spoke Layer 3 VPN Service Order	1042
Viewing the Service Definition	1043
Configuring Service Parameters Information	1044
Specifying General Settings	1044
Specifying PE-CE Settings Information	1048
Selecting N-PE Devices or Nodes	1049
Setting Attributes for Endpoints or Nodes	1050
Adding and Deleting UNI Interfaces	1053
Setting Attributes for UNIs or Sites	1054
Deploying the New Service	1057

	Modifying a Full Mesh Layer 3 VPN Ethernet Service	1057
	Adding an Endpoint	1058
	Adding a UNI Interface	1060
	Deleting a UNI Interface and Deleting an Endpoint	1062
	Understanding Service Validation	1063
	Highlighting of Endpoints in the Layer 3 VPN, RSVP LSP, and VPLS Service Modification Wizards	1064
Part 12	Auditing Services and Viewing Audit Results	
Chapter 37	Service Provisioning: Auditing Services	1067
	Performing a Functional Audit	1067
	Performing a Configuration Audit	1077
	Troubleshooting N-PE Devices Before Provisioning a Service	1080
	Modifying the Application Settings of Connectivity Services Director	1082
	Troubleshooting the Endpoints of Services	1088
	Troubleshooting Services Using Operational Scripts	1090
	Basic Requirements of Operational Scripts	1095
	Predefined Scripts for Troubleshooting	1097
	P2P LDP Service	1097
	P2P BGP Service	1097
	VPLS Service	1097
	L3VPN Service	1097
	RSVP LSP Service	1098
	Viewing Configuration Audit Results	1098
	Viewing Functional Audit Results	1102
	Viewing Functional Audit Results for an Inverse Multiplexing for ATM Service . .	1106
	Modifying a Saved Service Order	1107
	Viewing Service-Level Alarms	1110
Chapter 38	Troubleshooting Devices and Services	1113
	Performance Management Overview	1113
	Monitoring Performance Statistics	1113
	On-Demand Mode	1114
	Proactive Mode	1114
	Performance Management of Test Traffic	1114
	Monitoring Performance Management Statistics	1115
	Monitoring Statistics for a Point-to-Point Service	1116
	Monitoring Statistics for a VPLS Service	1118
	Viewing Performance Management Statistics	1121
	Viewing Y.1731 Performance Monitoring Statistics for Point-to-Point Services	1121
	Viewing Y.1731 Performance Monitoring Statistics for VPLS Services	1125
	Service Troubleshooting Overview	1129

Part 13**Chapter 39****Working in Monitor Mode****About Monitor Mode 1133**

Understanding Monitor Mode in Views Other than Service View of Connectivity

Services Director 1133

Scope and Monitor Tab Availability 1133

Monitors and Tasks 1134

Scope and Data Aggregation 1134

How Connectivity Services Director Collects and Displays Monitoring

Data 1134

How Connectivity Services Director Displays and Stores Trend Data 1135

More About the Monitor Tabs 1136

The Summary Tab 1136

The Traffic Tab 1136

Understanding the Monitor Mode Tasks Pane in Views Other than Service

View 1136

Chapter 40**Monitoring Traffic 1139**

Monitoring Traffic on Devices 1139

Monitoring Port Traffic Statistics 1140

Procedure for Monitoring Port Traffic Statistics 1140

Port on Device Window 1140

Port Traffic Stats Window 1141

Monitoring Traffic on Layer 3 VLANs 1142

Procedure for Monitoring Layer 3 VLAN Traffic Statistics 1142

L3 VLAN Traffic Stats Window 1142

Monitoring Port Utilization 1143

How to Access the Port Utilization Task 1143

Port Utilization Details Window 1144

Utilization for Device Window 1144

Device View 1145

Port View 1145

Utilization for IP Fabric Window 1146

Device View 1146

Port View 1147

Monitoring Routing Instances 1147

Procedure for Monitoring Routing Instances 1148

Show Routing Instances Window 1148

Show Interfaces Window 1149

Show Bridge Domains Window 1150

Show Connections 1151

Show Routing Tables 1154

Show MAC Table 1156

Viewing Congestion Events 1157

Chapter 41	Monitoring Devices	1159
	Comparing Device Statistics	1159
	Procedure for Comparing Device Statistics	1159
	Compare Interfaces Window	1159
	Showing ARP Table Information	1160
	Procedure for Showing ARP Table Information	1160
	Show ARP Table Information Window	1161
Chapter 42	General Monitoring	1163
	Selecting Monitors To Display on the Summary Tab	1163
	Changing Monitor Polling Interval and Data Collection	1164
	Pinging Host Devices	1164
	Troubleshooting Network Connections Using Traceroute	1165
Chapter 43	Monitor Reference	1167
	Error Trend Monitor	1167
	Error Trend	1168
	Error Trend Details	1168
	Equipment Status Summary Monitor	1169
	Equipment Summary By Type Monitor	1170
	Equipment Summary By Type	1170
	Equipment Summary By Type Details	1170
	Port Status Monitor	1170
	Port Status Summary	1171
	Port Status Details	1171
	Port Utilization Monitor	1172
	Status Monitor for Routers	1172
	Traffic Trend Monitor	1173
	Unicast vs Broadcast/Multicast Monitor	1173
	Unicast vs Broadcast/Multicast Trend Monitor	1174
	Session Trends Monitor	1175
	Session Trends	1175
	Session Details	1175
	Current Sessions by Type Monitor	1177
	Current Sessions by Type	1177
	Current Session Details	1177
	User Session Details Window	1177
	Current Active Alarms Monitor (All Views Except Service View)	1179
	Top Sessions by MAC Address Monitor	1180
	Top Sessions	1180
	Top Session by MAC Details	1180
	Top APs by Session Monitor	1181
	Top APs by Session Summary	1181
	Top APs by Session Details	1181
	Radio Technology Type Statistics Monitor	1182
	Radio Technology Type Statistics Summary	1182
	Radio Technology Type Statistics Details	1183

Chapter 44

Top Talker - Wired Devices Monitor	1183
Top Talker - Wired Devices Summary	1183
Top Talker - Wired Devices Details	1184
Top Users Monitor	1184
Top Users	1184
Top Session By User Details	1185
Top APs by Traffic Monitor	1185
Top APs by Traffic Summary	1186
Top APs by Traffic Details	1186
Top Talker - Wireless Devices Monitor	1186
Top Talker-Wireless Devices Summary	1186
Top Talker-Wireless Devices Details	1187
RF Interference Sources Monitor for Devices	1187
Detecting and Examining the Health and Performance of Services	1191
Service Monitoring Capabilities in Connectivity Services Director	1192
Computation of Statistics Polled from Devices for Display in Widgets on Monitoring Pages	1193
Configuring the Aggregation Method for Viewing Monitoring Details	1194
Viewing the Service Monitoring Summary Page for a Consolidated Listing of Services	1196
Monitoring the Service Summary Details of P2P Services for Optimal Debugging	1199
Service Status	1201
Connections	1201
Traffic Summary	1202
Section	?
Monitoring the Service Summary Details of VPLS Services for Optimal Debugging	1202
Service Status	1204
Connections	1205
Traffic Summary	1205
Monitoring the Service Summary Details of Layer 3 VPN Services for Optimal Debugging	1206
Service Status	1207
VPN Routes	1208
VPN Traffic Trend	1208
Monitoring the Service Traffic Statistics of P2P Services for Correlating Device Counters	1209
Traffic Graph	1210
Pseudowire Traffic	1211
Interface Traffic Statistics/Endpoint Users	1212
Monitoring the Service Traffic Statistics of VPLS Services for Correlating Device Counters	1213
Traffic Matrix	1214
Interface Statistics	1214
Traffic Pattern	1215

Monitoring the Service Traffic Statistics of Layer 3 VPN Services for Correlating	
Device Counters	1215
Interface Statistics	1217
VPN Traffic Trend	1217
Monitoring the Service Transport Details of P2P Services for Easy Analysis	1218
Connections	1219
LSP Information	1220
LSP Traffic	1221
Monitoring the Service Transport Details of VPLS Services for Easy Analysis	1221
Connections	1223
LSP Information	1223
LSP Traffic	1224
Monitoring the Service Transport Details of Layer 3 VPN Services for Easy	
Analysis	1225
Transport Statistics	1226
VPN Routes	1227
Label/LSP Information	1227
LSP Traffic	1229
Viewing Y.1731 Performance Monitoring Statistics for Point-to-Point Services	1229
Connections	1231
Loss Measurement	1231
Delay Measurement	1232
Delay Variation	1232
Viewing Y.1731 Performance Monitoring Statistics for VPLS Services	1233
Connections	1234
Loss Measurement	1235
Delay Measurement	1235
Delay Variation	1235
Clearing Interface Statistics	1237
Viewing MAC Table Details	1239
Viewing Interface Statistics	1241
Viewing Interface Status Details	1243
MPLS Connectivity Verification and Troubleshooting Methods	1245
Using MPLS Ping	1247
Pinging VPNs, VPLS, and Layer 2 Circuits	1249
Monitoring Network Reachability by Using the MPLS Ping Capability	1250
Monitoring Network Reachability by Using the Layer 3 VPN Ping Capability	1253
Routing Table Overview	1256
Viewing Routing Table Details	1256

Part 14

Chapter 45

Working in Fault Mode

About Fault Mode 1263

About Fault Mode in All Views of Connectivity Services Director 1263

Understanding the Tasks Pane in Fault Mode 1264

Chapter 46

Using Fault Mode 1267

Using Fault Management Monitors 1267

 What Are Events and Alarms? 1267

 Alarm Severity 1268

	Alarm Classification	1268
	Alarm State	1269
	Alarm Notifications	1269
	Threshold Alarms	1270
	Alarm Severities and States Overview	1270
	Alarm Severity	1270
	Alarm State	1271
	Events and Alarms Overview	1271
	Alarm Severity	1271
	Customizing Alarms	1272
	Changing Alarm State	1272
	Searching Alarms	1273
Chapter 47	Fault Reference	1277
	Alarm Detail Monitor (All Views Except Service View)	1277
	Finding Specific Alarms	1277
	Sorting Alarms	1279
	Reading Events	1279
	Investigating Event Attributes	1280
	Changing the Alarm State	1280
	Alarm Detail Monitor (Service View)	1280
	Finding Specific Alarms	1281
	Sorting Alarms	1282
	Reading Events	1282
	Investigating Event Attributes	1283
	Changing the Alarm State	1283
	Current Active Alarms Monitor (Service View)	1284
	Alarms by Category Monitor	1285
	Alarms by Severity Monitor (Service View)	1285
	Alarms by State Monitor	1286
	Alarm Trend Monitor (Service View)	1287
	Alarms by Severity Monitor (All Views Except Service View)	1287
	Alarms by State Monitor (All Views Except Service View)	1288
	Current Active Alarms Monitor (All Views Except Service View)	1288
	Alarm Trend Monitor (All Views Except Service View)	1289
Part 15	End-to-End Configuration Examples	
Chapter 48	Configuration Scenarios	1293
	Example: Configuring and Deploying a Point-to-Point Ethernet Service	1293
	Preparing Devices for Discovery	1294
	Discovering Devices	1294
	Preparing Devices for Prestaging	1296
	Discovering and Assigning N-PE Roles	1297
	Choosing or Creating a Service Definition	1298
	Creating a Customer	1300
	Creating and Deploying a Point-to-Point Service Order	1301

	Performing a Functional Audit and a Configuration Audit	1303
	Example: Configuring and Deploying a Multipoint-to-Multipoint VPLS	
	Service	1305
	Preparing Devices for Discovery	1306
	Discovering Devices	1307
	Preparing Devices for Prestaging	1308
	Discovering and Assigning N-PE Roles	1311
	Choosing or Creating a Service Definition	1312
	Creating a Customer	1315
	Creating and Deploying a Multipoint-to-Multipoint Service Order	1316
	Performing a Functional Audit and a Configuration Audit	1318
	Example: Configuring and Deploying a Layer 3 VPN Full-Mesh Service	1319
	Preparing Devices for Discovery	1320
	Discovering Devices	1321
	Preparing Devices for Prestaging	1322
	Discovering and Assigning N-PE Roles	1323
	Choosing or Creating a Service Definition	1324
	Creating a Customer	1326
	Creating and Deploying a Layer 3 VPN Service Order	1327
	Performing a Functional Audit and a Configuration Audit	1329
Part 16	Working with Chassis View	
Chapter 49	Working with Devices	1335
	About Chassis View	1335
	Accessing the Chassis View from the Physical Inventory Page	1337
	Viewing a Graphical Image of the Chassis and Components	1338
	Deleting Devices from Chassis View	1345
	Rebooting Devices After Examining the Status in Chassis View	1346
Chapter 50	Managing CLI Configlets	1349
	CLI Configlets Overview	1349
	Configlet Variables	1350
	Default Variables	1350
	User-defined Variables	1350
	Predefined Variables	1350
	Velocity Templates	1350
	Directives	1351
	CLI Configlets Workflow	1352
	Configlet Context	1355
	Context of an Element	1356
	Context filtering	1357
	Creating a CLI Configlet	1360
	Modifying a CLI Configlet	1363
	Deleting CLI Configlets	1363
	Viewing CLI Configlets	1364
	Creating a Parameter for a CLI Configlet	1366
	Applying a CLI Configlet to Devices	1368
	Deploying CLI Configlet Details	1372

Part 17	Managing Optical Interfaces, OTUs, ODUs, ILAs, and IPLCs on MX Series and PTX Series Routers	
Chapter 51	Overview of Optical Interfaces, OTUs, and ODUs	1377
	Optical Interfaces Management and Monitoring on MX Series and PTX Series Routers Overview	1378
	Ethernet DWDM Interface Wavelength Overview	1380
	Attenuation and Dispersion in a Fiber-Optic Cable on PTX Series Routers Overview	1380
	Understanding Pre-FEC BER Monitoring and BER Thresholds	1381
	DWDM Controllers Overview	1384
	PTX5000 PIC Description	1385
	PTX5000 PIC Slots	1385
	PTX5000 PIC Function	1385
	PICs Supported on the PTX5000	1385
	PTX5000 PIC Components	1385
	PTX3000 PIC Description	1386
	PIC Slots	1386
	PIC Function	1388
	PICs Supported	1388
	PIC Components	1388
	100-Gigabit Ethernet OTN Optical Interface Specifications	1389
	OTU4 4I1-9D1F Optical Interface Specifications	1389
	100-Gigabit DWDM OTN PIC Optical Interface Specifications	1390
	100-Gigabit DWDM OTN PIC (PTX Series)	1394
	Software Release	1394
	Hardware Features	1395
	Software Features	1395
	Cables and Connectors	1397
	LEDs	1397
	Alarms, Errors, and Events	1397
	100-Gigabit Ethernet OTN PIC with CFP2 (PTX Series)	1402
	Software Release	1402
	Hardware Features	1402
	Software Features	1403
	Cables and Connectors	1403
	LEDs	1404
	100-Gigabit Ethernet PIC with CFP2 (PTX Series)	1405
	Software Release	1405
	Hardware Features	1405
	Software Features	1406
	Cables and Connectors	1406
	LEDs	1407
	Alarms, Errors, and Events	1407
	100-Gigabit Ethernet PIC with CFP (PTX Series)	1408
	Software Release	1408
	Hardware Features	1409
	Software Features	1409
	Cables and Connectors	1411

LEDs	1412
Alarms, Errors, and Events	1413
100GbE PICs for PTX Series Routers	1414
Architecture and Key Components	1414
P2-10G-40G-QSFPP PIC Overview	1415
Understanding Dual Configuration on P2-10G-40G-QSFPP PIC	1415
Port Numbering on P2-10G-40G-QSFPP PIC	1416
10-Gigabit Ethernet Mode	1418
40-Gigabit Ethernet Mode	1418
Understanding the P2-100GE-OTN PIC	1419
Interface Features	1419
Layer 2 and Layer 3 Features	1421
OTN Alarms and Defects	1422
TCA Alarms	1422
100-Gigabit DWDM OTN PIC with CFP2 (PTX Series)	1423
Software Release	1423
Hardware Features	1424
Software Features	1425
Cables and Connectors	1426
LEDs	1426
Alarms, Errors, and Events	1426
100-Gigabit DWDM OTN MIC with CFP2	1432
100-Gigabit Ethernet OTN Options Configuration Overview	1440
Configuring the 10-Gigabit or 100-Gigabit Ethernet DWDM Interface	
Wavelength	1442
Chapter 52	
Overview of Optical ILAs and IPLCs	1445
Optical ILA Hardware Component Overview	1445
Optical ILA Cooling System Description	1446
Fan Modules	1446
Optical ILA AC Power Supply Description	1447
Optical ILA DC Power Supply Description	1448
Optical ILA Chassis Status LEDs	1449
Optical ILA Component Redundancy	1451
Optical ILA Field-Replaceable Units	1452
Optical ILA Management Panel	1453
Optical ILA Management Port LEDs	1454
Optical Inline Amplifier Description	1455
Front Panel	1456
FRU Panel	1456
Optical ILA Power Supply LEDs	1457
PTX3000 IPLC Description	1459
IPLC Base Module	1460
IPLC Base Module Components	1461
IPLC Expansion Module	1463
IPLC Components	1464

IPLC Architecture and Functional Components Overview	1466
Architecture Overview	1466
Single Node Two Optical Line Terminations	1467
Functional Component Overview	1467
IPLC Base Module Functional Components	1467
IPLC Expansion Module Functional Components	1468
Understanding IPLC Base and Expansion Modules	1469
Overview	1469
Configuring, Managing, and Monitoring the IPLC	1470
SNMP	1470
Connectivity Services Director	1470
Optical Supervisory Channel	1470
High Availability, Resiliency, and Integrity	1470
Usability, Serviceability, Security and Troubleshooting	1470
Performance Monitors	1471
Usage Scenarios	1471
Optical Bypass Node Configuration	1471
Understanding the IPLC Configuration	1471
Understanding the Front Panel Connections	1472
Slot Placement in the Chassis	1472
Understanding How to Configure the Add and Drop Ports	1472
Frequency, Wavelength, and Port Default Mapping Configuration	1473
PTX3000 IPLC LED	1477
Communication of SNMP Traps Between Optical ILA and NMS Systems	1478
Communication of SNMPv2 and SNMPv3 Commands over OSC Between an Optical ILA and NMS	1478
Overview of Configuring and Managing Optical ILAs from Connectivity Services Director Using DMI	1479
Configuration Settings Performed Using the CLI	1479
Set Parameters for SNMP	1480
Get Parameters for SNMP	1480
Alarms	1480
IPLC Specifications	1481
Understanding the Performance Monitors and TCAs for IPLCs	1482
Chapter 53	
Configuring and Monitoring Optical Interfaces, OTUs, and ODUs	1487
Viewing a Graphical Image of the Optical Interface Components	1487
Configuring and Managing OTN Port Details of MX Series and PTX Series Routers for Easy Administration	1497
Configuring and Managing OTU Details of MX Series and PTX Series Routers for Simplified Management	1505
Configuring and Managing ODU Details of MX Series and PTX Series Routers for Simplified Management	1512
Configuring and Managing Optical PIC Details for Effective Provisioning	1517
Configuring Threshold-Crossing Alarms for OTN Ports for Monitoring Link Performance	1519
Configuring Threshold-Crossing Alarms for OTUs for Monitoring Link Performance	1523

	Configuring Threshold-Crossing Alarms for ODUs for Monitoring Link Performance	1527
	Viewing Performance Monitoring Details of OTN Ports for Detecting and Diagnosing Faults	1530
	Viewing Performance Monitoring Details of OTUs for Detecting and Diagnosing Faults	1541
	Viewing Performance Monitoring Details of ODUs for Detecting and Diagnosing Faults	1549
	Viewing a Graphical Image of the Chassis of PTX Series Routers	1556
	Diagnosing, Examining, and Correcting Optical Interface Problems	1561
	Optical Alarms, 24 Hour Threshold-Crossing Alarms (TCA), and 15 Minute Threshold-Crossing Alarms (TCA)	1562
	OTU Alarms, 24 Hour Threshold-Crossing Alarms (TCA), and 15 Minute Threshold-Crossing Alarms (TCA)	1563
	ODU Alarms, 24 Hour Threshold-Crossing Alarms (TCA), and 15 Minute Threshold-Crossing Alarms (TCA)	1564
	Changing Alarm Settings for the Optics and OTN Interfaces	1565
	Alarms for Optical Interfaces	1566
	Alarms for OTN Interfaces	1571
	Configuring Global Alarm Notifications	1576
	Retaining Alarm History	1576
	Specifying Event History	1577
	Enabling Alarms	1577
	Changing the Severity of Individual Alarms	1577
	Configuring Threshold Alarms	1577
	Configuring Individual Alarm Notifications	1578
Chapter 54	Configuring and Monitoring Optical Inline Amplifiers	1579
	Viewing a Graphical Image of Optical Inline Amplifier	1579
	Viewing Optical ILA Configuration and Status Details for Simplified Administration	1583
	Viewing Performance Monitoring Details of Optical ILAs for Detecting and Diagnosing Faults	1588
	Configuring Threshold-Crossing Alarms for Optical ILAs for Monitoring Link Performance	1597
	Changing Alarm Settings for the Optical ILAs	1599
	Alarms for Optical ILAs	1600
	Configuring Global Alarm Notifications	1602
	Retaining Alarm History	1602
	Specifying Event History	1602
	Enabling Alarms	1602
	Changing the Severity of Individual Alarms	1603
	Configuring Threshold Alarms	1603
	Configuring Individual Alarm Notifications	1603

Chapter 55	Configuring and Monitoring Optical Integrated Photonic Line Cards . . .	1605
	Viewing a Graphical Image of the Optical Integrated Photonic Line Card	1605
	Configuring Optical IPLC for Easy and Optimal Deployment	1609
	Viewing Performance Monitoring Details of Optical IPLCs for Detecting and Diagnosing Faults	1617
	Configuring Threshold-Crossing Alarms for Optical IPLCs for Monitoring Link Performance	1629
	Increasing the Add and Drop Port Capacity of the IPLC Node to 64 Channels . .	1634
	Configuring a Two-Degree IPLC Node for Express Traffic by Increasing the Line Capacity	1636
	Configuring Optical IPLC Line Connectivity for Interoperation with Optical ILAs	1638
	Configuring the Wavelengths That Are Added and Dropped by the IPLC	1645
	Configuring the IPLC to Add or Drop Wavelengths to an Optical Interface on a Remote Chassis	1649
	Configuring the IPLC to Add or Drop Wavelengths to an Optical Interface on the Same Chassis	1651
	Bypassing a Wavelength on the IPLC	1652
	Changing Alarm Settings for the Optical IPLCs	1654
	Alarms for Optical IPLCs	1655
	Configuring Global Alarm Notifications	1659
	Retaining Alarm History	1659
	Specifying Event History	1659
	Enabling Alarms	1659
	Changing the Severity of Individual Alarms	1659
	Configuring Threshold Alarms	1660
	Configuring Individual Alarm Notifications	1660
	Viewing Routing Engine Switchover Indicators in the Chassis Image	1661
	Routing Engine Redundancy Overview	1661
	Conditions That Trigger a Routing Engine Failover	1662
	Viewing Alarm Indicators in the Chassis Image	1663
	Viewing Port Statistics for OTN PICs	1664
	Example: Configuring Two Fiber Line Terminations Using IPLCs for Optical Amplification in a Metro Linear Packet Optical Network	1668
Part 18	Working with User Roles	
Chapter 56	Managing User Roles	1687
	Creating a User-Defined Role	1687
	Managing Roles	1689
	Viewing User Role Details	1689
	Performing Manage Roles Commands	1690
Part 19	Working with Tunnel Services	
Chapter 57	Tunnel Services Overview	1693
	Tunnel Services Overview	1693
	Traffic Engineering Capabilities	1694

Components of Traffic Engineering	1694
Packet Forwarding Component	1695
Packet Forwarding Based on Label Swapping	1695
How a Packet Traverses an MPLS Backbone	1695
Information Distribution Component	1696
Path Selection Component	1696
Signaling Component	1697
Routers in an LSP	1697
How a Packet Travels Along an LSP	1698
Types of LSPs	1698
Scope of LSPs	1699
Constrained-Path LSP Computation	1699
How CSPF Selects a Path	1700
CSPF Path Selection Tie-Breaking	1701
Computing CSPF Paths Offline	1702
MPLS and RSVP Overview	1702
RSVP Overview	1704
Fast Reroute Overview	1704
Point-to-Multipoint LSPs Overview	1706
RSVP Operation Overview	1708
RSVP Hello Packets and Timers	1709
RSVP Message Types	1710
Path Messages	1710
Resv Messages	1710
PathTear Messages	1710
ResvTear Messages	1711
PathErr Messages	1711
ResvErr Messages	1711
ResvConfirm Messages	1711
MTU Signaling in RSVP	1711
Link Protection and Node Protection	1712
Node Protection	1713
LSP Protection Overview	1714
LSP Protection Types Comparison	1715
One-to-One Backup Implementation	1715
Facility Backup Implementation	1716
Chapter 58	
Service Design and Provisioning: Managing and Deploying Tunnel Services	1719
Managing Devices and Tunnel Services Overview	1719
Discovering Tunnel Devices	1720
Creating an RSVP LSP Service Order	1722
Configuring LSP Order General Settings	1722
Configuring LSP Service Order Advanced Settings	1726
Configuring Common LSP Settings	1727
Configuring LSP Path Settings in the Service Order	1730
Configuring BFD Settings for LSPs in the Service Order	1735
Creating a Name Pattern for LSPs in the Service Order	1738
Configuring Node Settings for LSPs in the Service Order	1740

	Configuring MPLS Path Settings	1741
	Configuring LSP Primary Path Settings	1745
	Configuring LSP Secondary Path Settings	1747
	Reviewing the Configured Settings	1748
	Viewing the Configured LSP Services	1749
	Modifying an Explicit Path in RSVP LSP Services	1751
	Modifying an RSVP LSP Service	1753
	Viewing LSP Services in Deploy Mode	1754
	Viewing LSP Service Orders in a Table	1756
	Deactivating an LSP Service	1757
	Reactivating an LSP Service	1759
	Force-Deploying an LSP Service	1761
	Viewing Alarms for an LSP Service	1763
	Managing Deployment of LSP Services Configuration to Devices	1763
	Selecting Configuration Deployment Options	1765
	Discarding the Pending Configurations	1766
	Deploying Service Configuration Changes to Devices Immediately	1767
	Scheduling Configuration Deployment of Services	1768
	Specifying Configuration Deployment Scheduling Options	1768
	Deploying an LSP Service	1769
	Deleting a Partial Configuration of an LSP Service Order	1770
	Deleting an LSP Service Order	1772
	Validating the Pending Configuration of an LSP Service Order	1773
	Viewing the Configuration of a Pending LSP Service Order	1774
	Viewing the Configuration Details of RSVP LSP Services	1777
	Viewing Decommissioned LSP Service Orders	1779
Chapter 59	Monitoring and Troubleshooting Tunnel Services	1781
	Performing a Functional Audit for LSP Services	1781
	Viewing Functional Audit Results for LSP Services	1789
	Examining the LSP Summary Details for Effective Troubleshooting	1793
	Operational Status	1794
	Status Matrix	1795
	LSP Information	1795
	LSP Traffic	1796
	Troubleshooting the Endpoints of RSVP LSP Services	1796
	Troubleshooting Services Using Operational Scripts	1798
	Clearing LSP Statistics	1801
	Monitoring Network Reachability by Using the MPLS Traceroute Capability	1803
	Monitoring Network Reachability by Using the MPLS Ping Capability for RSVP LSPs	1806

Part 20	Appendix: Managing Network Activate Features Using the Older Version of Services Activation Director	
Chapter 60	Service Design: Working with Point-to-Point, Layer 3 VPN, and VPLS Service Templates	1811
	Service Templates Overview	1812
	Service Templates Workflow	1813
	Service Designer Tasks	1813
	Service Provisioner Tasks	1813
	Applying a Service Template to a Service Definition	1814
	Creating a Service Template	1815
	Naming a Template and Selecting Configuration Options	1816
	Configuration Options, Their Data Types and the Tabs Displayed	1818
	Deleting a Service Template	1819
	Exporting a Service Template	1820
	Finding Configuration Options	1821
	Importing a Service Template	1824
	Modifying a Service Template	1825
	Specifying Service-Specific Values	1826
	User Privileges in Service Templates	1836
	Provisioning Dynamic Attributes to Specify the Device XPath	1837
	Viewing Service Template Inventory	1838
Chapter 61	Service Provisioning: Working with Threshold Alarm Profiles	1841
	Creating a Threshold Alarm Profile	1842
	Viewing Threshold Alarm Profile Performance Parameters	1844
	Attaching a Threshold Alarm Profile to a Service Definition	1845
	Viewing Threshold Alarm Profile Performance Status	1846
	Editing a Threshold Alarm Profile	1847

List of Figures

Part 1	Overview	
Chapter 1	Working with Connectivity Services Director	3
	Figure 1: The Connectivity Services Director User Interface Components	10
	Figure 2: Connectivity Services Director Banner	11
	Figure 3: Performing Search on the View Pane	15
	Figure 4: Column Drop-Down Menu	17
Chapter 3	Network Services Overview	49
	Figure 5: Dashboard Page	51
	Figure 6: Point-to-Point LDP Connection Transports Traffic	57
	Figure 7: Point-to-Point Ethernet Services with 802.1Q Interfaces	57
	Figure 8: Point-to-Point Ethernet Service with Q-in-Q Interfaces for Range of VLANs	58
	Figure 9: Point-to-Point Ethernet Service with Q-in-Q Interfaces for Range of VLANs on Separate Service Provider VLANs	59
	Figure 10: Multipoint-to-Multipoint VPLS Service—Full Mesh	59
	Figure 11: Point-to-Multipoint VPLS Service with Single Hub	60
	Figure 12: Point-to-Multipoint VPLS Service with Multiple Hubs	61
	Figure 13: Autodiscovery of Service Connectivity	61
	Figure 14: Autodiscovery in a Point-to-Multipoint Service	62
	Figure 15: Service Order States and State Transitions	86
	Figure 16: Rendezvous Point as Part of the RPT and SPT	101
	Figure 17: Rendezvous Point as Part of the RPT and SPT	105
Part 2	Getting Started With Connectivity Services Director	
Chapter 4	Understanding Connectivity Services Director System Administration and Preferences	115
	Figure 18: Accessing the Preferences Page	123
Part 3	Working with the Dashboard	
Chapter 5	About the Dashboard	157
	Figure 19: Dashboard Page	157
Part 5	Building a Topology View of the Network	
Chapter 16	Downloading and Installing CSD-Topology	261
	Figure 20: Interfaces and Addresses Preconfigured on the x86 Appliance	283
	Figure 21: CSD-Topology Main Menu	284
	Figure 22: CSD-Topology Controller Main Menu	287

Chapter 18	Accessing the Topology View of CSD-Topology	299
	Figure 23: Topology Map Window	305
	Figure 24: Device Details in the Topology Map Window	317
	Figure 25: LSP Details in the Topology Map Window	318
	Figure 26: Link Details in the Topology Map Window	321
	Figure 27: Service Details in the Topology Map Window	323
Part 6	Prestaging	
Chapter 21	Prestaging: Managing IP Addresses	389
	Figure 28: Add New IP Pool Dialog Box	390
	Figure 29: Manage Resource Page	392
Chapter 22	Device Configuration Prerequisites to Prestaging Examples	397
	Figure 30: Connectivity in a Simple Network	402
Part 7	Service Design: Working with Service Definitions	
Chapter 24	Service Design: Predefined Service Definitions	465
	Figure 31: Point-to-Point Service	466
	Figure 32: Multipoint-to-Multipoint Service	490
	Figure 33: Point-to-Multipoint Service	515
	Figure 34: Point-to-Point Service	518
	Figure 35: Multipoint-to-Multipoint Service	551
	Figure 36: Point-to-Multipoint Service with One Hub	578
	Figure 37: Point-to-Multipoint Service with Two Hubs	584
Part 8	Service Provisioning: Working with Customers	
Chapter 28	Service Provisioning: Managing Customers	737
	Figure 38: Add Customer Dialog Box	738
Part 10	Service Provisioning: Working with Service Orders	
Chapter 32	Service Provisioning: Viewing the Configured Services and Service Orders	801
	Figure 39: View Service Details Window	804
	Figure 40: View Network Services Page	810
Chapter 34	Service Provisioning: Managing VPLS Service Orders	881
	Figure 41: Choose Endpoints Dialog Box	892
	Figure 42: Choose Endpoints Dialog Box	899
	Figure 43: Manage Service Orders Page	907
	Figure 44: Choose Endpoints Dialog Box	917
	Figure 45: Choose Endpoints Dialog Box	924
Chapter 35	Service Provisioning: Managing Layer 3 VPN Service Orders	939
	Figure 46: Choose Endpoints Dialog Box	989
	Figure 47: Manage Service Orders Page	994

Part 11	Service Provisioning: Working with Services Deployment	
Chapter 36	Service Provisioning: Managing Deployed Services	1003
	Figure 48: Delete Partial Configuration Confirmation	1010
	Figure 49: Discard Pending Configuration Confirmation	1012
Part 12	Auditing Services and Viewing Audit Results	
Chapter 37	Service Provisioning: Auditing Services	1067
	Figure 50: Accessing the Preferences Page	1082
	Figure 51: Service Order States	1108
Part 13	Working in Monitor Mode	
Chapter 44	Detecting and Examining the Health and Performance of Services	1191
	Figure 52: Service Monitoring Summary Page	1198
	Figure 53: Service Traffic Page for a P2P Service	1210
	Figure 54: Traffic Graph Monitor for P2P Service with Resiliency	1211
	Figure 55: Service Traffic Page for a VPLS Service	1214
	Figure 56: Service Traffic Page for an L3VPN Service	1217
	Figure 57: Service Transport Page for a VPLS Service	1223
	Figure 58: Service Transport Page for an L3VPN Service	1226
	Figure 59: Interface Traffic Status for a P2P Service	1244
	Figure 60: Interface Traffic Status for a VPLS Service	1244
Part 15	End-to-End Configuration Examples	
Chapter 48	Configuration Scenarios	1293
	Figure 61: Simple Point-to-Point Service	1293
	Figure 62: Simple Multipoint-to-Multipoint Service	1306
	Figure 63: Simple Layer 3 VPN Full-Mesh Service	1319
	Figure 64: Example of a Simple VPN Topology	1320
Part 17	Managing Optical Interfaces, OTUs, ODUs, ILAs, and IPLCs on MX Series and PTX Series Routers	
Chapter 51	Overview of Optical Interfaces, OTUs, and ODUs	1377
	Figure 65: PIC Faceplate	1386
	Figure 66: PIC Slots	1387
	Figure 67: PIC Faceplate	1389
Chapter 52	Overview of Optical ILAs and IPLCs	1445
	Figure 68: Fan Numbering	1447
	Figure 69: Fan Module	1447
	Figure 70: Power Supply Numbering	1447
	Figure 71: AC Power Supply in an Optical ILA	1448
	Figure 72: DC Power Supply in an Optical ILA	1449
	Figure 73: Chassis Status LEDs on an Optical ILA	1450
	Figure 74: Optical ILA FRU Panel	1452
	Figure 75: Optical ILA Management Panel Components	1453
	Figure 76: Management Port LEDs on the Optical ILA	1454

	Figure 77: Point-to-Point Configuration	1455
	Figure 78: Optical ILA Front Panel	1456
	Figure 79: Optical ILA FRU Panel	1456
	Figure 80: AC Power Supply LEDs	1457
	Figure 81: DC Power Supply LEDs	1457
	Figure 82: Point-to-Point Configuration	1459
	Figure 83: IPLC Base Module Faceplate	1461
	Figure 84: IPLC Expansion Module Faceplate	1464
	Figure 85: Combined Functions of the IPLC Base and Expansion Modules	1467
	Figure 86: IPLC Point-to-Point Configuration	1469
	Figure 87: IPLC LED	1477
Chapter 53	Configuring and Monitoring Optical Interfaces, OTUs, and ODUs	1487
	Figure 88: Chassis View of a PTX Series Router with an OTN MIC	1489
	Figure 89: Optical Port Dialog Box	1498
	Figure 90: OTU Section Dialog Box	1507
	Figure 91: ODU Path Dialog Box	1514
	Figure 92: PIC Status/Config Dialog Box	1518
	Figure 93: TCA Config Tab of the Optics PMs Dialog Box	1521
	Figure 94: TCA Config Tab of the OTU PMs Dialog Box	1525
	Figure 95: TCA Config Tab of the ODU PMs Dialog Box	1529
	Figure 96: Perf Mon Tab of the Optics PMs Dialog Box	1532
	Figure 97: 15 Mins Parameter-Name Tab of the Optics PMs Dialog Box	1536
	Figure 98: 24 Hours Parameter-Name Tab of the Optics PMs Dialog Box	1538
	Figure 99: Perf Mon Tab of the OTU PMs Dialog Box	1542
	Figure 100: 15 Mins Parameter-Name Tab of the OTU PMs Dialog Box	1544
	Figure 101: 24 Hours Parameter-Name Tab of the OTU PMs Dialog Box	1546
	Figure 102: Perf Mon Tab of the ODU PMs Dialog Box	1550
	Figure 103: 15 Mins Parameter-Name Tab of the ODU PMs Dialog Box	1552
	Figure 104: 24 Hours Parameter-Name Tab of the ODU PMs Dialog Box	1554
	Figure 105: Chassis View of a PTX Series Router	1557
Chapter 54	Configuring and Monitoring Optical Inline Amplifiers	1579
	Figure 106: Chassis View of an Optical ILA	1580
	Figure 107: Status/Config Tab of an Optical ILA	1584
	Figure 108: ILA Optics PMs Dialog Box	1589
	Figure 109: 24 Hours Parameter-Name Tab of the ILA Optics PMs Dialog Box	1595
	Figure 110: TCA Config Tab of the ILA Optics PMs Dialog Box	1598
Chapter 55	Configuring and Monitoring Optical Integrated Photonic Line Cards	1605
	Figure 111: Chassis View of a PTX Series Router with an Optical IPLC	1607
	Figure 112: Status/Config Tab of the IPLC Line Dialog Box	1610
	Figure 113: Perf Mon Tab of the IPLC Optics PMs Dialog Box	1618
	Figure 114: IPLC LineOut PMs Dialog Box	1620
	Figure 115: IPLC EDFA PMs Dialog Box	1622
	Figure 116: 15 Mins Parameter-Name Tab of the IPLC Optics PMs Dialog Box	1624
	Figure 117: 24 Hours Parameter-Name Tab of the IPLC LineOut Optics PMs Dialog Box	1626
	Figure 118: 24 Hours Parameter-Name Tab of the IPLC EDFA Optics PMs Dialog Box	1627

	Figure 119: TCA Config Tab of the IPLC Optics PMs Dialog Box	1631
	Figure 120: TCA Config Tab of the IPLC LineOut PMs Dialog Box	1632
	Figure 121: TCA Config Tab of the IPLC EDFA PMs Dialog Box	1633
	Figure 122: IPLC Line Connectivity Dialog Box	1640
	Figure 123: Line Connectivity Details Dialog Box	1644
	Figure 124: IPLC in Metro Linear Packet Optical Deployment	1670
Part 19	Working with Tunnel Services	
Chapter 57	Tunnel Services Overview	1693
	Figure 125: CSPF Computation Process	1700
	Figure 126: Label Encoding	1703
	Figure 127: Class-of-Service Bits	1703
	Figure 128: Detours Established for an LSP Using Fast Reroute	1705
	Figure 129: Detour After the Link from Router B to Router C Fails	1705
	Figure 130: Detours Merging into Other Detours	1706
	Figure 131: Point-to-Multipoint LSPs	1707
	Figure 132: Link Protection Creating a Bypass LSP for the Protected Interface . .	1713
	Figure 133: Node Protection Creating a Next-Next-Hop Bypass LSP	1714
	Figure 134: One-to-One Backup	1716
	Figure 135: Facility Backup	1717
Chapter 58	Service Design and Provisioning: Managing and Deploying Tunnel Services	1719
	Figure 136: Delete Partial Configuration Confirmation	1771
Chapter 59	Monitoring and Troubleshooting Tunnel Services	1781
	Figure 137: LSP Summary Page	1794
	Figure 138: Clear LSP Statistics Dialog Box	1802
	Figure 139: MPLS Traceroute Service Type - Service Name Window	1804
Part 20	Appendix: Managing Network Activate Features Using the Older Version of Services Activation Director	
Chapter 60	Service Design: Working with Point-to-Point, Layer 3 VPN, and VPLS Service Templates	1811
	Figure 140: Choose Templates dialog Box	1815
	Figure 141: Point-to-Point Example: Device Configuration Deployed Through Network Services	1828
	Figure 142: VPLS Example: Device Configuration Deployed Through Network Services	1829
	Figure 143: L3VPN Example: When OSPF Is a CE-PE Protocol	1830
	Figure 144: L3VPN Example: When BGP Is a CE-PE Protocol	1831

List of Tables

	About the Documentation	lv
	Table 1: Notice Icons	lvi
	Table 2: Text and Syntax Conventions	lvi
Part 1	Overview	
Chapter 1	Working with Connectivity Services Director	3
	Table 3: Connectivity Services Director Banner Functions	11
	Table 4: Numerical Sorts and Lexical Sorts	18
Chapter 3	Network Services Overview	49
	Table 5: Selecting a Layer 2 Service	55
	Table 6: Physical and Logical Encapsulation Compatibilities in Point-to-Point Ethernet Services	76
	Table 7: Physical and Logical Encapsulation Compatibilities in Multipoint Ethernet (VPLS) Services	76
	Table 8: VLAN Tag Rewrite Operations at UNI Ingress for Ethernet Services	90
	Table 9: VLAN Tag Rewrite Operations at UNI Egress for Ethernet Services	91
Part 2	Getting Started With Connectivity Services Director	
Chapter 4	Understanding Connectivity Services Director System Administration and Preferences	115
	Table 10: System Tasks	117
	Table 11: Audit Logs Page Fields	118
	Table 12: Job Management Page Fields	119
	Table 13: Log Files in the troubleshooting.zip File	121
	Table 14: Parameters in the Services Activation Tab	123
	Table 15: Monitor Mapping for Data Collectors	130
	Table 16: Default Polling Intervals	130
	Table 17: Alarm Descriptions	133
Part 3	Working with the Dashboard	
Chapter 7	Dashboard Widget Reference	161
	Table 18: Fields in the Current Active Flows Window	164
Part 4	Working in Build Mode	
Chapter 8	About Build Mode	171
	Table 19: Device Discovery Tasks	175
	Table 20: Device Management Tasks	175

	Table 21: Connectivity Tasks	176
	Table 22: Profile and Configuration Management Tasks	176
Chapter 9	Discovering Devices	177
	Table 23: Viewing Device Discover Jobs	182
	Table 24: Brownfield Job Page Fields	185
Chapter 10	Creating Custom Device Groups	187
	Table 25: Three Options of a Rule Statement	188
	Table 26: Three Options of a Rule Statement	191
Chapter 11	Configuring Quick Templates	193
	Table 27: Variable Data Types	193
	Table 28: Quick Templates	195
	Table 29: Quick Template Details	199
	Table 30: View Deployed Template	199
Chapter 12	Configuring Device Settings	201
	Table 31: Manage Device Common Settings Settings	202
	Table 32: Device Profile Basic Settings	205
	Table 33: Device Profile Management Settings for Routing	209
	Table 34: Device Profile Protocol Settings for Routing	211
Chapter 13	Configuring Class of Service (CoS)	219
	Table 35: 3-Bit CoS Field in Ethernet Header with VLAN Tagging	220
	Table 36: Managing Wired CoS Profile Fields	225
	Table 37: CoS Profile Settings for Routers, EX and Campus Switching ELS	228
	Table 38: Traffic Configuration and Shaping for EX Switching and Campus Switching ELS	228
	Table 39: CoS Profile Basic Settings for Campus Switching ELS CoS Profile with Hierarchical Port Scheduling (ETS)	232
	Table 40: Add Priority Group and Traffic Control Profile Window	233
	Table 41: Priority Group and Traffic Settings Table Properties	233
	Table 42: Edit and Add Traffic Classification and Shaping for Priority Group Window	233
	Table 43: PFC Settings for Campus Switching ELS CoS Profile with Hierarchical Port Scheduling (ETS)	234
	Table 44: Rewrite Rule Settings for Campus Switching ELS CoS Profile with Hierarchical Port Scheduling (ETS)	235
	Table 45: CoS Profile Basic Settings for Data Center Switching	236
	Table 46: Add Priority Group and Traffic Control Profile Window	237
	Table 47: Priority Group and Traffic Settings Table Properties	237
	Table 48: Edit and Add Traffic Classification and Shaping for Priority Group Window	237
	Table 49: Traffic Configuration and Shaping for EX Switching and Campus Switching ELS	239
	Table 50: PFC Settings for Data Center Switching Hierarchical Port Scheduling (ETS) CoS Profile	242
	Table 51: PFC Settings for Data Center Switching Non-Hierarchical Port Scheduling CoS Profile	242
	Table 52: Rewrite Rule Settings for Data Center Switching CoS Profile	242

Chapter 14	Configuring Link Aggregation Groups (LAGs)	245
	Table 53: LACP (Link Aggregation Control Protocol) Configuration Fields	246
Chapter 15	Managing Network Devices	251
	Table 54: Fields in the Device Inventory Table	252
	Table 55: Fields in the Device Physical Inventory Table	254
	Table 56: Viewing Licenses with Connectivity Services Director	254
Part 5	Building a Topology View of the Network	
Chapter 16	Downloading and Installing CSD-Topology	261
	Table 57: Minimum Hardware Requirements for VMware	263
	Table 58: Software Requirements for VMware	264
Part 6	Prestaging	
Chapter 20	Prestaging: Managing Devices and Device Roles	369
	Table 59: Prestage Device Jobs Page Fields	386
Chapter 21	Prestaging: Managing IP Addresses	389
	Table 60: Resource Pool Landing Page Details	392
Chapter 23	Prestaging Services	405
	Table 61: Service Recovery Jobs Page Fields	433
	Table 62: Mapping of Parameters, XPaths, and Supported Operations for Point-to-Point Services	441
	Table 63: Mapping of Parameters, XPaths, and Supported Operations for Layer 3 VPN Services	442
	Table 64: Mapping of Parameters, XPaths, and Supported Operations for VPLS Services	443
Part 7	Service Design: Working with Service Definitions	
Chapter 24	Service Design: Predefined Service Definitions	465
	Table 65: Standard Service Definitions	466
	Table 66: Standard Service Definitions	491
	Table 67: Standard Service Definitions	516
	Table 68: Standard Ethernet Point-to-Point Ethernet Service Definitions	519
	Table 69: Standard Multipoint-to-Multipoint Service Definitions	552
	Table 70: Standard Point-to-Multipoint Service Definitions	577
	Table 71: Standard Full-Mesh Layer 3 VPN Service Definitions	590
	Table 72: Standard Hub-and-Spoke Service Definitions	591
Chapter 25	Service Design: Managing Point-to-Point Service Definitions	593
	Table 73: Standard Ethernet Point-to-Point Service Definitions	594
	Table 74: Standard Multipoint-to-Multipoint Service Definitions	596
	Table 75: Standard Point-to-Multipoint Service Definitions	598
	Table 76: Maximum Bandwidth for M Series, MX Series, and ACX Series Routers	605
	Table 77: Maximum Bandwidth for M Series, MX Series, and ACX Series Routers	631

	Table 78: Service Definition Table Fields	650
Chapter 26	Service Design: Managing VPLS Service Definitions	653
	Table 79: Maximum Bandwidth for M Series, MX Series, and ACX Series Routers	663
	Table 80: Maximum Bandwidth for M Series, MX Series, and ACX Series Routers	689
Chapter 27	Service Design: Managing Layer 3 VPN Service Definitions	709
	Table 81: Layer 3 VPN Service Definition – General Settings	710
	Table 82: Layer 3 VPN Service Definition – PE-CE UNI Settings	713
	Table 83: Maximum Bandwidth for M Series, MX Series, and ACX Series Routers	714
	Table 84: Layer 3 VPN Service Definition – General Settings	721
	Table 85: Layer 3 VPN Service Definition – PE-CE UNI Settings	724
	Table 86: Maximum Bandwidth for M Series, MX Series, and ACX Series Routers	725
Part 9	Working in Deploy Mode	
Chapter 29	About Deploy Mode	745
	Table 87: Configuration Deployment Tasks	748
	Table 88: Image Management Tasks	749
	Table 89: Device Management Tasks	749
	Table 90: Device Configuration File Management Tasks	749
	Table 91: Baseline Management Tasks	749
Chapter 30	Deploying and Managing Device Configurations	751
	Table 92: Devices with Pending Changes Page	753
	Table 93: Devices with recent configuration changes	754
	Table 94: Change Requests	755
	Table 95: Change Request Details	755
	Table 96: Pending Changes Window	758
	Table 97: Configuration Validation Window	759
	Table 98: Deploy Options Window	760
	Table 99: Deploy Configuration Table Description	763
	Table 100: Deploy Configuration Window	764
	Table 101: Change request(s) pending approval	765
	Table 102: approved/declined change request(s)	766
	Table 103: Device Page Fields	767
	Table 104: EX Series Switches Traps	769
	Table 105: Controllers Traps	770
	Table 106: Resynchronize Device Configuration Fields	779
	Table 107: Manage Device Configuration Table	784
Chapter 31	Deploying and Managing Software Images	789
	Table 108: Device Image Repository Table	790
	Table 109: Device Image Summary Window	791
	Table 110: Select images for devices Table	793
	Table 111: Image Management Job Options	794
	Table 112: Image Deployment Jobs Table	796

	Table 113: Device Image Staging Window Description	797
Part 10	Service Provisioning: Working with Service Orders	
Chapter 32	Service Provisioning: Viewing the Configured Services and Service Orders	801
	Table 114: Fields in the Services Table	808
	Table 115: Fields in the Services Table	811
Chapter 35	Service Provisioning: Managing Layer 3 VPN Service Orders	939
	Table 116: Layer 3 VPN Service Order - Service Settings	944
	Table 117: Layer 3 VPN Service Order - PE-CE Settings	947
	Table 118: Layer 3 VPN Service Order - Topology Settings	950
	Table 119: Layer 3 VPN Service Order - Static Routes	952
	Table 120: Layer 3 VPN Service Order - MVPN and PIM Settings	953
	Table 121: Layer 3 VPN Service Order - Modify or alter UNI Interface	955
	Table 122: Layer 3 VPN Service Order - Configure Site Settings	957
	Table 123: Layer 3 VPN Service Order - Service Settings	966
	Table 124: Layer 3 VPN Service Order - PE-CE Settings	969
	Table 125: Layer 3 VPN Service Order - Topology Settings	971
	Table 126: Layer 3 VPN Service Order - Static Routes	973
	Table 127: Layer 3 VPN Service Order - MVPN and PIM Settings	974
	Table 128: Layer 3 VPN Service Order - Modify or alter UNI Interface	977
	Table 129: Layer 3 VPN Service Order - Configure Site Settings	978
Part 11	Service Provisioning: Working with Services Deployment	
Chapter 36	Service Provisioning: Managing Deployed Services	1003
	Table 130: Deployment Jobs Table Description	1004
	Table 131: Deploy Options Window	1013
	Table 132: Deploy Configuration Window	1013
Part 12	Auditing Services and Viewing Audit Results	
Chapter 37	Service Provisioning: Auditing Services	1067
	Table 133: Commands Available in the Troubleshoot Device Window	1080
	Table 134: Parameters in Connectivity Services Director Application Settings	1083
	Table 135: OP Scripts Contexts for Different Service Types	1089
	Table 136: Point-to-Multipoint Service Endpoint Icons	1103
	Table 137: Functional Audit Success Status Icons	1103
	Table 138: Multipoint-to-Multipoint Service Control Plane and Data Plane Validation Icons	1104
	Table 139: Command Status Icons	1105
Part 13	Working in Monitor Mode	
Chapter 39	About Monitor Mode	1133
	Table 140: Summary Tab Tasks	1137
	Table 141: Traffic Tab Tasks	1137
Chapter 40	Monitoring Traffic	1139

	Table 142: Port on Device table field descriptions	1140
	Table 143: Port Traffic Window	1141
	Table 144: Layer 3 VLAN Traffic Statistics Table	1143
	Table 145: Fields in the Show Routing Instances Window	1148
	Table 146: Show Interfaces Information	1149
	Table 147: Show Bridge Domains Information	1150
	Table 148: Show Connections Information	1151
	Table 149: Show Routing Table Field Descriptions	1154
	Table 150: Show MAC Table fields	1156
Chapter 41	Monitoring Devices	1159
	Table 151: Show ARP Table Information Window	1161
Chapter 42	General Monitoring	1163
	Table 152: Ping Host Advanced Search Criteria Field Descriptions	1164
	Table 153: Traceroute Advanced Options Field Descriptions	1166
Chapter 43	Monitor Reference	1167
	Table 154: Error Trend Details Table	1169
	Table 155: Error Trend Additional Details Table	1169
	Table 156: Equipment Status Summary Fields	1169
	Table 157: Equipment Summary By Type Detail View	1170
	Table 158: Port Status Details Table	1171
	Table 159: Status Monitor Fields	1172
	Table 160: User Session Details Table	1176
	Table 161: User Session Details Table	1178
	Table 162: Current Active Alarms Monitor	1179
	Table 163: Top Session Details Table	1181
	Table 164: Top APs by Sessions Window	1181
	Table 165: Radio Technology Type Statistics Summary Categories	1182
	Table 166: Radio Type Statistics Window	1183
	Table 167: Top Hosts Monitor Details	1184
	Table 168: Top Session Details Table	1185
	Table 169: Top APs by Traffic Details Window	1186
	Table 170: Top Talker-Wireless Devices Details Window	1187
	Table 171: Wireless Objects With Interference Tracking	1187
	Table 172: Information on RF Interference Sources for a Radio	1188
Chapter 44	Detecting and Examining the Health and Performance of Services	1191
	Table 173: Mapping Between Polled Values and Counter Values Displayed in the GUI	1194
	Table 174: Computation of Counters Using Polling Intervals	1194
	Table 175: Ping MPLS Tasks Summary and the Corresponding CLI show Commands	1248
	Table 176: Routing Table Window Field Descriptions	1257
Part 14	Working in Fault Mode	
Chapter 46	Using Fault Mode	1267
	Table 177: Connectivity Services Director Alarm Classifications	1268
	Table 178: Alarm Search Fields	1274

Chapter 47	Fault Reference	1277
	Table 179: Alarm Detail Fields	1278
	Table 180: Sort Options for Alarms	1279
	Table 181: Event Detail Fields	1279
	Table 182: Alarm Detail Fields	1281
	Table 183: Event Detail Fields	1283
	Table 184: Current Active Alarms Monitor	1284
	Table 185: Current Active Alarms Monitor	1288
Part 16	Working with Chassis View	
Chapter 49	Working with Devices	1335
	Table 186: Active Alarms Monitor	1339
	Table 187: Fields for Physical Interfaces in the Component Info Pane	1340
	Table 188: Pseudo Interfaces Columns	1341
	Table 189: Logical Interfaces Columns	1341
	Table 190: Fields in the Chassis View Details Page	1342
Chapter 50	Managing CLI Configlets	1349
	Table 191: Default Variables	1350
	Table 192: Parameters for a CLI Configlet	1352
	Table 193: Attributes of CLI Configlet Parameters	1353
	Table 194: Commands to View XML from the CLI	1355
	Table 195: Context Path and XML node referred for different element types	1356
	Table 196: XPath expressions for different elements	1356
	Table 197: CLI Configlets Contexts for Different Service Types	1359
	Table 198: Columns on the Manage CLI-Applied Configlets Page	1365
	Table 199: Attributes of a parameter	1366
	Table 200: Columns on the Manage CLI-Applied Configlets Page	1373
Part 17	Managing Optical Interfaces, OTUs, ODUs, ILAs, and IPLCs on MX Series and PTX Series Routers	
Chapter 51	Overview of Optical Interfaces, OTUs, and ODUs	1377
	Table 201: Example—Signal Degrade and Clear Threshold Values at 1 dBQ	1382
	Table 202: Example—Signal Degrade and Clear Thresholds After Configuration	1383
	Table 203: CLI Representation of PIC Slots	1387
	Table 204: OTU4 40I-9DIF (ITU-T 959.1) Optical Interface Specifications	1390
	Table 205: 100-Gigabit DWDM OTN PIC Optical Interface Specifications	1390
	Table 206: 100-Gigabit DWDM OTN Supported Wavelengths	1391
	Table 207: Software Features Supported	1395
	Table 208: 100-Gigabit DWDM OTN PIC LEDs	1397
	Table 209: Software Features Supported	1403
	Table 210: 100-Gigabit Ethernet OTN PIC with CFP2 LEDs	1404
	Table 211: Software Features Supported	1406
	Table 212: 100-Gigabit Ethernet PIC with CFP2 LEDs	1407
	Table 213: Software Features Supported	1409
	Table 214: 100-Gigabit Ethernet PIC with CFP LEDs	1412
	Table 215: Port Numbering Table	1416

	Table 216: Software Features Supported	1425
	Table 217: 100-Gigabit DWDM OTN PIC with CFP2 LEDs	1426
	Table 218: OTN Alarms and Defects	1431
	Table 219: OTN Alarms and Defects	1439
	Table 220: Wavelength-to-Frequency Conversion Matrix	1442
Chapter 52	Overview of Optical ILAs and IPLCs	1445
	Table 221: Optical ILA Hardware Components	1446
	Table 222: Optical ILA Chassis Status LEDs	1450
	Table 223: Required Actions Before Removing a FRU from the Optical ILA	1452
	Table 224: Optical ILA RJ-45 Management Port LEDs	1454
	Table 225: Optical ILA AC Power Supply LED	1458
	Table 226: Optical ILA DC Power Supply LED	1458
	Table 227: Supported Wavelength Allocation for the IPLC Base Module (PTX-IPLC-B-32)	1462
	Table 228: Supported Wavelength Allocation for the IPLC Expansion Module (PTX-IPLC-E-32)	1465
	Table 229: Default Port, Frequency, and Wavelength Mapping	1473
	Table 230: PTX3000 IPLC LED	1477
	Table 231: IPLC Optical Performance Monitors	1482
	Table 232: IPLC Threshold Crossing Alert Minimum and Maximum Values	1483
Chapter 53	Configuring and Monitoring Optical Interfaces, OTUs, and ODUs	1487
	Table 233: Active Alarms Monitor	1490
	Table 234: Fields for Physical Interfaces in the Component Info Pane	1490
	Table 235: Pseudo Interfaces Columns	1492
	Table 236: Logical Interfaces Columns	1492
	Table 237: Fields in the Chassis View Details Page	1493
	Table 238: Wavelength-to-Frequency Conversion Matrix	1503
	Table 239: Default Clear Threshold Values	1509
	Table 240: Default Signal Degrade Threshold Values	1510
	Table 241: Active Alarms Monitor	1560
Chapter 54	Configuring and Monitoring Optical Inline Amplifiers	1579
	Table 242: Active Alarms Monitor	1582
Chapter 55	Configuring and Monitoring Optical Integrated Photonic Line Cards	1605
	Table 243: Active Alarms Monitor	1608
	Table 244: Choose IPLC Dialog Box—Top Pane	1641
	Table 245: Choose IPLC Dialog Box—Bottom Pane	1642
	Table 246: IPLC Port, Frequency, and Wavelength Mapping	1645
	Table 247: Wavelength, Port, and IPLC Nodes Mapping	1671
Part 19	Working with Tunnel Services	
Chapter 57	Tunnel Services Overview	1693
	Table 248: One-to-One Backup Compared with Facility Backup	1715
Chapter 58	Service Design and Provisioning: Managing and Deploying Tunnel Services	1719
	Table 249: Fields in the Services Table	1749

	Table 250: Fields in the Services Table	1755
	Table 251: Deploy Options Window	1768
Chapter 59	Monitoring and Troubleshooting Tunnel Services	1781
	Table 252: Service Endpoint Icons	1790
	Table 253: Functional Audit Success Status Icons	1791
	Table 254: Control Plane and Data Plane Validation Icons	1791
	Table 255: Command Status Icons	1792
	Table 256: OP Scripts Contexts for RSVP LSP Services	1798
Part 20	Appendix: Managing Network Activate Features Using the Older Version of Services Activation Director	
Chapter 60	Service Design: Working with Point-to-Point, Layer 3 VPN, and VPLS Service Templates	1811
	Table 257: Data Types and Tabs	1818
	Table 258: Service Definition Types and Associated Service Variables	1826

About the Documentation

- [Documentation and Release Notes on page lv](#)
- [Documentation Conventions on page lv](#)
- [Documentation Feedback on page lvii](#)
- [Requesting Technical Support on page lviii](#)

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <https://www.juniper.net/documentation/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <https://www.juniper.net/books>.

Documentation Conventions

[Table 1 on page lvi](#) defines notice icons used in this guide.

Table 1: Notice Icons







Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page lvi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>

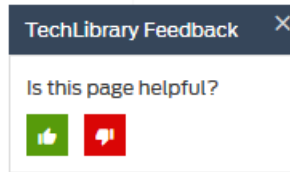
Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none">To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i>>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	<pre>[edit] routing-options { static { route default { nexthop <i>address</i>; retain; } } }</pre>
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none">In the Logical Interfaces box, select All Interfaces.To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>

- Join and participate in the Juniper Networks Community Forum:
<https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

PART 1

Overview

- [Working with Connectivity Services Director on page 3](#)
- [Service View Tasks and Lifecycle Modes on page 33](#)
- [Network Services Overview on page 49](#)

CHAPTER 1

Working with Connectivity Services Director

- [Connectivity Services Overview on page 3](#)
- [Understanding the Need for Connectivity Services Director for Managing Services on page 4](#)
- [Benefits of a Unified User Interface for Routing and Tunnel Services with Connectivity Services Director on page 6](#)
- [Connectivity Services Director Overview on page 8](#)
- [Understanding the Connectivity Services Director User Interface on page 10](#)
- [Understanding the Usage and Layout of Connectivity Services Director Views and Tasks on page 21](#)
- [Understanding the Management Lifecycle Modes in Connectivity Services Director on page 22](#)
- [Understanding Connectivity Services Director User Administration on page 24](#)
- [Logging In to Connectivity Services Director on page 25](#)
- [Accessing the Services Activation Director GUI on page 27](#)
- [Changing Your Password for Connectivity Services Director on page 28](#)
- [Logging Out of Connectivity Services Director on page 30](#)
- [Getting Started Assistant Overview in Services Activation Director on page 31](#)

Connectivity Services Overview

Connectivity services include the Layer 2 VPN and Layer 3 VPN services, quality-of-service (QoS) profile services, timing synchronization services, tunneling and label-switched path (LSP) services, and connectivity fault management (CFM) services.

With connectivity services, you can perform the following tasks in your deployment:

- Design, provision, and monitor Label Discovery Protocol (LDP) and Border Gateway Protocol (BGP) services, and VPN services, for the management of Layer 2 and Layer 3 protocols, on devices.
- Configure the Operation, Administration and Maintenance (OAM) functionality on all devices and monitor, detect, isolate, and troubleshoot networking faults. The supported

OAM features include link fault management (LFM), CFM, and real-time performance monitoring (RPM).

- Configure Precision Time Protocol (PTP) and synchronous Ethernet services, which are timing functionalities for devices.
- Design, provision, and deploy MPLS-dynamic, RSVP-signaled LSP, and static LSP services on devices.
- Configure QoS or class-of-service (CoS) capabilities for services on devices.

To enable you to design and provision connectivity services in your network, you can use Connectivity Services Director, which is a robust and highly-intuitive next-generation application that runs on the Junos Space Network Management Platform. This application also enables validation and monitoring of service performance, and management of timing and clock synchronization.

**Related
Documentation**

- [Understanding the Need for Connectivity Services Director for Managing Services on page 4](#)
- [Benefits of a Unified User Interface for Routing and Tunnel Services with Connectivity Services Director on page 6](#)
- [Connectivity Services Director Overview on page 8](#)
- [Understanding the Connectivity Services Director User Interface on page 10](#)
- [Understanding the Usage and Layout of Connectivity Services Director Views and Tasks on page 21](#)
- [Understanding the Management Lifecycle Modes in Connectivity Services Director on page 22](#)
- [Understanding Connectivity Services Director User Administration on page 24](#)
- [Logging In to Connectivity Services Director on page 25](#)
- [Logging Out of Connectivity Services Director on page 30](#)

Understanding the Need for Connectivity Services Director for Managing Services

An important aspect of any network management system is to monitor, control, and plan the network infrastructure that comprises a large number of devices and extensive configuration parameters in a streamlined, easy, and cohesive way. The bulk propagation of settings on large sets of devices without impacting the working efficiency and traffic-handling capacity of the network is a salient objective. With networks constantly increasing in size, heterogeneity, and complexity, effective management and planning for such network becomes more important.

The following network management capabilities are essential for effective management of services on devices:

- In IP networks, services are essentially a combination of Layer 2 Ethernet and Layer 3 (IP-based) VPNs deployed over pseudowires or LSPs. These services are complex to provision and manage. Furthermore, as networks evolve, many network operators have hybrid networks that offer both legacy TDM and next-generation IP-based services.

Network management systems must be able to manage such hybrid networks. Simplification of essential tools required to set up, configure, provision, and operate devices and the services that run on them are key to keeping operational costs down and achieving efficiency.

- Detection and resolution of faults are essential to maintaining high availability of deployed services and ensuring service performance to meet service-level agreements (SLAs). For instance, a delay in detecting loss of signal (LOS) or in responding to the delay with appropriate switchover mechanisms can result in loss of service and impact operator revenue.

A network management system must offer simple and efficient tools to detect service faults and performance so that service levels are assured. Such a system includes tools to correlate faults with the alarms and traps generated on devices, and provide a real-time view of the complete operational status of a network.

- In many cases, operators already own an OAM system or a third-party tool to manage the legacy network. Any new network management system needs to provide seamless support for legacy functions while enabling new features to support packet-based networks. This may require the use of standards-based open interfaces to enable such OAM systems to query, configure, provision, and manage the new devices and services being deployed.
- Networks contain devices from various vendors. An ideal network management system should present a unified device management interface for all devices from the access network to the core network. Multivendor, standards-based management is becoming increasingly important now, in the context of SDN and service automation. In the context of mobile backhaul, a unified network device management interface is essential to efficiently deploy a large number of devices such as cell site gateways.

Assuming that these devices are hosted in remote locations, it is essential to ensure that the device management interfaces (DMIs) provides the right level of automation to reduce the time required to set up and configure each device without requiring additional manual intervention at the site, after the device is deployed.

- Centralized configuration management, rapid deployment, polling, statistics capture, and reporting of services are some of the essential components of a good DMI. Management systems must be standards compliant and provide open interfaces for interoperability with existing systems in an operator's network.

Standards-based northbound interfaces that use REST APIs are becoming the norm for such interoperability. Mobile backhaul networks typically contain tens of thousands of cell sites connected to aggregation devices and further, into the core network.

- Network management systems must be able to cope with such scale and offer efficient, user-friendly mechanisms to provision services in bulk. For example, reduction in the number of steps required to provision a pseudowire from end to end greatly improves the efficiency of a network provisioner, while also reducing the number of provisioning errors.

The aforementioned key objectives are achieved using the Connectivity Services Director application. You can configure your network topology in an optimal and effective manner using Connectivity Services Director for administration, provisioning, and monitoring of routing devices.



NOTE: In Connectivity Services Director Release 2.0, point-to-point Ethernet services, VPN services, VPLS services, and RSVP LSP services are supported. All other than these service types can be configured using the Services Activation Director GUI, which is installed with the Connectivity Services Director software image.

**Related
Documentation**

- [Connectivity Services Overview on page 3](#)
- [Benefits of a Unified User Interface for Routing and Tunnel Services with Connectivity Services Director on page 6](#)
- [Connectivity Services Director Overview on page 8](#)
- [Understanding the Connectivity Services Director User Interface on page 10](#)
- [Understanding the Usage and Layout of Connectivity Services Director Views and Tasks on page 21](#)
- [Understanding the Management Lifecycle Modes in Connectivity Services Director on page 22](#)
- [Understanding Connectivity Services Director User Administration on page 24](#)
- [Getting Started Assistant Overview in Services Activation Director on page 31](#)
- [Logging In to Connectivity Services Director on page 25](#)
- [Logging Out of Connectivity Services Director on page 30](#)

Benefits of a Unified User Interface for Routing and Tunnel Services with Connectivity Services Director

Junos Space Connectivity Services Director is a compact and optimal application for configuring, deploying, and monitoring Layer 2 and Layer 3 services has been available for purchase and installation as separate software packages, running over a compatible release of Junos Space Network Management Platform.

The following are the salient benefits and capabilities of the Connectivity Services Director application:

- Because the Connectivity Services Director GUI uses a cohesive and effective lifecycle management mode of presentation and organization in the banner, the activities that you can perform through various stages and phases of your device and service deployment are easily manageable, optimally administered, and seamlessly handled.
- A consistent, uniform, consolidated, and streamlined user interface and elegant experience is introduced by using the Service View component in the Connectivity Services Director GUI for defining services.
- You can install this application to leverage Layer 2, Layer 3, label-switched path (LSP), and class of service (CoS) functionalities on devices in your network (previously available by installing different applications, such as Network Activate, Transport Activate, Sync Design, or OAM Insight), based on your deployment needs and device models to be managed, on a Junos Space JA2500 Appliance or a Junos Space Virtual Appliance that satisfied the hardware requirements.
- Instead of a different look-and-feel and framework between Network Director and Services Activation Director, a consistent and intuitive next-generation user interface is designed. You do not need to familiarize and adapt yourself to the layout and the design of Services Activation Director by using the Service View from within Connectivity Services Director. If you have already deployed Services Activation Director in your environment, you can derive the advantages and salient functionalities of Service View by migrating to this application.
- If you are deploying the network management utility in your topology for the first time for routing and tunnel services provisioning, and if you have previously deployed Network Director for the administration of devices, such as EX Series switches and QFX Series switches, you can seamlessly install the Connectivity Services Director application or software package on different appliances to perform Layer 2 through Layer 3 services management on several platforms, such as ACX Series routers, M Series routers, MX Series routers, PTX Series routers, and TCA Series Timing Appliances.



NOTE: Network Director cannot be installed on the same system as Connectivity Services Director.

Related Documentation

- [Connectivity Services Overview on page 3](#)
- [Connectivity Services Director Overview on page 8](#)
- [Understanding the Connectivity Services Director User Interface on page 10](#)
- [Understanding the Usage and Layout of Connectivity Services Director Views and Tasks on page 21](#)
- [Understanding the Management Lifecycle Modes in Connectivity Services Director on page 22](#)
- [Understanding Connectivity Services Director User Administration on page 24](#)
- [Logging In to Connectivity Services Director on page 25](#)
- [Logging Out of Connectivity Services Director on page 30](#)

Connectivity Services Director Overview

Service providers and enterprises must be able to rapidly provision and offer new MPLS and Carrier Ethernet services across their networks. In order to reduce operational costs and enable quick service rollouts, network operators need an intelligent provisioning application that facilitates the design, deployment, and management of services. Junos Space Connectivity Services Director facilitates lifecycle management of connectivity services such as point-to-point, VPLS, L2VPN, L3VPN, and RSVP LSP services, QoS profile configuration, service performance validation and monitoring, and synchronization management. In addition to an intuitive graphical user interface, the application also supports a rich set of API functions to enable northbound interface integration and service orchestration with other operations support systems (OSS) platforms.

Telecommunication establishments and organizations worldwide that offer MPLS and carrier Ethernet services face common business challenges such as controlling capital and operating expenses, accelerating time to market and increasing customer satisfaction. At the same time, these companies also have to deal with the following technical challenges:

- Provisioning a customer service rapidly and accurately
- Scaling to keep up with customer demand
- Tracking site-specific quality of service (QoS)
- Troubleshooting and pinpointing problems in the network
- Finding trained personnel with expertise in networking and MPLS technologies

Junos Space Connectivity Services Director allows service providers and enterprises to rapidly enable new service offerings. It facilitates an automated and streamlined approach to the service design and provisioning process and helps reduce fallout from misconfigured customer services, thereby increasing customer satisfaction and retention. Besides automating key provisioning tasks, Junos Space Connectivity Services Director also provides a complete network management solution, including automated service discovery, MPLS resource management, point-and-click service provisioning, validation, and troubleshooting for MPLS and carrier Ethernet service environments.

Junos Space Connectivity Services Director is a Junos Space application for unified management of the ACX Series routers, M Series routers, MX Series routers, PTX Series routers, and TCA Series Timing Appliances in your network.

The Junos Space Connectivity Services Director essentially manages the lifecycle of Layer 2 and Layer 3 services comprising resource pool management, service design and provisioning, troubleshooting and performance monitoring, and service decommissioning. The following are the broad, salient capabilities and advantages of the product:

- Automating the design of Layer 2 and Layer 3 VPN services, activating the services, provisioning the services, and validating the Layer 2 and Layer 3 VPN services across MPLS and Carrier Ethernet networks, enabling service providers to efficiently and cost-effectively manage deployments while reducing fallout from misconfigured services.
- Designing, provisioning, and activating RSVP-signaled label-switched paths (LSPs), as well as static LSPs, which can be configured as end-to-end, point-to-point, point-to-multipoint, or full-mesh LSPs.
- Monitoring faults and performance of VPN services using standards-based protocols and technologies such as Ethernet connectivity fault management (CFM), Ethernet link-level fault detection and management, and Bidirectional Forward Detection (BFD).
- Configuring and applying class-of-service (CoS) profiles to interfaces of devices.
- Provisioning synchronization interfaces such as IEEE1588-2008 (PTP) and Synchronous Ethernet.

The Junos Space Network Management Platform and Junos Space Connectivity Services Director are accessible through a northbound Representational State Transfer (REST)-based API. This enables network providers to tap into the rich functionality of Junos Space and build native applications on their operations support systems (OSS) and business support systems (BSS) as they begin to embrace SDN architectures in their networks.

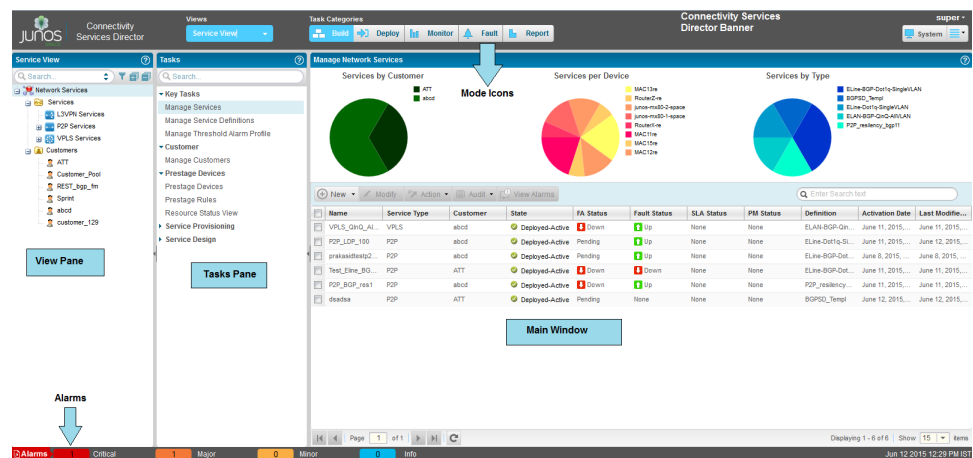
**Related
Documentation**

- [Connectivity Services Overview on page 3](#)
- [Benefits of a Unified User Interface for Routing and Tunnel Services with Connectivity Services Director on page 6](#)
- [Understanding the Connectivity Services Director User Interface on page 10](#)
- [Understanding the Usage and Layout of Connectivity Services Director Views and Tasks on page 21](#)
- [Understanding the Management Lifecycle Modes in Connectivity Services Director on page 22](#)
- [Understanding Connectivity Services Director User Administration on page 24](#)
- [Logging In to Connectivity Services Director on page 25](#)
- [Logging Out of Connectivity Services Director on page 30](#)

Understanding the Connectivity Services Director User Interface

Junos Space Connectivity Services Director provides a simple-to-use, HTML5-based, Web 2.0 user interface that you can access through standard Web browsers. The user interface uses task-based workflows to help you accomplish administrative tasks quickly and efficiently. It provides you with the flexibility to work with single or multiple devices grouped by logical relationship, location, or device type. You can filter, sort, and select columns in tables, making looking for specific information easy.

Figure 1 on page 10 illustrates the main components of the interface.



This topic describes:

- [Connectivity Services Director Banner on page 10](#)
- [View Pane on page 12](#)
- [Tasks Pane on page 15](#)
- [Alarms on page 16](#)
- [Main Window or Workspace on page 16](#)
- [Tables in Connectivity Services Director on page 16](#)

Connectivity Services Director Banner

Use the Connectivity Services Director banner, shown in [Figure 2 on page 11](#), to select the working mode. You can also use the Connectivity Services Director banner to perform other global tasks, such as setting up your preferences or accessing Junos Space.

[Table 3 on page 11](#) describes the functions available to you on the banner.

Figure 2: Connectivity Services Director Banner

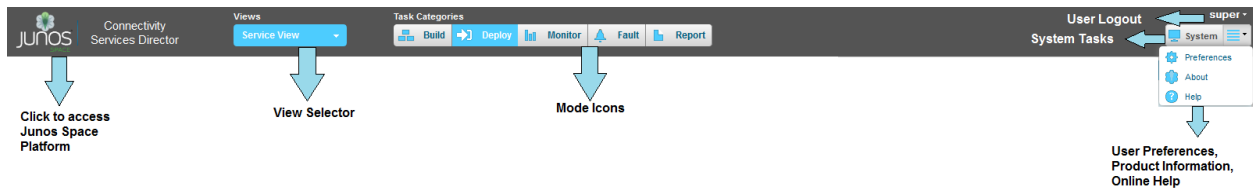



Table 3: Connectivity Services Director Banner Functions

Item	Function
Accessing Junos Space Platform	Click to exit Connectivity Services Director and open the Junos Space Network Application Platform. You can switch back and forth between Connectivity Services Director and Junos Space without logging in again.
Network View Selector	<p>Select the network view that you want to work in. You can choose from one of the following views:</p> <ul style="list-style-type: none"> • Dashboard View • Service View • Device View • Custom Group View • Topology View
Mode Icons	<p>Select the mode you want to work in.</p> <p>NOTE: You might not have access to all the Connectivity Services Director modes. What modes you have access to depends on your assigned user role.</p>
User Log out	<p>Displays the username using which you logged in to Connectivity Services Director.</p> <p>Click the down arrow next to the username and select Logout to log out of Connectivity Services Director and Junos Space. You can also click the down arrow next to the username and select the scope of the view, such as global, to view information pertaining to the entire network.</p>
System Tasks	<p>Access the system tasks such as viewing audit logs and jobs and collecting troubleshooting logs.</p> <p>Click the down arrow next to System on the Connectivity Services Director banner and select Preferences to set your Connectivity Services Director user and system preferences.</p>

Table 3: Connectivity Services Director Banner Functions (continued)

Item	Function
System Preferences, Product Information, and Online Help 	Click this button and select an appropriate option: <ul style="list-style-type: none"> • Preferences—Enables you to set your Connectivity Services Director user and system preferences. • Help—Enables you to open searchable Help. This Help icon is not context-sensitive—it always opens Help to the first page. From here, you can browse or search Help. Context-sensitive Help is available from the Help icon provided on each pane or page. • About—Displays information about Connectivity Services Director, such as the currently running version.

View Pane

On the View pane, Connectivity Services Director provides you with a unified, hierarchal view of your networks in the form of a tree that is expandable and collapsible. By selecting both a view and a node from the tree, you indicate the *scope* over which you want an operation or task to occur. For example:

- By selecting the MX240 node in Device View, you indicate that the scope for a task is all MX240 routers in your network.

You can perform the following actions on the View pane:

- [Displaying Devices Using Various Network Views on page 12](#)
- [Filtering the Network Tree on page 13](#)
- [Expanding or Collapsing Nodes in the Network Tree on page 14](#)
- [Searching the Network Tree on page 15](#)

Displaying Devices Using Various Network Views

Use the selection box on the Connectivity Services Director banner to choose one of the following network views:

- Dashboard View—This is a customizable view that provides information about your network. You can select and add monitoring widgets to the Dashboard View based on your requirements. This is the default view that opens when you log in to Connectivity Services Director.
- Device View—Devices are organized by device type: routers. Within each device type, devices are organized by device model. For example, all models of MX240 routers are grouped together under one node in the tree.
- Custom Group View—If you have defined one or more custom groups, Connectivity Services Director displays these custom groups in this view. You can manually add devices to a custom group or define a rule to automatically add devices to the custom group after they are discovered in Connectivity Services Director. The devices are grouped under each custom group.

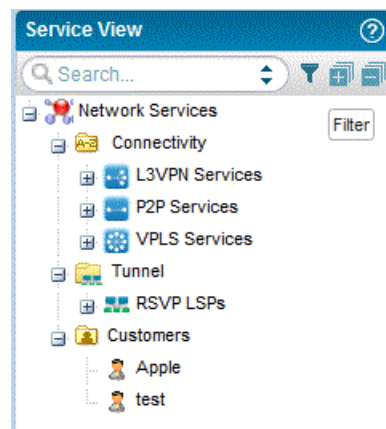
- **Topology View**—This view enables you to view a graphical representation of the discovered devices in your network, organized by groups or zones. The topology map window displays important link and node properties. Links are color coded according to utilization. You can also view physical and logical connectivity between various discovered interconnected devices.
- **Service View**—You can create services, policies, and filters for devices that are managed by Connectivity Services Director. The service templates and attributes for services, policies, and filters help you classify and control the manner in which packets must be handled by the various services.
- **Chassis View** (accessible from the View Physical Inventory page of Device View)—You can view a high-level, graphical representation or an image of the chassis. It indicates the state of the interfaces. If the administrative and operational statuses of the interface are up, the interface is displayed in green. If the administrative status is down, the interface is displayed in grey. If the administrative status is up and operational status is down, the interface is displayed in red. The image is a replica of the device chassis. If you are connected to a virtual chassis, the image includes all the member routers of the virtual chassis. The chassis view also displays a count of alarms generated in the system; major alarms are displayed in red, and minor alarms in orange. The purpose of the view is to try and provide a comprehensive view of the health and status of the deployed devices across the network.

Filtering the Network Tree

To make it easier for you to focus on selected aspects of your network, you can apply predefined filters to your network tree so that only nodes and devices that meet the filter criteria are shown. For example, you can apply a filter so that only devices in a specific building are shown in the network tree in all views.

To apply filters:

1. From the View pane, click the filter icon:



The Filters dialog box is displayed.

2. In the Filters dialog box, click **Show available filters**.

The Available Filters section of the dialog box appears.

- Under Available Filters, click the tab for the view you want to use to define your filter. For example, if you want to filter on devices—that is, show only certain types of devices—click the **Device** tab.

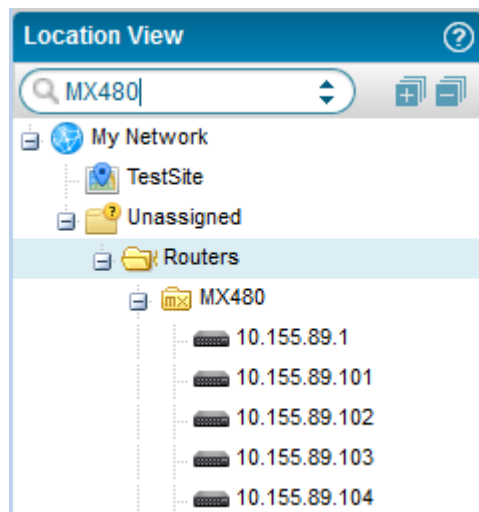
The filters that you can apply are listed below the Device tab.

- To select a filter, click its associated plus icon.

The filter appears on the Selected Filters section of the dialog box. You can repeat steps 3 and 4 until you have selected all the filters you want to apply.

- Click **Apply**.

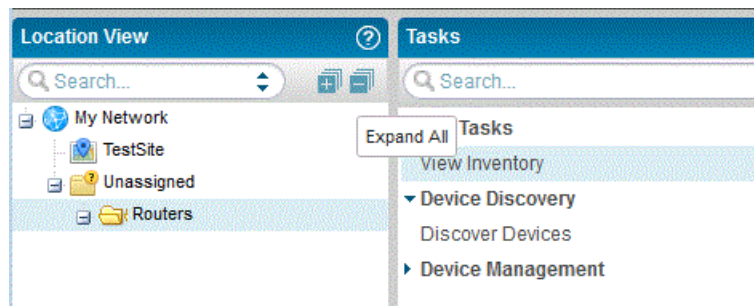
The Filters dialog box closes and the filters are applied. The filter icon changes appearance to indicate that filters have been applied:



To remove a filter, click the filter icon, click the trash can next to the filter on the Selected Filters list, and click **Apply**.

Expanding or Collapsing Nodes in the Network Tree

To expand a node in the network tree, select the node and then click the **Expand All** icon:



The node you selected and any child nodes under the selected node are expanded to show their contents.

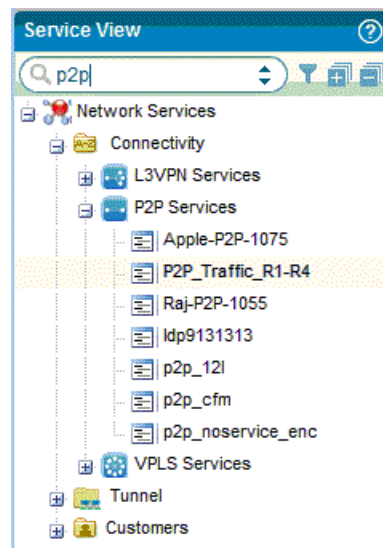
Similarly, to collapse a node in the network tree, select the node and then click the **Collapse All** icon (next to the Expand All icon). The node you selected is collapsed and no nodes under it are shown.

Searching the Network Tree

To quickly find and select a device or device group, use the search function.

To perform a search, type three or more characters in the Search box and click the **Search** icon, as shown in [Figure 3 on page 15](#).

Figure 3: Performing Search on the View Pane



Connectivity Services Director finds the first instance of a node whose name contains the characters. To find the next instance, click the right arrow.

Searches are not case-sensitive: a search on *wla115* and one on *WLA115* return the same results. You can also use wildcard characters in search strings.

Tasks Pane

The Tasks pane is available in every mode and lists tasks specific to that mode. In addition to changing according to the mode selected, tasks listed in the Tasks pane can change. For example, some tasks are appropriate only at the device level and thus appear only when you have selected an individual device. Clicking a task brings up task-specific content in the main window. In general, to perform a task in Connectivity Services Director, you navigate to the task.

Alarms

The Alarms bar that is displayed at the bottom of your browser window provides a quick summary of how many critical, major, minor, and informational alarms are currently active in the network and is visible in every mode.

To display more information about alarms, click the alarm count or the Alarms bar. You are automatically placed in Fault mode and the Fault mode monitors are displayed.

Main Window or Workspace

The main window or workspace displays content relevant to the mode, scope, and task you have selected. When you log in to Connectivity Services Director, the main window displays the dashboard. The dashboard enables you to allow the users that are assigned roles as operators to quickly monitor health and status of the managed devices. The sections or frames on the dashboard allows the operator to understand the device problem or fault at the macro level (comprehensive and widespread network health and status) and the micro level (individual device health and status). The health representation of the devices can be customized based on the monitoring properties defined.

Tables in Connectivity Services Director

Tables are used throughout Connectivity Services Director to display data. These tables share common features. By becoming familiar with these features, you can navigate and manipulate tabular data quickly and efficiently.

The following sections describe:

- Moving and resizing columns
- Navigating pages
- Displaying the column drop-down menu
- Sorting on a column
- Hiding and exposing columns
- Searching table contents
- Filtering table contents

Moving and Resizing Columns

You can reposition and resize columns in a table. To move a column, drag the column head to the new location. Connectivity Services Director displays a green check mark when you mouse over a valid column location. To resize a column, mouse over the edge of a column until the cursor becomes two vertical lines with outward arrows. Drag the column width to the new size.

Navigating Pages

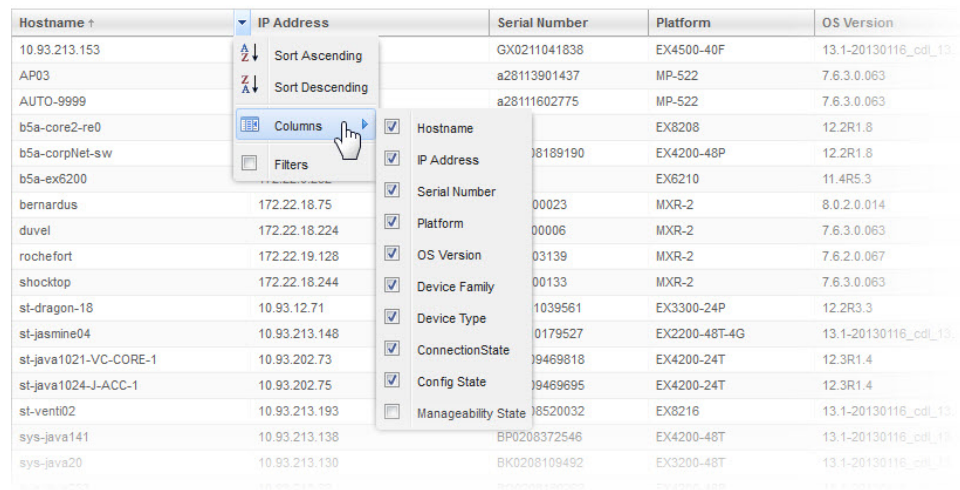
Paging controls at the bottom of an applicable page allow you to navigate the entries on the pages when the inventory is too large to fit on one page. Using these controls, you

can go to a specific page, navigate to the next or previous page, navigate to the first or last page of the inventory, or refresh the inventory view.

Displaying the Column Drop-Down Menu

A drop-down menu is available from each column head, allowing you to perform additional operations on columns. To display the column drop-down menu, mouse over the column head. A down arrow appears. By clicking the arrow, you display the drop-down menu, as shown in [Figure 4 on page 17](#).

Figure 4: Column Drop-Down Menu



Hostname	IP Address	Serial Number	Platform	OS Version
10.93.213.153		GX0211041838	EX4500-40F	13.1-20130116_cdl_13
AP03		a28113901437	MP-522	7.6.3.0.063
AUTO-9999		a28111602775	MP-522	7.6.3.0.063
b5a-core2-re0			EX8208	12.2R1.8
b5a-corpNet-sw		8189190	EX4200-48P	12.2R1.8
b5a-ex6200			EX6210	11.4R5.3
bernardus	172.22.18.75			
duvel	172.22.18.224			
rochefort	172.22.19.128			
shocktop	172.22.18.244			
st-dragon-18	10.93.12.71			
st-jasmine04	10.93.213.148			
st-java1021-VC-CORE-1	10.93.202.73			
st-java1024-J-ACC-1	10.93.202.75			
st-venti02	10.93.213.193			
sys-java141	10.93.213.138			
sys-java20	10.93.213.130			

Sorting on a Column

You can sort the table on a column by clicking the column head—each click changes the direction of the sort. In addition, you can use the Sort Ascending and Sort Descending options on the drop-down menu.

When you sort on a column, a small arrow appears next to the column name to indicate that the table is being sorted by the column and the direction of the sort.

Connectivity Services Director uses a lexical sort for tabular data that is not strict numeric data, which means that data such as IP addresses do not sort in numerical sequence, as shown in [Table 4 on page 18](#).

Table 4: Numerical Sorts and Lexical Sorts

Numerical Sort	Lexical Sort
10.93.200.65	10.93.200.129
10.93.200.129	10.93.200.199
10.93.200.199	10.93.200.65

Hiding and Exposing Columns

You can customize your tables by hiding or exposing columns. This way, you can choose to see only relevant information.

To hide or expose columns, display the drop-down menu for any column head and mouse over the Columns option, as shown in [Figure 4 on page 17](#). Select the check box beside a column in the drop-down menu to expose it. Clear the check box beside a column to hide it.

As a general rule, Connectivity Services Director displays all columns in a table by default. However, some tables have more columns than can fit easily within the page. In these tables, some columns are hidden by default.

Searching Table Contents

You can search for specific data in large tables by using search criteria.

To search for an item in a table, enter the search term in the text box. Select ANY for Connectivity Services Director to search for the term in all columns in the table. Every table has a predefined default column that the system searches; before it proceeds to search other columns.

You can also choose to search a particular column for a term. Connectivity Services Director displays a list of all the columns in a table. To search a particular column for a term, select that column for the list.



NOTE: When you enter a search expression, note the following:

- You must add a back slash “\” if you want to use the following special characters in the search text:

+ ~ & & || ! () { } [] ^ “ ~ * ? : \

- Field names are case-sensitive.

For example, if you have a few systems running on Junos OS 12.3 Release 4.5, then `os: 12.3R4.5` returns search results, whereas `OS: 12.3R4.5` does not return search results. This is because the field name that is indexed is `os` and not `OS`.

- If you want to search for a term that includes a space, enclose the term within double quotation marks.

For example, to search for all devices that are synchronized (that is, In Sync), enter “In Sync” in the Search field.

- You must append “*” if you want to search using partial keywords. Otherwise, the search returns 0 (zero) matches or hits.

You can filter search results by specifying one or more search terms. Connectivity Services Director uses the AND operator for each search term that you enter. Connectivity Services Director lists the search results in the table, depending on the search criteria that you specified.

For example, perform the following steps to search for an MX480 router that is running Junos OS Release 14.1:

1. Enter **MX480** as the search term in the text box.

The device model is saved as a search term.

2. From the list that appears, select to search the Platform column.

Connectivity Services Director lists all the MX480 routers in your network.

3. Enter **14.1** as the search term after the comma separator in the text box.

The Junos OS release is saved as a search team.

4. From the list, select to search from the OS Version column.

Connectivity Services Director lists all the MX480 routers in your network that are running Junos OS Release 14.1.

Filtering Table Contents

For large tables, it is helpful to be able to sort data to show only relevant entries. When you mouse over the Filters option on the column drop-down menu, a fill-in box appears where you can type filter criteria. If you type a text string and click **Go**, entries that do not contain the text string (filter criterion) are removed from the table. A red asterisk appears on the column head to indicate that the column has been filtered. To restore all entries to the table, clear the Filters option.

For example, to filter the Device Inventory page so that only devices in the **192.168.1.0** subnet are displayed:

1. Mouse over the right side of the IP Address column head to expose the down arrow.
2. Click the arrow to display the column drop-down menu.
3. Mouse over **Filters** to display the Filter field.
4. Type **192.168.1.** in the field and click **Go**.

Only the devices in the **192.168.1.0** subnet are shown.

Related Documentation

- [Connectivity Services Overview on page 3](#)
- [Benefits of a Unified User Interface for Routing and Tunnel Services with Connectivity Services Director on page 6](#)
- [Connectivity Services Director Overview on page 8](#)
- [Understanding the Usage and Layout of Connectivity Services Director Views and Tasks on page 21](#)
- [Understanding the Management Lifecycle Modes in Connectivity Services Director on page 22](#)
- [Understanding Connectivity Services Director User Administration on page 24](#)
- [Logging In to Connectivity Services Director on page 25](#)
- [Logging Out of Connectivity Services Director on page 30](#)

Understanding the Usage and Layout of Connectivity Services Director Views and Tasks

The Connectivity Services Director user interface is based on the network management lifecycle. The interface provides five main working modes that are aligned to the network management lifecycle, and a sixth mode for working with Connectivity Services Director itself. On the View pane, Connectivity Services Director provides you a unified, hierarchical view of your networks in the form of a tree that is expandable and collapsible. You can select the Service View option from the View drop-down list to display the workspaces and settings that you can define for network services and tunnel services.

The lifecycle mode icons are displayed on the banner to guide you through the different phases of configuration and monitoring that you can perform with Service View. Network services-related pages or GUI pages are used for Layer 2 and Layer 3 service provisioning.

The Tasks pane is available in every mode and lists tasks specific to that mode. In addition to changing according to the mode selected, tasks listed on the Tasks pane can change as you select Service View on the View pane instead of another view. Clicking a task brings up task-specific content in the main window.

The System Tasks pane provides tasks for viewing audit logs of Connectivity Services Director user activities, for managing jobs, and for collecting troubleshooting logs.

See [“Understanding the Connectivity Services Director User Interface” on page 10](#) for an illustration of the main components of the Connectivity Services Director GUI.

Related Documentation

- [Connectivity Services Overview on page 3](#)
- [Benefits of a Unified User Interface for Routing and Tunnel Services with Connectivity Services Director on page 6](#)
- [Connectivity Services Director Overview on page 8](#)
- [Understanding the Connectivity Services Director User Interface on page 10](#)
- [Understanding the Management Lifecycle Modes in Connectivity Services Director on page 22](#)
- [Understanding Connectivity Services Director User Administration on page 24](#)
- [Logging In to Connectivity Services Director on page 25](#)
- [Logging Out of Connectivity Services Director on page 30](#)

Understanding the Management Lifecycle Modes in Connectivity Services Director

Connectivity Services Director enables automated design and provisioning of VPN services, such as point-to-point services, virtual private LAN (VPLS), and Layer 3 VPN services, label-switched path (LSP) services, such as MPLS, RSVP, and static LSP services, configuration of QoS profiles, validation and monitoring of service performance and management of synchronization.

By providing full network lifecycle management, Connectivity Services Director simplifies the discovery, configuration, visualization, monitoring, and administration of large networks. Operators can quickly deploy a network by using Connectivity Services Director, configure it optimally to improve network uptime and maximize resources, and respond agilely to the needs of applications and users.

The Connectivity Services Director user interface is based on the network management lifecycle. The interface provides five main working modes that are aligned to the network management lifecycle, and a sixth mode for working with Connectivity Services Director itself. Each mode provides access to different tasks:

- **Build mode**—You use Build mode to discover the devices in your network, to create and manage device configurations, and to manage devices. You can also organize your devices into hierarchical groups based on logical relationships or physical locations. To support flexible, large-scale deployment of devices, Build mode enables you to apply configurations across multiple devices grouped by logical relationships, physical locations, or type.

In Build mode, you can create services for devices that are managed by Connectivity Services Director. You can define service templates and attributes of different services, and also specify policies and filters to classify and control the manner in which packets are handled by the various services. You can define point-to-point services to provide transport and encapsulation of Layer 2 Ethernet circuits between two endpoints. You can also configure virtual private LAN service (VPLS), which in turn provides multipoint-to-multipoint services and point-to-multipoint services, and Layer 3 virtual private network (VPN) functionality, which supports full-mesh and hub-and-spoke services. The service designer is responsible for creating the service definitions that the service provisioner uses as the basis for creating a service order.

- **Deploy mode**—The Deploy mode enables you to deploy service order configuration changes to devices. When you make configuration changes in Build mode, the changes are not deployed to devices automatically. You must manually deploy the changes to devices in Deploy mode. Every time you make configuration changes in Build mode that affect a service, you must propagate the service order changes to the device by commissioning the configuration to the device. Configuration changes are deployed to devices at the device level. When you deploy configuration changes to a device, all pending configuration changes for that device are deployed. You can do the following configuration deployment tasks on devices that have pending changes:
 - Run configuration deployment jobs immediately or schedule them for later.
 - Preview pending configuration changes before deploying the service settings to devices.

- Validate that the pending changes are compatible with the device configuration.
- Manage configuration deployment jobs.
- **Monitor mode**—In a network environment, it is essential and important for a network administrator or a supervisor to quickly, easily assess the device performance and operating efficiency to be able to take corrective action and restoration measures for any device alarms, overloaded conditions, or traffic drops observed. Monitor mode in Connectivity Services Director enables you to view your network status and performance. The Connectivity Services Director application monitors its managed services on devices and maintains the information it collects from the devices in a database. Monitor mode displays this information in easy-to-understand graphs and in tables that you can sort and filter, allowing you to quickly visualize the state of your network, spot trends developing over time, and find important details. The main purpose of monitoring functionalities is to allow the operators to quickly monitor the health (working condition), operating efficiency, traffic-handling capacity, and performance status of the managed devices and configured services.
- **Fault mode**—Fault mode in Connectivity Services Director enables you to view your network health and welfare. Connectivity Services Director monitors its managed devices and maintains the information it collects from the devices in a database. Fault mode displays the alarms in easy-to-understand graphs and in tables that you can sort and filter, enabling you to resolve the system conditions that generated the alarms. When certain types of events are persistent, or when the condition causing the event crosses a threshold, SNMP sends a notification (also called a trap) to Connectivity Services Director. Connectivity Services Director correlates traps, describing a condition, into an alarm. To assist in diagnosing network problems and the operating efficiency of devices, the Fault mode shows you information about the health of your network and changing conditions of your equipment.



NOTE: Although the Report Mode icon is displayed in the Connectivity Services Director banner, for Release 2.0, no functionalities are available under this mode.

- **Dashboard**—This view enables you to allow the operators to quickly monitor health and status of the managed devices using the Dashboard view, which is a view that can be customized and provides information about your network. It is the default view that opens when you log in. You can select monitoring widgets to display on the Dashboard that show various information about the network. The health representation of the devices can be customized based on the monitoring properties defined.

In addition to these modes, Connectivity Services Director enables you to specify customized viewing patterns from the Preferences button under the System menu on the Connectivity Services Director banner. Depending on your system authority, Preferences page can display either user settings or a combination of user settings and system settings. You can specify preferences for features such as whether monitors and reports need to display local time or server time, the options for search indexing, and the polling interval for data collection.

Related Documentation

- [Connectivity Services Overview on page 3](#)
- [Benefits of a Unified User Interface for Routing and Tunnel Services with Connectivity Services Director on page 6](#)
- [Connectivity Services Director Overview on page 8](#)
- [Understanding the Connectivity Services Director User Interface on page 10](#)
- [Understanding the Usage and Layout of Connectivity Services Director Views and Tasks on page 21](#)
- [Understanding Connectivity Services Director User Administration on page 24](#)
- [Logging In to Connectivity Services Director on page 25](#)
- [Logging Out of Connectivity Services Director on page 30](#)

Understanding Connectivity Services Director User Administration

Connectivity Services Director uses the user administration features of the Junos Space platform on which it runs. Using these features, you can add, delete, and edit user accounts and roles and changing user passwords. Refer to the *Junos Space Network Application Platform User Guide* for more information about user administration.

When Connectivity Services Director is installed, some additional user administration options are available in Junos Space, which are specific to Connectivity Services Director:

In addition to the Super Administrator role, the following predefined roles are available to Connectivity Services Director users:

- The Device Manager role allows an administrator to discover devices.
- The Service Manager role allows an administrator to perform device pre-staging actions including discovering and assigning device roles.
- The Service Designer roles allows an administrator to create and publish a service definition.
- The Service Activator (less privileged) role allows an administrator to perform provisioning tasks including creating and managing customers, service orders, and services.

You can also create custom roles to grant users different access rights to the Connectivity Services Director modes. Connectivity Services Director modes—Deploy, Monitor, Fault, and Build—are available to assign to custom user roles in the list of application workspaces and associated tasks.



NOTE: The tasks listed under the Connectivity Services Director modes are disabled. Access is controlled at the mode level, so if you grant a role access to a mode, the role has access to all tasks in that mode, regardless of which tasks you select.



NOTE: For the Service Manager, Service Designer, and Service Activator user roles in Services Activation Director, the roles are migrated with additional access privileges to enable access to the different lifecycle modes of Connectivity Services Director after upgrading to Connectivity Services Director, Release 2.0.

If you try to log in to Connectivity Services Director by using an account that does not have access rights to any Connectivity Services Director modes, you are redirected to Junos Space instead.



NOTE: Access to Connectivity Services Director system preferences is controlled by user access rights. For more information, see [“Setting Up User and System Preferences” on page 122](#).

Related Documentation

- [Connectivity Services Overview on page 3](#)
- [Benefits of a Unified User Interface for Routing and Tunnel Services with Connectivity Services Director on page 6](#)
- [Connectivity Services Director Overview on page 8](#)
- [Understanding the Connectivity Services Director User Interface on page 10](#)
- [Understanding the Usage and Layout of Connectivity Services Director Views and Tasks on page 21](#)
- [Understanding the Management Lifecycle Modes in Connectivity Services Director on page 22](#)
- [Logging In to Connectivity Services Director on page 25](#)
- [Logging Out of Connectivity Services Director on page 30](#)

Logging In to Connectivity Services Director

You connect to Connectivity Services Director using your Web browser. The following Web browsers are supported: Internet Explorer 9.0 and 10.0, Mozilla Firefox version 3.6 and later, and Google Chrome version 17 and later. The minimum screen resolution is 1280 x 1024.

To log in to Connectivity Services Director directly:

1. In the Address field of your browser, enter the following URL:

```
https://<n.n.n.n>/csd/
```

where *n.n.n.n* is the IP address of the Junos Space Web interface. You can bookmark the login page for future use.

2. Enter the login credentials, such as the username and password.

The default username and password are the same for both Junos Space and Connectivity Services Director:

- Username—super
- Password—juniper123

After successful login, the Dashboard page of Connectivity Services Director is displayed.

To log in to Connectivity Services Director through Junos Space:

1. In the Address field of your Web browser, enter the following URL:

```
https://<n.n.n.n>/mainui
```

where *n.n.n.n* is the IP address of the Junos Space Web interface.

The Junos Space login page is displayed.

2. In the **Username** text box, enter your username.

For information about how to change your username, consult your system administrator.

3. In the **Password** text box, enter your password.

The default username and password are the same for both Junos Space and Connectivity Services Director:

- Username—super
- Password—juniper123

For information about how to change your password, see [“Changing Your Password for Connectivity Services Director” on page 28](#).

4. (Optional) If the remote authentication server is configured for Challenge/Response, you are presented with the challenge questions. Provide valid responses to the challenge questions you are asked, to log in successfully.

5. Click **Log In**.

The Junos Space home page appears. If the home page is not set, the Junos Space Dashboard page is displayed.

If the home page is inaccessible due to role or domain restrictions, a warning message is displayed and the Junos Space Dashboard page is loaded.



NOTE: If you are a user with access to more than one domain, then an informational message about switching domains is displayed in a dialog box.

Do one of the following:

- To prevent the informational message from appearing again, ensure that the **Don't show again** check box is selected and click OK. The **Don't show again** check box is selected by default.
- To allow the informational message to continue appearing, clear the **Don't show again** check box and click OK.

You can then switch to the Connectivity Services Director interface by selecting Connectivity Services Director from the Applications list in the left pane of the Junos Space user interface. To access the older version of the Services Activation Director GUI, select Services Activation Director from the Applications list of the Junos Space user interface.

Related Documentation • [Logging Out of Connectivity Services Director on page 30](#)

Accessing the Services Activation Director GUI

In Connectivity Services Director Release 2.0, you can also access the Services Activation Director GUI interface to launch workspaces to configure functionalities. You must install Junos Space Platform before trying to access the Services Activation Director GUI, perform the following steps after Junos Space Platform is installed:



NOTE: The appendixes at the end of this documentation describes the workspaces and functionalities that you can configure using the Services Activation Director GUI. The applications in the Services Activation Director suite are a legacy implementation that provide backward compatibility and are no longer recommended for use. Although you can configure features such as service orders and service definitions using the Services Activation Director GUI, we recommend that you use the Network Services utility of the Connectivity Services Director GUI to define such capabilities. The older look-and-feel of the GUI might be removed completely in a future release. In Connectivity Services Director Release 2.0, the Service Templates, and Threshold Alarm Profile workspaces or windows of the Network Activate application of the Services Activation Director suite are not implemented. You can use the Services Activation Director GUI to navigate to these workspaces and configure the corresponding functionalities.



NOTE: The software image for Connectivity Services Director Release 2.0 enables you to install the Connectivity Services Director GUI. Also, Network Activate, Transport Activate, OAM Insight, and Sync Design are installed and presented in the same look-and-feel as Services Activation Director, after you install Connectivity Services Director. The Representational State Transfer (REST) APIs for Connectivity Services Director are installed along with the GUI.

Before You Begin:

- Configure the Junos Space appliance with a Junos Space image. For complete configuration steps, see [Configuring a Junos Space Appliance](#) or [Configuring the Basic Settings of a Junos Space Virtual Appliance](#).
- Install the Connectivity Services Director image on the Junos Space appliance. See *Installing Connectivity Services Director* for step-by-step instructions on installing the image.

To access the Services Activation Director GUI:

1. Log in to Junos Space by using the following URL:

```
https://<n.n.n.n>/mainui
```

where *n.n.n.n* is the IP address of the Junos Space Web interface.

The Junos Space login page appears.

2. Enter your login credentials, such as the username and password, and click **Log In**.

The Junos Space Platform GUI is displayed.

3. Select Services Activation Director from the Applications list on the left pane of the Junos Space user interface.

The Services Activation Director GUI is launched.

Alternatively, if you select Connectivity Services Director from the Applications list on the left pane of the Junos Space user interface, the Connectivity Services Director GUI is launched.

Related Documentation

- [Logging In to Connectivity Services Director on page 25](#)
- [Logging Out of Connectivity Services Director on page 30](#)

Changing Your Password for Connectivity Services Director

Any user, regardless of user role, can change his or her password.

You use the same username and password that you use for Junos Space and Connectivity Services Director.

To change your password:

1. From the Connectivity Services Director user interface, click the Junos Space icon on the Connectivity Services Director banner.
The Junos Space Platform user interface is displayed.

2. Click the **User Settings** icon on the Junos Space banner.
The **Change User Settings** dialog box appears.

3. In the **Old Password** text box, enter your old password.



NOTE: Mouse over the information icon (small blue *i*) next to the **New Password** text box to view the rules for password creation. For more information about the password rules, see *Modifying Junos Space Network Management Platform Settings*.

4. In the **New Password** text box, enter your new password. The minimum value for this field is 6 (the default) and the maximum value is 999. The password can include alphanumeric and special characters, but not control characters.

5. In the **Confirm Password** text box, enter your new password again to confirm it.



NOTE: The fields on the X.509 Certificate tab are applicable when you want to use certificate-based authentication. If you are using password-based authentication, you can ignore these fields. For more information about certificate-based authentication, see the *Certificate Management Overview* topic in the *Junos Space Network Management Platform Workspaces Feature Guide*.

6. (Optional) Select the **Manage objects from all assigned domains** check box on the **Object Visibility** tab to view and manage objects from all the domains for which you are assigned.

7. Click **OK**.

You are logged out of the system. To log in to Junos Space again, you must use your new password. Other sessions logged in with the same username are unaffected until the next login.

Related Documentation

- [Logging In to Connectivity Services Director on page 25](#)
- [Accessing the Services Activation Director GUI on page 27](#)

- [Logging Out of Connectivity Services Director on page 30](#)

Logging Out of Connectivity Services Director

After you finish using Connectivity Services Director, log out to prevent unauthorized access. You can log out manually or set an automatic logout period for Connectivity Services Director to automatically log you out.

Logging out manually—To log out of Connectivity Services Director manually, click the down arrow next to the username on the Connectivity Services Director banner and select Logout from the list.

Logging out automatically—Connectivity Services Director automatically logs you out if you have not performed any action on it, such as by using keystrokes or mouse-clicks, for a set period of time. This automatic logout conserves server resources and protects the system from unauthorized access. By default, automatic logout occurs if a session has been idle for 60 minutes. You can change the setting on the Applications inventory page. Select **Administration > Applications > Network Management Platform > Modify Application Settings** (from the Actions menu) > **User**.

Connectivity Services Director uses the same automatic logout period as Junos Space.

To change the automatic logout period:

1. Click the System Platform icon on the Connectivity Services Director banner.
The logout page appears.
2. Click the **Click here to log in again** link on the logout page to log in to the system again.
3. Navigate to **Administration > Applications**.
The Applications page is displayed.
4. Right-click **Network Management Platform** and select **Modify Application Settings**.
The Modify Application Settings page appears.
5. In the Modify Network Management Settings page, select **User**.
The User page is displayed.
6. In the **Automatic logout after inactivity (minutes)** field, move the slider to modify the automatic logout setting.
The logout setting is modified.
7. Click **Modify** to save the setting.
You are returned to the Modify Applications page.

- Related Documentation**
- [Logging In to Connectivity Services Director on page 25](#)
 - [Accessing the Services Activation Director GUI on page 27](#)

Getting Started Assistant Overview in Services Activation Director


The Getting Started assistant is a section in the sidebar that shows you how to perform common tasks. The tasks in the Getting Started assistant are workspace specific. The tasks displayed in this section vary according to the workspace. The Getting Started assistant provides instructions on how to perform tasks related to a device, service template, or a policy and filter template configuration.

The Getting Started topics are context-sensitive per application. Getting Started displays all the steps of a task. From a step in a task, you can jump to that point in the user interface to actually complete it. If **Show Getting Started on Startup** check box is selected, the Getting Started assistant automatically displays the tasks when you log in. If this check box was not selected, click the **Help** icon and click **Getting Started** from the resulting sidebar.

To use a Getting Started assistant:

1. Select an application from the **Applications** list above the task tree.
2. In the sidebar, expand **Getting Started**.

A main Getting Started topic link appears on the sidebar.

If the sidebar is not displayed, select the **Help** () icon at the right side of the Junos Space header. The sidebar appears.

3. Select a main topic.

For example, if you are in the Network Management Platform application user interface, click the **Increase Space Capacity** link. A list of required steps appears in the sidebar. Each step contains a task link and a link to Help.

4. Perform a specific step by clicking the link.

You jump to that point in the user interface. The assistant remains visible on the sidebar to aid navigation to subsequent tasks.

5. Access help for a specific step by clicking the Help icon next to that step.

CHAPTER 2

Service View Tasks and Lifecycle Modes

- [Understanding the Service View Tasks Pane in Build Mode on page 33](#)
- [Understanding the Service View Tasks Pane in Deploy Mode on page 36](#)
- [Understanding the Service View Tasks Pane in Monitor Mode on page 38](#)
- [Understanding the Service View Tasks Pane in Fault Mode on page 40](#)
- [About Build Mode in Service View of Connectivity Services Director on page 41](#)
- [About Deploy Mode in Service View of Connectivity Services Director on page 43](#)
- [About Fault Mode in All Views of Connectivity Services Director on page 45](#)
- [About Monitor Mode in Service View of Connectivity Services Director on page 45](#)

Understanding the Service View Tasks Pane in Build Mode

The Tasks pane in Service View contains all the operations that you can perform to create the network managed by Junos Space Connectivity Services Director by using the prestaging process that discovers devices in the Junos Space database and assigns roles to those devices and their interfaces. In Build mode, you can use the Tasks pane to define service definitions, which specify the service parameters for the devices or endpoints and associated interfaces for controlling traffic flow.

Click a specific task to begin that task. Not all tasks are available in the Service View when you launch it the first time. Depending on the service definitions that you create, those configured service definitions are displayed under the corresponding service trees, such as VPLS or L3VPN, in the task pane. Service View tasks are divided into the following categories in the Tasks pane.

- **Key Tasks**—Connectivity Services Director enables you to group the tasks that you perform frequently and create a list of key tasks. The most preferred tasks that you want to do while using the Service View are listed under Key Tasks. You can add tasks from the service task menu to the Key Tasks category. The Key Tasks category is a duplicate of the added tasks from the Service Provisioning and Service Design tasks menu. You can add any task from the Tasks pane to the Key Tasks list by selecting a task and clicking the plus (+) sign that appears adjacent to the task. For some modes, you can see that Connectivity Services Director has predefined some key tasks for you. You can also modify this set of tasks to suit your requirements. This modification feature is available in the Task pane irrespective of your current mode, scope, or view.
- **Manage Service Templates** (accessible from the Services Activation Director GUI)—Provides a powerful mechanism to configure advanced service-related options that are not exposed via the service order creation workflow. Create and attach one or more service templates to a service definition to define any provisioning-related configuration option beyond the current coverage of Connectivity Services Director.
- **Service Design**—Enables you to create and manage service definitions and service templates. A service definition specifies the attributes that are common among a group of service orders that have similar service requirements. Service templates are specific to service definitions. Both are specific to service types, so that if you are dealing with an L3VPN service type, for example, both your service definition and service template must be of that type.
- **Manage Service Definitions**—Provides a set of predefined service definitions for point-to-point services, multipoint-to-multipoint (full mesh) services, point-to-multipoint (hub and spoke) services, and RSVP LSP services. These service definitions are capable of providing the basis for most of the service orders your organization will need to create.
- **View Services**—Enables you to view the configured point-to-point, L3VPN, and VPLS services by the service types and the service statuses. In the View pane, if you select the Connectivity item in the tree under Network Services, without expanding the tree and selecting a specific service type, such as P2P Services, L3VPN Services, or VPLS Services, the top pane displays a set of five pie charts that enable you to view the different service orders configured, and their associated audit and monitoring statuses. The FA Status chart displays the functional audit status for the service orders. The Device State graph displays the statuses of devices on which services are being provisioned and commissioned. The Fault Status chart displays the connectivity fault management details for the service orders. The SLA Status chart displays the service-level agreement details for the service orders. The PM Status chart displays the performance management details for the service orders. The count or percentage of service orders in the pie chart segments sum up to the total number of configured service orders. Mouse over each segment of the pie to view the number corresponding to the percentage of service orders for each of the charts. These charts provide a visual overview of customers and service orders on your network, and enables you to quickly access related and commonly needed information. For example, you can check for failed service orders and then access a list of failed requests so you can begin to take restoration measure.
- **View LSPs**—Enables you to view the configured RSVP LSP services.

- **View Details**—Enables you to view comprehensive information about the configured parameters of a service.
- **Audit/Results**—Enables you to run configuration and functional audit operations, and view the results of the audit job.
 - **Configuration Audit**—Enables you to perform a configuration audit and view the results of the operation. A configuration audit can help you determine whether the service configuration on the device has been changed out of band.
 - **Functional Audit**—Enables you to perform a functional audit and view the results of the operation.
 - **Troubleshoot**—Enables you to run the operational scripts that are either created or imported to the platform from the local machine before you start troubleshooting the services or you can run the scripts that are of local type directly from the Functional Audit Result window by clicking the **Troubleshoot** button.
- **Prestage Devices**—Enables you to change the device and interface role assignments, view prestaging rules, and manage resource pools.
 - **Prestage Devices**—Enables you to assign network provider edge (N-PE) and provider (P) roles to devices and user-to-network interface (UNI) roles to interfaces.
 - **Prestage Rules**—Enables you to view the prestaging rule details.
 - **Manage Resources**—Enables you to view resource pools, such as IP addresses and VLANs, and create IP address pools to be used in services.
- **Customer**—Displays the tasks that you can perform to manage customers
 - **Add Customers**—Enables you to add new customers on the system before you can provision and activate a service order for each of them.
 - **Delete Customer**—Enables you to delete a previously created customer.
 - **View Customer**—Enables you to view customers for which service orders need to be configured and deployed.

**Related
Documentation**

- [Understanding the Service View Tasks Pane in Deploy Mode on page 36](#)
- [Understanding the Service View Tasks Pane in Monitor Mode on page 38](#)
- [Understanding the Service View Tasks Pane in Fault Mode on page 40](#)
- [About Build Mode in Service View of Connectivity Services Director on page 41](#)
- [About Deploy Mode in Service View of Connectivity Services Director on page 43](#)
- [About Fault Mode in All Views of Connectivity Services Director on page 45](#)
- [About Monitor Mode in Service View of Connectivity Services Director on page 45](#)

Understanding the Service View Tasks Pane in Deploy Mode

The Tasks pane in Deploy mode lists the operations that you can perform in Service View to propagate and provision the configuration settings of the service orders to the corresponding devices. All Deploy mode tasks are always available, regardless of the scope selected in the View pane. Service View tasks are divided into the following categories in the Tasks pane.

- **Key Tasks**—Connectivity Services Director enables you to group the tasks that you perform frequently and create a list of key tasks. The most preferred tasks that you want to do while using the Service View are listed under Key Tasks. You can add tasks from the service task menu to the Key Tasks category. The Key Tasks category is a duplicate of the added tasks from the Service Provisioning and Service Design tasks menu. You can add any task from the Tasks pane to the Key Tasks list by selecting a task and clicking the plus (+) sign that appears adjacent to the task. For some modes, you can see that Connectivity Services Director has predefined some key tasks for you. You can also modify this set of tasks to suit your requirements. This modification feature is available in the Task pane irrespective of your current mode, scope, or view.
- **Service Provisioning**—The tasks you do to create and manage service orders for the topology of your network. A service order is an instance of the service definition that completes the definition for a specific customer's use. The service order always specifies the customer and the endpoints that link the customer sites through the network.
- **Deploy Services: Manage Network Services and Manage LSP**—Enables you to modify, delete, validate, and deploy services to enable the configuration parameters to be propagated and provisioned on the managed devices. You can perform the following tasks from the Manage Network Services page:
 - **Create a New Service Order**—Creates a service order for point-to-point, VPLS, Layer 3 VPN, and RSVP LSP protocols. A service order is an instance of the service definition that completes the definition for a specific customer's use. The service order always specifies the customer and the endpoints that link the customer sites through the network
 - **Modify a Service**—Modifies a previously configured service for point-to-point, VPLS, Layer 3 VPN, and RSVP LSP protocols. When a service is based on a service definition that you created in the Service Design workflow (Build mode of Service View), you can edit only those parameters of a service that were marked as **Editable in Service Order** in the service definition.
 - **Reactivate a Service**—Reactivates a previously disabled service order for point-to-point, VPLS, Layer 3 VPN, and RSVP LSP services. After you disable a service order to deactivate the configuration settings on devices mapped to the service, you might require the service settings to be reenabled after you have modified the service parameters, either directly on the device or using the Connectivity Services Director application.
 - **Deactivate a Service**—Disables a service order for a particular protocol that you have previously created on the network. By disabling a service, the traffic processing for the traversed packets is impacted. In certain network topologies, you might require

a service-related settings to be disabled for a certain period to perform troubleshooting or modification to the traffic-handling method.

- **Decommission a Service**—Decommissions a service that a customer no longer needs. You cannot decommission a service if a service order requesting action on that service is in the Requested, Scheduled, In Progress, or Invalid state.
- **Force-Deploy a Service**—Forcefully deploys the service to push the configuration to the device. Forceful deployment pushes the same configuration to the device that was pushed during the deployment of the service, thus allowing the operator to recover from a state in which the configuration on the device was lost or changed out-of-band.
- **Run Functional Audit**—Performs a functional audit and view the results of the operation. A functional audit determines whether a deployed service instance is functioning.
- **Run Configuration Audit**—Performs a configuration audit and view the results of the operation. A configuration audit can help you determine whether the service configuration on the device has been changed out of band.
- **View Alarms**—Displays the Alarm Detail monitor to locate a specific alarm, research the events causing the alarm, and to assign a disposition to the alarm. When an alarm is highlighted in the sorting sequence, the events contributing to the alarm are listed in the Event Details monitor and the variable settings are shown in the Event Attribute Detail table.
- **Deploy Services: Manage Service Orders and Manage LSP Deployment**—Schedule a service order for deployment on the network at a particular time, or propagate the service settings to devices for publishing and commissioning the settings immediately. You can perform the following tasks from the Manage Service Orders page:
 - **Modify a Service Order**—Enables you to modify a previously configured service order for point-to-point, VPLS, and Layer 3 VPN protocols. When a service order is based on a service definition that you created in the Service Design workflow (Build mode of Service View), you can edit only those parameters of a service that were marked as **Editable in Service Order** in the service definition. The other attributes can be updated only in the service definition or service template.
 - **Deploy now**—Propagates the service settings and provisions them on the devices immediately.
 - **Schedule Deploy**—Commissions the service settings on the devices at a specified future time.
 - **Discard Pending Configuration**—Discards all the pending service configurations that were made on a device
 - **Validate Pending Configuration**—Performs analysis and validation checks to verify that the pending changes are compatible with a device when you deploy configuration changes to the device.
 - **View Pending Configuration**—Displays the configuration of a service order that is in the requested state, the scheduled state, the invalid state, or the failed deployment state.

- **Delete Partial Configuration**—Removes the residual configuration for a failed service order of type Provisioning that can leave parts of the service configuration on the devices.
- **Deploy Configuration Changes**—Deploys pending configuration changes to devices.
- **View Deployment Jobs**—Manages configuration deployment jobs. When you deploy configuration changes or schedule a configuration deployment, a configuration deployment job is created. You can view the details of a service configuration deployment job or cancel a scheduled service configuration deployment job.

Related Documentation

- [Understanding the Service View Tasks Pane in Build Mode on page 33](#)
- [Understanding the Service View Tasks Pane in Monitor Mode on page 38](#)
- [Understanding the Service View Tasks Pane in Fault Mode on page 40](#)
- [About Build Mode in Service View of Connectivity Services Director on page 41](#)
- [About Deploy Mode in Service View of Connectivity Services Director on page 43](#)
- [About Fault Mode in All Views of Connectivity Services Director on page 45](#)
- [About Monitor Mode in Service View of Connectivity Services Director on page 45](#)

Understanding the Service View Tasks Pane in Monitor Mode

The Tasks pane in Monitor mode displays a list of operations that you can perform to analyze and identify network conditions that require corrective action for the configured services on devices. A set of graphs and statistical details in tables are displayed to enable you to easily view the state of your network in an intuitive format. Connectivity Services Director monitors its managed services on devices and maintains the information it collects from the devices in a database. Service View tasks are divided into the following categories in the Tasks pane.

- **Key Tasks**—Connectivity Services Director enables you to group the tasks that you perform frequently and create a list of key tasks. The most preferred tasks that you want to do while using the Service View are listed under Key Tasks. You can add tasks from the service task menu to the Key Tasks category. You can add any task from the Tasks pane to the Key Tasks list by selecting a task and clicking the plus (+) sign that appears adjacent to the task. For some modes, you can see that Connectivity Services Director has predefined some key tasks for you. You can also modify this set of tasks to suit your requirements. This modification feature is available in the Task pane irrespective of your current mode, scope, or view.
- **Service Summary**—Displays the consolidated and cumulative status of a service. This tab is applicable for P2P, L3VPN, and VPLS services. The Connections monitor show the status of the connection or link (up or down) between peer devices. In the table displayed for this monitor, the row represents the source device and the column denotes the destination device. The status of the link is displayed for P2P and VPLS services. The Traffic Summary monitor represents the total Egress (Packets out) traffic passing through all the UNI or CE interfaces that are part of the cumulative services. It is

displayed for point-to-point (P2P), Layer 3 VPN (L3VPN), and virtual private LAN (VPLS) services. The Current Active Alarms monitor shows any active alarm that has not yet been cleared

- **Service Transport**—Displays the transport or packet statistics for data against time between the source and destination devices that you select, and based on the LSP that is used by the endpoint. The source device is the row selected in the Connection Matrix widget on the Service Transport tab. The destination device is chosen from the Traffic Statistics widget on the Service Transport tab. By default, no destination devices are selected. Service transport statistical values are displayed for P2P, VPLS, and L3VPN services.
- **Service Traffic**—Displays the end-to-end traffic matrix that signifies the traffic between peer devices. You can view statistical counters and metrics for input packets, input bytes, output packets, and output bytes. The Interface Statistics monitor shows traffic data on all the user-to-network interfaces (UNI) or site interfaces that are part of the service. These values are on-demand statistical values and the data is retrieved from the device directly without being cached (polling at periodic intervals and displaying a snapshot). This tab is supported for P2P, VPLS, and L3VPN services. The data is available only if queues are enabled on the interface.
- **Service Performance**—Displays frame delay, frame loss, frame delay variation, and service availability. These measurements are achieved by triggering a one-way delay, two-way delay, or loss. The performance measurement is useful for generating periodic service-level agreement conformance reports from the deployed network and for studying traffic patterns in the network over a period of time. In proactive mode, SLA measurements are triggered by an iterator application. An iterator is designed to periodically transmit SLA measurement packets in form of ITU-Y.1731-compliant frames for two-way delay measurement or loss measurement for each of the connections registered to it. Iterators make sure that measurement cycles do not occur at the same time for the same connection to avoid CPU overload. The iterator profiles are configured on remote MEP for measurement of Ethernet frame delay measurement (ETH-DM), Ethernet frame loss measurement (ETH-LM), and statistical frame loss (SFL).
- **LSP Summary**—Displays a comprehensive and cohesive view about the configured RSVP LSP service. The status of the LSP and the status of connections between the ingress router and egress routers in an LSP are displayed. The LSP status details are shown for the ingress router. You can also view the ingress, egress, and transit LSP information, such as the primary and secondary states.
- **Clear Interface Statistics**—Deletes all of the interface-related counters and values associated with the selected service. It is effective for PTP, VPLS, and L3VPN services.
- **Clear LSP Statistics**—Deletes all of the interface-related counters and values associated with the selected RSVP LSP service.
- **MPLS Ping**—Sends a probe from one endpoint to the other endpoint of a service, such as P2P, L3VPN, LSP, and VPLS. Use the Ping MPLS functionality to diagnose the state of label-switched paths (LSPs), Layer 2 and Layer 3 virtual private networks (VPNs), and Layer 2 circuits. You can ping an MPLS endpoint using various options. You can send variations of ICMP echo request packets to the specified MPLS endpoint.

- **MPLS Traceroute**—Enables you to trace the route followed by an LDP-signaled LSP. LDP LSP traceroute is based on RFC 4379, Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures. This feature allows you to periodically trace all paths in a FEC.
- **Show Interface Statistics**—Displays the interface-related settings and parameters associated with the selected service, such as P2P, L3VPN, and VPLS.
- **Show Interface Status**—Displays interface status details to monitor interface bandwidth utilization and traffic statistics associated with the selected service, such as P2P, L3VPN, and VPLS.
- **Show Routing Table**—Displays the routing table information for the selected virtual routing instance. For L3VPN services, you can determine which LSPs or tunnels are being used by looking at the routing tables.
- **Show MAC Table**—Displays the learned MAC address information for a device associated with a particular service:
- **PM Statistics**—Enables you to start and stop the collection of performance monitoring statistical details.

**Related
Documentation**

- [Understanding the Service View Tasks Pane in Build Mode on page 33](#)
- [Understanding the Service View Tasks Pane in Deploy Mode on page 36](#)
- [Understanding the Service View Tasks Pane in Fault Mode on page 40](#)
- [About Build Mode in Service View of Connectivity Services Director on page 41](#)
- [About Deploy Mode in Service View of Connectivity Services Director on page 43](#)
- [About Fault Mode in All Views of Connectivity Services Director on page 45](#)
- [About Monitor Mode in Service View of Connectivity Services Director on page 45](#)

Understanding the Service View Tasks Pane in Fault Mode

The Tasks pane in Fault mode provides you with a set of tools for effectively managing alarms on your system. When certain types of events are persistent, or when the condition causing the event crosses a threshold, SNMP sends a notification, also called a trap to Connectivity Services Director that are correlated and displayed as alarms.

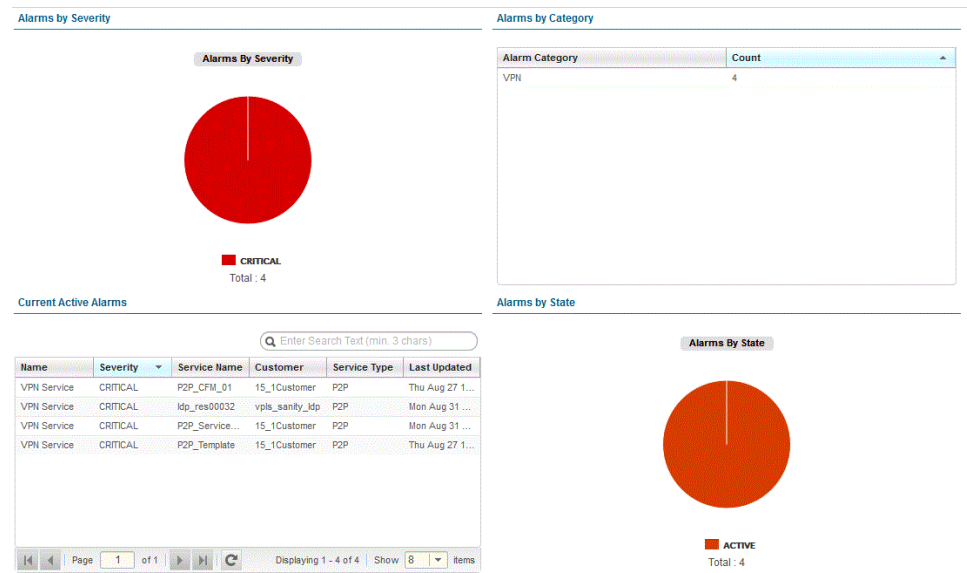
From the Tasks pane, you can filter known alarms to locate a specific alarm or error condition by clicking Search Alarms. Use this task to isolate alarms that occurred during a known time-frame or that have annotations associated with them. Although each of the Fault mode monitors can sort the alarms, Search Alarms enable you to submit multiple search and sort arguments as part of your search query.

In addition, Connectivity Services Director enables you to group the tasks that you perform frequently and create a list of key tasks. You can add any task from the Tasks pane to the Key Tasks list by selecting a task and clicking the plus (+) sign that appears adjacent to the task. For some modes, you can see that Connectivity Services Director has predefined some key tasks for you. You can modify this set of tasks to suit your

requirements. This feature is available in Task pane irrespective of your current mode, scope, or view.

The following monitors are displayed in Fault mode:

- **Alarms by Severity**—Displays the fault alarm details sorted based on severity—that is in the following order: critical, major, minor, and info.
- **Alarms By Category**—Displays the fault alarm details sorted based on category—that is in the following order: active, acknowledged, and cleared.
- **Alarms By State**—Displays the fault alarm details sorted based on state—that is in the following order: active, acknowledged, and cleared.
- **Current Active Alarms**—Displays any active alarm that has not yet been cleared.



Related Documentation

- [Understanding the Service View Tasks Pane in Build Mode on page 33](#)
- [Understanding the Service View Tasks Pane in Deploy Mode on page 36](#)
- [Understanding the Service View Tasks Pane in Monitor Mode on page 38](#)
- [About Build Mode in Service View of Connectivity Services Director on page 41](#)
- [About Deploy Mode in Service View of Connectivity Services Director on page 43](#)
- [About Fault Mode in All Views of Connectivity Services Director on page 45](#)
- [About Monitor Mode in Service View of Connectivity Services Director on page 45](#)

About Build Mode in Service View of Connectivity Services Director

In Build mode, you can create services for devices that are managed by Connectivity Services Director. You can define service templates and attributes of different services,

and also specify policies and filters to classify and control the manner in which packets must be handled by the various services.

Configuring a service has a major impact on the flow of routing information or packets within and through the router. For example, you can configure a routing service that does not allow routes associated with a particular customer to be placed in the routing table. As a result of this configured service, the customer routes are not used to forward data packets to various destinations and the routes are not advertised by the routing protocol to neighbors. The service designer uses the Build mode for managing the service definitions that the service provisioner uses as the basis for creating a service order. You can create a service definition that specifies the attributes that are common among a group of service orders that have similar service requirements, and a service order, which is an implementation object or a derivative of a service definition.

This topic describes the following functionalities that are available in Build mode of Service View:

- [Manage Service Definitions on page 42](#)
- [Prestage Devices on page 42](#)
- [Prestage Services on page 42](#)
- [Manage Threshold Alarm Profiles on page 43](#)
- [Service Definition Operations on page 43](#)
- [Audit and Troubleshooting of Services on page 43](#)

Manage Service Definitions

Connectivity Services Director software provides a set of predefined service definitions for point-to-point services, multipoint-to-multipoint (full mesh) services, and point-to-multipoint (hub and spoke) services. These service definitions are capable of providing the basis for most of the service orders your organization will need to create. In case these predefined service definitions are not adequate for all your needs, however, the Network Activate software enables you to create service definitions of your own.

Prestage Devices

Prestaging takes the devices already under Junos Space management and prepares them for service activation. The prestaging process discovers network provider edge (N-PE) devices in the Junos Space database and assigns roles to those devices and their interfaces. N-PE routers and user-to-network interfaces (UNIs) are basic building blocks required for Layer 2 and Layer 3 provisioning

Prestage Services

The Service Recovery feature functions within the pre-staging operation of the Network Activate application. Service Recovery has two parts. First, Service Recovery parses each device's configuration searching for service configurations and existing Network Activate service elements (P2P services, Layer 2 circuits, routing instances, firewalls, policy options, routing options, and OAM interface branches of Junos Space configurations that are being processed).

Manage Threshold Alarm Profiles

You can create profiles to measure performance monitoring counters and parameters, and attach such threshold alarm profiles to a service definition. In performance management (PM), the Connectivity Services Director application provides an option to measure the frame delay, frame loss, frame delay variation, and service availability. These measurements are achieved in either of the following ways:

- Triggering a one-way delay
- Triggering a two-way delay
- Loss

The performance measurement is useful for generating periodic service level agreement conformance reports from the deployed network and for studying traffic patterns in the network over a period of time. The iterator profiles are configured on remote MEP for measurement of frame delay (ETH-DM), frame loss (ETH-LM) and statistical frame loss (SFL).

Service Definition Operations

You can perform several tasks on service definitions, such as editing, publishing, or unpublishing a service definition. You can modify a service definition to suit your network needs. The service designer must publish a customized service definition before a service provisioner can use that definition to create a service request. The service designer can unpublish a custom service definition to make it unavailable to service provisioners for creating a service request. You cannot unpublish a predefined service definition.

Audit and Troubleshooting of Services

After the service is deployed, a functional audit establishes whether the service is up or down. If the functional audit reports that the service is up, the customer can begin using the service. Once the service is active, the service provisioner can monitor the health of the service by running a functional audit or a configuration audit. Users assigned the Service Activator role can perform these service provisioning tasks.

Related Documentation

- [About Deploy Mode in Service View of Connectivity Services Director on page 43](#)
- [About Monitor Mode in Service View of Connectivity Services Director on page 45](#)

About Deploy Mode in Service View of Connectivity Services Director

The Deploy mode enables you to deploy service order configuration changes to devices. When you make configuration changes in Build mode, the changes are not deployed to devices automatically. You must manually deploy the changes to devices in Deploy mode. Every time you make configuration changes in Build mode that affect a service, you must propagate the service order changes to the device by commissioning the configuration to the device. Configuration changes are deployed to devices at the device level. When you deploy configuration changes to a device, all pending configuration changes for that device are deployed.

This topic describes the following functionalities that are available in Deploy mode of Service View:

- [Manage Network Services on page 44](#)
- [Manage Deployment of Service Orders on page 44](#)

Manage Network Services

A service is an instance of the service order that defines the configuration parameters and attributes for transmission and management of traffic in a customer network. A service is created for a deployed service order. The service always specifies the customer and the endpoints that link the customer sites through the MPLS network. For each endpoint, the service provisioner specifies the network provider edge device and the UNI on that device that connects the customer site to the N-PE device. The service can also specify any additional attributes that are configured in the service definition as editable in the service order. These attributes might include the virtual circuit ID (VCID), maximum transmission unit (MTU) for the ingress or user-to-network interface (UNI), MTU for the connection across the network, VLAN-ID, rate limiting bandwidth, and so forth.

You can modify the properties of the service, conduct a functional or configuration audit, activate or deactivate the service, and view alarms associated with a particular service order for debugging and corrective action.

You can decommission a service that a customer no longer needs. You cannot decommission a service if a service order requesting action on that service is in the Requested or Draft, Scheduled, In Progress, or Invalid state.

Manage Deployment of Service Orders

A service order is an instance of the service definition that completes the definition for a specific customer's use. In Deploy mode, you can do the following configuration deployment tasks on devices for which service orders are configured to be provisioned or that have pending changes:

- Modify the parameters of a service order to suit your deployment needs or to resolve traffic-forwarding problems caused by service attributes.
- Validate the configuration of service orders.
- Delete partial configuration of services on devices.
- Discard the pending configuration of services from being deployed to devices.
- Run configuration deployment jobs immediately or schedule them for future times.
- Preview pending configuration changes before deploying.
- Manage configuration deployment jobs.

Related Documentation

- [About Build Mode in Service View of Connectivity Services Director on page 41](#)
- [About Monitor Mode in Service View of Connectivity Services Director on page 45](#)

About Fault Mode in All Views of Connectivity Services Director

Fault mode in Connectivity Services Director provides you visibility into your network status and performance by displaying alarms and events generated on devices and configured services on devices. Connectivity Services Director monitors its managed devices and maintains the information it collects from the devices in a database. Fault mode displays this information in easy-to-understand graphs and in tables that you can sort and filter, allowing you to quickly visualize the state of your network, spot trends developing over time, and find important details. When certain types of events are persistent, or when the condition causing the event crosses a threshold, SNMP sends a notification, also called a trap to Connectivity Services Director.

Connectivity Services Director correlates traps, describing a condition, into an alarm. For example, multiple power supply traps coming from a device are correlated into a single power supply alarm for the device. The main purpose and benefit of monitoring functionalities is to allow the operators to quickly monitor the health (working condition), operating efficiency, traffic-handling capacity, and performance status of the managed devices and configured services such as P2P, VPLS, and L3VPN.

The monitoring mechanism is tool that enables the operator to understand the network health and status by drilling down to all the components of a device. The device status is marked as green, red, orange, or blue, based on the health, availability, performance and other important key performance indicators.

- Red denotes an emergency condition, which is a system panic or other conditions that cause the routing platform to stop functioning. It also indicates that the device is offline or turned down.
- Orange denotes an alert, which can be conditions that must be corrected immediately, such as a corrupted system database.
- Yellow indicates a notice, which signifies conditions that are not error conditions but are of interest or might warrant special handling. It can also include a severity level equivalent to informational or debugging messages.
- Blue denotes an informational message; no action is necessary. Informational alarms do not necessarily indicate an error. It could indicate that a device or entity has changed state.

Related Documentation

- [About Build Mode in Service View of Connectivity Services Director on page 41](#)
- [About Deploy Mode in Service View of Connectivity Services Director on page 43](#)
- [About Monitor Mode in Service View of Connectivity Services Director on page 45](#)

About Monitor Mode in Service View of Connectivity Services Director

Monitor mode in Connectivity Services Director provides you visibility into the transmission of packets between peer devices, health and traffic-handling capacity, and consolidated statistical details of important packet metrics based on the services configured. The

Connectivity Services Director application monitors its managed services on devices and maintains the information it collects from the devices in a database. Monitor mode displays this information in easy-to-understand graphs and in tables that you can sort and filter, allowing you to quickly visualize the state of your network, spot trends developing over time, and find important details.

This topic describes the following functionalities that are available in Monitor mode of Service View:

- [Quick Access to Important Troubleshooting Details on page 46](#)
- [Performance Monitoring on page 46](#)
- [View and Clear Interface Information on page 46](#)
- [View Interface Status on page 47](#)
- [View Routing Table on page 47](#)
- [View MAC Table on page 47](#)
- [Traceroute for an MPLS LSP on page 47](#)
- [MPLS Ping on page 47](#)

Quick Access to Important Troubleshooting Details

The main purpose and benefit of monitoring functionalities is to allow the operators to quickly monitor the health (working condition), operating efficiency, traffic-handling capacity, and performance status of the managed devices and configured services. Several monitors or widgets are displayed to enable you to track, diagnose, and rectify problems and discrepancies associated with services configured on devices. For example, you might observe that an L3VPN service is reported as down from the summarized information presented for that service on the monitoring page. This high-level view enables you to navigate to the settings for that service and tune them properly to function properly.

Performance Monitoring

You can employ the ITU-T Y.1731 standard-compliant Ethernet loss measurement (ETH-LM), Ethernet synthetic loss measurement (ETH-SLM), and Ethernet delay measurement (ETH-DM) capabilities to analyze and examine the operating efficiency and performance status. These performance monitoring functionalities can be run for P2P and VPLS services. You can start and stop the collection of performance monitoring statistics on the services that you want to monitor. The retrieval and computation of statistical details are performed using SNMP MIBs.

View and Clear Interface Information

You can view the learned MAC address information for a device associated with a particular service, the interface statistical counters and metrics, and the status of an interface. The functionalities available in Monitor mode of Service View are equivalents to the operational commands you can run from the Junos CLI interface to view interface information or MAC address details. You can also clear the interface statistics maintained on a device.

View Interface Status

You can view the interface status to monitor interface bandwidth utilization and traffic statistics on the device. When you view the interface status for a particular service, all the interfaces configured on the different devices associated the service are retrieved and displayed.

View Routing Table

The Routing Table window enables you view the routing table information for the selected virtual routing instance. For L3VPN services, you can determine which LSPs or tunnels are being used by looking at the routing tables.

View MAC Table

You can view the learned MAC address information for a device associated with a particular service. You can manage MAC entries more efficiently by viewing the configured aging time for a MAC entry, which is the maximum time that an entry can remain in the MAC address table before it is deleted because it has reached its maximum age

Traceroute for an MPLS LSP

You can perform a traceroute operation to examine the network reachability and identify connection failures from a source or ingress host to a remote host for an MPLS LSP signaled by RSVP. It a debugging tool to locate MPLS label-switched path (LSP) forwarding issues in a network. (Currently supported for IPv4 packets only.)

MPLS Ping

You can use the MPLS ping application to examine the network reachability and identify any broken links for diagnostic purposes. In IP networks, the ping and traceroute functionalities enable you to verify network connectivity and find broken links or loops. In MPLS-enabled networks, you can use the ping capability to determine whether IP connectivity exists to a destination even when the ping packets must traverse multiple LSPs.

Related Documentation

- [About Build Mode in Service View of Connectivity Services Director on page 41](#)
- [About Deploy Mode in Service View of Connectivity Services Director on page 43](#)
- [About Fault Mode in All Views of Connectivity Services Director on page 45](#)

CHAPTER 3

Network Services Overview

- [Getting Started with Connectivity Services Director on page 50](#)
- [Prestaging Devices Overview on page 53](#)
- [Junos Space Layer 2 Services Overview on page 55](#)
- [Junos Space Layer 3 Services Overview on page 64](#)
- [Provisioning Process Overview on page 65](#)
- [Seamless MPLS Support in Junos Space Overview on page 69](#)
- [Service Attributes Overview on page 71](#)
- [Service Order States and Service States Overview on page 86](#)
- [Understanding VLAN Manipulation \(Normalization and VLAN Mapping\) on Ethernet Services on page 88](#)
- [VLAN Pool Profiles Overview on page 93](#)
- [Redundant Pseudowires for Layer 2 Circuits and VPLS on page 94](#)
- [VPLS over GRE Overview on page 95](#)
- [Junos Space Network Topology Overview on page 96](#)
- [Service Recovery Overview on page 97](#)
- [Multicast L3VPN Overview on page 98](#)
- [Multi-Chassis Automatic Protection Switching Overview on page 99](#)
- [Inverse Multiplexing for ATM Overview on page 100](#)
- [Rendezvous Point on page 101](#)
- [Understanding Multicast Rendezvous Points, Shared Trees, and Rendezvous-Point Trees on page 101](#)
- [Understanding PIM Sparse Mode on page 103](#)
- [Configuring Shared-Tree Data Distribution Across Provider Cores for Providers of MBGP MVPNs on page 106](#)
- [Configuring SPT-Only Mode for Multiprotocol BGP-Based Multicast VPNs on page 107](#)
- [Configuring VRF Route Targets for Routing Instances for an MBGP MVPN on page 109](#)
- [Static Pseudowire Provisioning for VPLS Services on page 110](#)

Getting Started with Connectivity Services Director

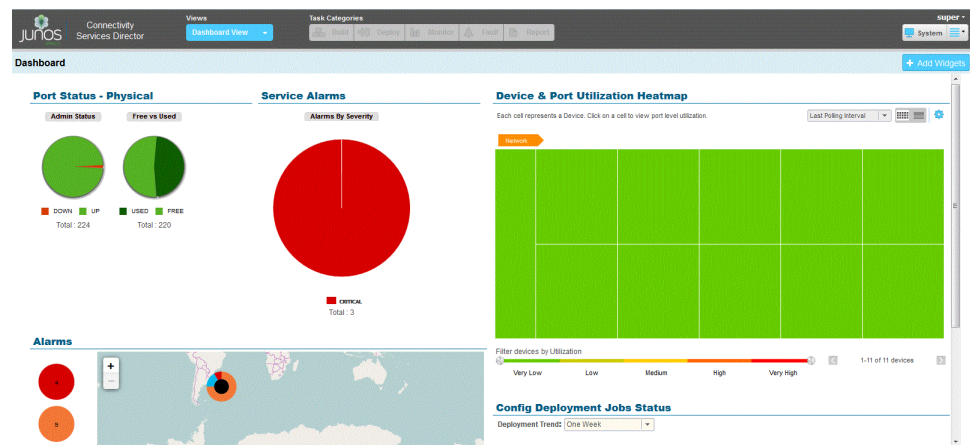
Based on your network deployment needs and configuration settings, you might require different service types, such as point-to-point, Layer 3 VPN, VPLS, or RSVP LSP services, to be applied on devices in your topology. It is essential to discover or add the devices that you want to be administered using Connectivity Services Director to the application database, before you can enable and define services. Also, the devices must be configured with the basic and mandatory device settings, such as routing instances, routing protocols, interfaces, and administrative groups, before they are imported or discovered for additional modifications, such as configuration of services, using the network management application.

When you install Connectivity Services Director, the single application package installs the capabilities for configuring network services, such as point-to-point, Layer 3 VPN, and VPLS, configuring MPLS and RSVP label-switched path (LSP) services, configuring Precision Time Protocol (PTP) and synchronous Ethernet services, configuring the OAM (Operations, Administration and Maintenance) functionality, and configuring class of service (CoS) profiles. To install Connectivity Services Director, see the *Installing and Uninstalling Connectivity Services Director* section in the *Junos Space Connectivity Services Director Quick Start Guide*.

You can also access the Services Activation Director GUI interface to launch workspaces to configure functionalities. To access the Services Activation Director GUI, see [“Accessing the Services Activation Director GUI” on page 27](#).

You need not separately install the different applications, such as Network Activate or Transport Activate, based on your deployment needs and device models to be managed, on a Junos Space JA1500 Appliance, Junos Space JA2500 Appliance, or a Junos Space Virtual Appliance that satisfied the hardware requirements. A consistent, uniform, consolidated, and streamlined user interface and elegant experience is introduced by using the Service View component in the Connectivity Services Director GUI. Besides offering a cohesive and user-friendly experience and interface for configuring point-to-point, Layer 3 VPN, VPLS, and RSVP LSP services, Network Activate, Transport Activate, Sync Design, and OAM Insight are available in the older GUI format in the same image package. The functionalities of QoS Design are available in Connectivity Services Director as CoS profiles, which you can reference in point-to-point, VPLS, and Layer 3 VPN services. QoS Design and Network Director cannot be installed on the same system as Connectivity Services Director.

Figure 5: Dashboard Page



The following workflow describes the tasks that you need to perform after the installation of the application to enable effective and streamlined management, provisioning, and troubleshooting of devices and services configured using Connectivity Services Director.

1. Discover devices using Connectivity Services Director GUI or the Junos Space Platform workspace. See [“Discovering Devices in a Physical Network” on page 177](#) for instructions on discovering devices from Build mode of Connectivity Services Director. See *Discovering Devices in the Junos Space Network Application Platform User Guide* for instructions on discovering devices using the Junos Space Platform workspace.



NOTE: Before you can add a device using device discovery, the following conditions must be met

- SSH v2 is enabled on the device. To enable SSH v2 on a device, issue the following CLI command:


```
set system services ssh protocol-version v2
```
- The NETCONF protocol over SSH is enabled on the device. To enable the NETCONF protocol over SSH on a device, issue the following CLI command:


```
set system services netconf ssh
```
- The device is configured with a static management IP address that is reachable from the Junos Space server. The IP address can be in-band or out-of-band.
- A user with full administrative privileges is created on the device for the Junos Space administrator.
- If you plan to use SNMP to probe devices as part of device discovery, ensure that SNMP is enabled on the device with appropriate read-only V1/V2C/V3 credentials.

2. Discover the roles of devices and assign network-provider edge (N-PE) roles as necessary. To prestage devices and assign device roles, see [“Discovering Device Roles” on page 374](#) and [“Excluding Devices from N-PE Role Assignment” on page 375](#).
3. Create service templates. Templates provide a powerful mechanism to configure advanced service-related options that are not exposed via the service order creation workflow. Templates are attached to a service definition. To work with service templates, see [“Service Templates Workflow” on page 1813](#) and [“Applying a Service Template to a Service Definition” on page 1814](#).
4. Review the predefined service definitions that are available by default, and determine whether you want to create a new customized service definition. A service definition specifies the attributes that are common among a group of service orders that have similar service requirements. To work with service definitions, see [“Predefined Service Definitions” on page 465](#), [“Creating a Point-to-Point Ethernet Service Definition” on page 625](#), [“Creating a Multipoint-to-Multipoint VPLS Service Definition” on page 653](#), [“Creating a Point-to-Multipoint VPLS Service Definition” on page 678](#), [“Creating a Full-Mesh Layer 3 VPN Service Definition” on page 709](#), and [“Creating a Hub-and-Spoke \(One Interface\) Layer 3 VPN Service Definition” on page 719](#).

5. Create customers that denote the users to be associated with service orders. New customers must be identified to the system before you can provision and activate a service order for them. To create customers, see [“Adding a New Customer” on page 737](#).
6. Create class-of-service profiles to prioritize the traffic flow and define policies for handling received packets to avoid network congestion and traffic disruption. See [“Creating and Managing Wired CoS Profiles” on page 224](#).
7. Create service orders for the types of protocols that your network environment requires for optimal and cohesive management of large numbers of devices. A service order is an instance of the service definition that completes the definition for a specific customer’s use. To work with service orders, see [“Creating a Service Order” on page 815](#).
8. Deploy service orders to propagate the service configuration to the corresponding devices. To transfer service order configurations to devices and apply the settings on the devices, see [“Deploying Services Configuration to Devices” on page 1005](#) and [“Managing Service Configuration Deployment Jobs” on page 1003](#).
9. Perform audit operations, such as functional and configuration audit, to examine the status of interfaces, LDP sessions, neighbor links, and endpoints of point-to-point services. You can also identify whether the service configuration on the device has been changed out of band. In addition, you can use op scripts to perform any function available through the remote procedure calls (RPCs) supported by either the Junos XML management protocol or the Junos XML API. See [“Performing a Functional Audit” on page 1067](#), [“Performing a Configuration Audit” on page 1077](#), and [“Troubleshooting N-PE Devices Before Provisioning a Service” on page 1080](#) for further information.
10. Monitor the health (working condition), operating efficiency, traffic-handling capacity, and performance status of the managed devices and configured services. Several monitors or widgets are displayed to enable you to track, diagnose, and rectify problems and discrepancies associated with services configured on devices. To evaluate and diagnose the services, traffic-flow, and device states, see [“Service Monitoring Capabilities in Connectivity Services Director” on page 1192](#).
11. View information about the health of your network and changing conditions of your equipment. Use Fault mode to find problems with equipment, pinpoint security attacks, or to analyze trends and categories of errors. For example, if you find that a particular device or a service has recorded a large number of critical or major alarms, you can then navigate to the appropriate device settings page or service order page to correct and modify the attributes or diagnose the problems that might be generating the alarms. To view alarms and events, see [“Understanding Fault Mode in Connectivity Services Director” on page 45](#).

Prestaging Devices Overview

In the Junos Space Connectivity Services Director product, prestaging takes the devices already under Junos Space management and prepares them for service activation. The prestaging process discovers network provider edge (N-PE) devices in the Junos Space database and assigns roles to those devices and their interfaces. N-PE routers and user-to-network interfaces (UNIs) are basic building blocks required for Layer 2 and Layer 3 provisioning.



NOTE: The Connectivity Services Director application does not support provisioning for J Series devices.

The Junos Space software makes it easy to complete all the prestaging activities you need for up to several hundred devices.

Prestaging uses the Connectivity Services Director application to automatically determine the role of a router based on rules that exist in the system. If a router is an N-PE router, the Junos Space software assigns it the N-PE role. The Junos Space software qualifies each interface on the N-PE router to be a serviceable UNI.

N-PE and UNI recommendations made automatically by the Connectivity Services Director application are appropriate for most situations. In some networks, however, you might need to make some exceptions. You might have recommended N-PE devices that you don't want to assign the N-PE role for provisioning. In addition, you might want to exclude some interfaces from qualification as UNIs.

Although the prestaging mechanism is automatically run in the background by default in the Connectivity Services Director application of Connectivity Services Director, you can manually configure the prestaging settings by using the Services Activation Director GUI, which provides the prestaging workspace.

To prestage devices while accepting all recommendations made by the Connectivity Services Director application, see [“Discovering and Assigning All N-PE Devices” on page 351](#). To make exceptions to the Connectivity Services Director recommendations, see [“Discovering and Assigning N-PE Devices with Exceptions” on page 353](#).



NOTE: After a device is prestaged in Connectivity Services Director, the prestaging job is not initiated on the same device again. When a device notification is received by the application, Connectivity Services Director synchronizes the prestaging database on the UI interfaces. If a mismatch is detected in the UNI status of the interface in Connectivity Services Director database and the UNI status of the interface on the device (caused by the application being down or network accessibility problems), the synchronization of the UNI interface might not occur. In such a case, the synchronization operation occurs when a configuration- commit on the device is done the next time. To manually resolve this discrepancy in the UNI status of the interface, you can unassign the UNI role of the interface, which causes prestaging to perform a synchronization.

Related Documentation

- [Prestaging Devices Process Overview on page 344](#)
- [Prerequisites for Prestaging Devices in Connectivity Services Director on page 350](#)
- [Discovering and Assigning All N-PE Devices on page 351](#)
- [Discovering and Assigning N-PE Devices with Exceptions on page 353](#)

- [Prestaging ATM and TDM Pseudowire Devices on page 356](#)
- [Prestaging Rules on page 364](#)

Junos Space Layer 2 Services Overview

Junos Space Connectivity Services Director application enables you to provision the following types of services:

- Point-to-point services across networks that use LDP or BGP for signaling in the network core. These services use directed pseudowire virtual circuits across the network to establish point-to-point virtual private networks (VPNs). The provisioner must specify the addresses of the ingress and egress routers of the virtual circuits.
- Multipoint services across networks that use LDP or BGP signaling in the network core. The Connectivity Services Director application supports multipoint-to-multipoint (full mesh) services and point-to-multipoint (hub and spoke) services.

For details about Juniper Networks Layer 2 technologies, see the *Junos OS VPNs Configuration Guide*.

Point-to-point services and multipoint services support the following interface types:

- Port-to-port—All traffic is transported across the network.
- 802.1Q (dot1q)—Supports 802.1Q VLAN-tagged network traffic in a point-to-point or multipoint Ethernet service. Network traffic is constrained using VLAN IDs.
- Q-in-Q—Supports double-tagged traffic in a point-to-point or multipoint Ethernet service.
- Asymmetric tag depth—Allows port-based, 802.1Q and Q-in-Q interfaces for UNIs to coexist in a service.
- ATM—Supports the transmission of ATM cells through point-to-point connections in an ATM network.
- TDM—Supports configuring SAToP or CESoPSN physical encapsulation of packets for transmission over the TDM interface.

[Table 5 on page 55](#) provides a guide to selecting the appropriate type of Layer 2 service for a specific customer need.

Table 5: Selecting a Layer 2 Service

Customer Requirement	Provision This Service
Send all VLAN traffic from one site to other sites in the service.	Layer 2 VPN port-to-port service OR Layer 2 VPN Q-in-Q to Q-in-Q service for all traffic

Table 5: Selecting a Layer 2 Service (continued)

Customer Requirement	Provision This Service
Send traffic associated with one specific VLAN from one site to other sites in the service.	Layer 2 VPN 802.1Q-to-802.1Q service
Send traffic associated with a range of VLANs from one site to other sites in the service.	Layer 2 VPN Q-in-Q to Q-in-Q service for a range of VLANs

Juniper Networks refers to this kind of connection as a *Layer 2 circuit*. For details about Layer 2 circuits, see the *Junos OS VPNs Configuration Guide*.

The Connectivity Services Director application enables you to provision a range of services from the following service families for your enterprise customers:

- [Point-to-Point Services on page 56](#)
- [VPLS Services on page 59](#)

Point-to-Point Services

Point-to-point services provide transport and encapsulation of Layer 2 Ethernet circuits between two endpoints. To provision a point-to-point service, the provisioner must select the network provider-edge (N-PE) routers that will be the service endpoints and configure the user-network interfaces (UNIs) at those endpoints. The Junos Space software automates the end-to-end provisioning of the pseudowire by establishing a virtual circuit between the N-PE routers using a unique virtual circuit ID (VC ID).

The IETF refers to these connections in RFC 4905, *Encapsulation Methods for Transport of Layer 2 Frames over MPLS Networks as emulated virtual circuits*, and in RFC 4447, *Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP) as pseudowire emulation* (see IETF RFC 4447).

The Metro Ethernet Forum (MEF) refers to these connections as *E-Line services*. See *Metro Ethernet Services – A Technical Overview* by Ralph Santitoro.

The Junos Space software enables you to provision the following point-to-point service options for your enterprise customers:

- [Port-to-Port Service on page 56](#)
- [Single VLAN Service Using 802.1Q Interfaces on page 57](#)
- [All Traffic Service Using Q-in-Q Interface on page 58](#)
- [Range of VLANs Service with Q-in-Q Interfaces on page 58](#)

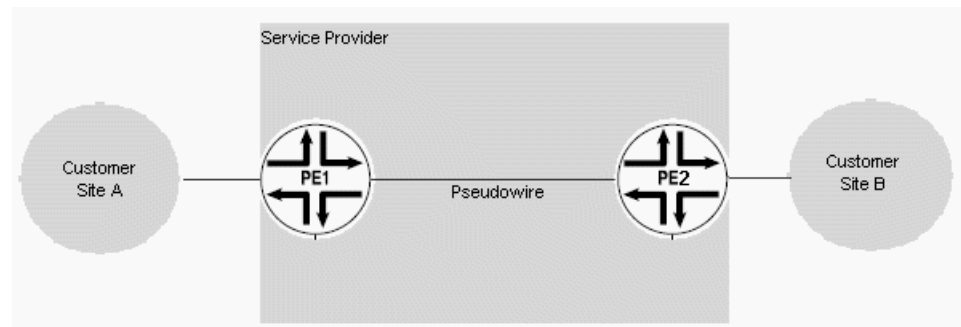
Port-to-Port Service

A port-to-port service transports all traffic on a port on a provider edge (N-PE) router across the network to a port of another N-PE router. enterprise customers needs to purchase only a single physical port for all their traffic. However, a single port might cost more than the bandwidth for a single VLAN or selected range of VLANs.

The service provider needs no knowledge of the enterprise customer's VLAN structure, because all the customer's traffic is transported.

Figure 6 on page 57 shows an example in which a port-to-port connection transports all VLAN traffic for an enterprise customer from customer site A to customer site B across the network.

Figure 6: Point-to-Point LDP Connection Transports Traffic

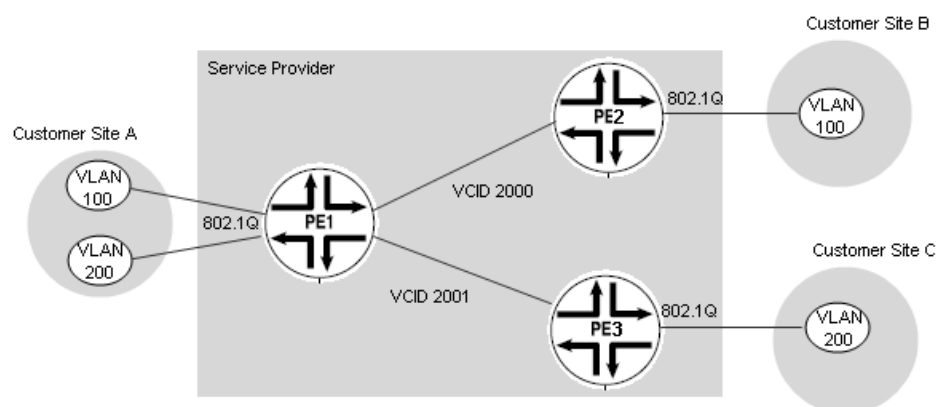


Single VLAN Service Using 802.1Q Interfaces

802.1Q services transport VLAN traffic from one site to another across the network. The selected payload is a single VLAN, so the enterprise customer needs to purchase only the bandwidth necessary to transport that VLAN. To implement this type of service, the service provider must exchange VLAN information with the enterprise customer.

Consider the example shown in Figure 7 on page 57. VLAN 100 might be used for payroll and spans sites A and B. VLAN 200 is used by engineering and spans sites A and C. Payroll and engineering are securely separated by provisioning separate point-to-point connections for each VLAN, each on a separate VCID. Service multiplexing at customer site A allows multiple virtual circuits to share the same port, yet provide secure connections to separate sites.

Figure 7: Point-to-Point Ethernet Services with 802.1Q Interfaces



All Traffic Service Using Q-in-Q Interface

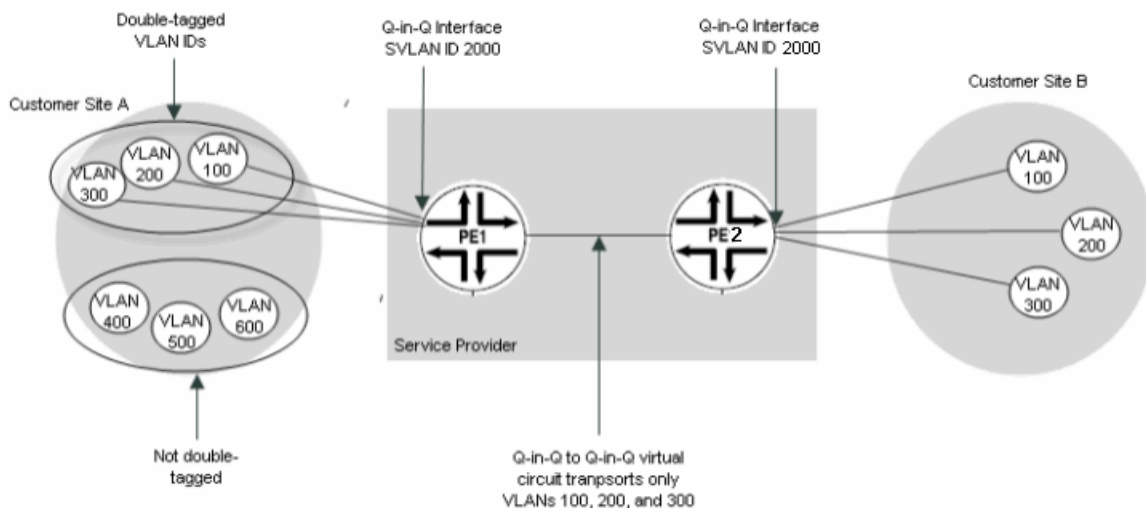
This type of point-to-point Ethernet (LDP) service uses Q-in-Q interfaces and transports all customer traffic from one site to another across the network. The Q-in-Q interface adds a service provider tag to the frame, which isolates the enterprise customer's VLAN tags. The service provider does not need knowledge of the customer's VLAN structure because all traffic is transported to the destination site.

Range of VLANs Service with Q-in-Q Interfaces

This type of point-to-point Ethernet (LDP) service uses Q-in-Q interfaces and carries a range of VLANs across the network. The service provider must establish with the enterprise customer which VLANs are to be transported. The service provider allocates a service provider VLAN ID as a second tag to the selected VLAN ID range, which isolates the traffic on selected VLANs from other traffic.

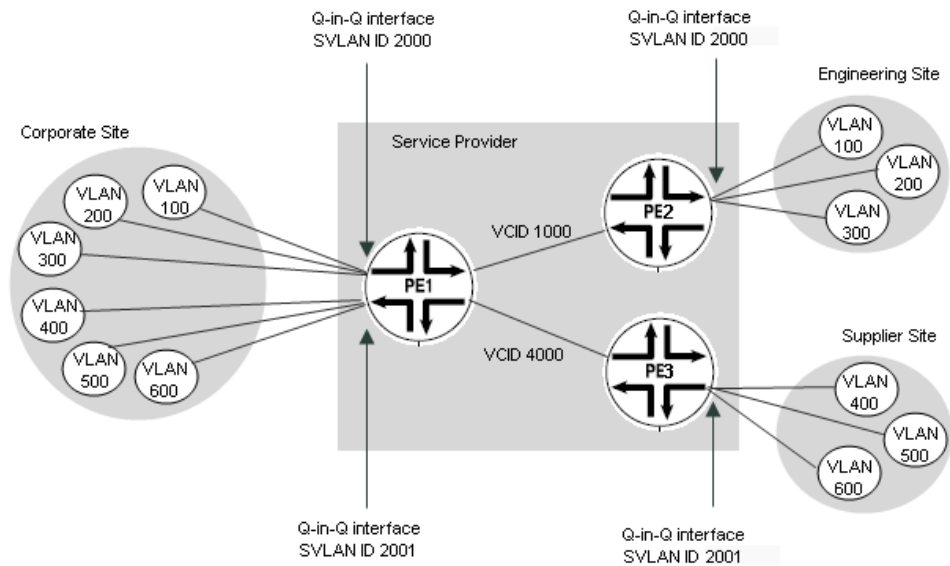
Figure 8 on page 58 shows an example in which an enterprise customer has six VLANs with VLAN IDs 100, 200, 300, 400, 500, and 600. The service is provisioned to carry only VLANs 100, 200, and 300 by tagging them with the service provider VLAN ID of 2000. VLANs 400, 500, and 600 do not cross the network.

Figure 8: Point-to-Point Ethernet Service with Q-in-Q Interfaces for Range of VLANs.



You can use separate service VLAN IDs to segregate traffic into secure groups of VLAN IDs. For example, VLANs 100, 200, and 300 might all be part of an enterprise's engineering organization, while VLANs 400, 500, and 600 might exchange information with suppliers. In this example, VLANs 100, 200, and 300 can be double-tagged with service VLAN ID 2000 and get transported only to the remote engineering site, while VLANs 400, 500, and 600 might be tagged with the service VLAN ID of 2001 and get transported only to the supplier's site along a separate pseudowire, as shown in Figure 9 on page 59.

Figure 9: Point-to-Point Ethernet Service with Q-in-Q Interfaces for Range of VLANs on Separate Service Provider VLANs



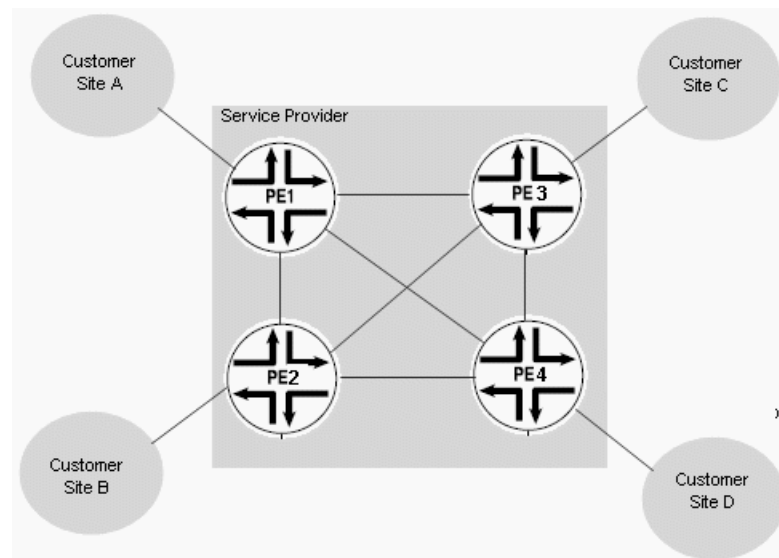
VPLS Services

The Connectivity Services Director application supports virtual private LAN service (VPLS), which in turn provides multipoint-to-multipoint services and point-to-multipoint services.

The Metro Ethernet Forum (MEF) refers to these connections as *E-LAN services*. See *Metro Ethernet Services – A Technical Overview* by Ralph Santitoro.

Figure 10 on page 59 shows an example of a multipoint service connecting four customer sites.

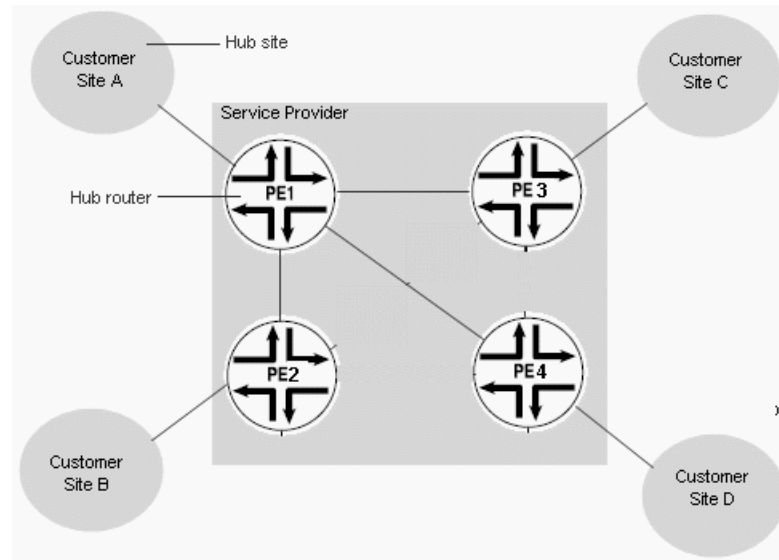
Figure 10: Multipoint-to-Multipoint VPLS Service—Full Mesh



This full mesh design enables direct communication among all PE routers in the service. This topology is efficient for services in which all sites need to communicate with all other sites.

[Figure 11 on page 60](#) shows a point-to-multipoint service with a single hub. The service provides connectivity between the hub router (PE1) and each of the spokes (PE2, PE3, and PE4), but no connectivity exists among the spokes.

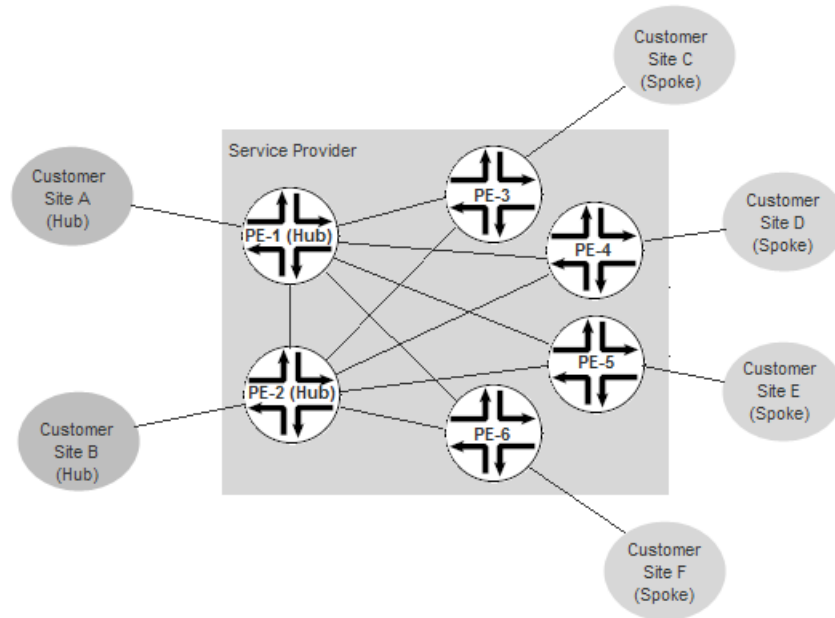
Figure 11: Point-to-Multipoint VPLS Service with Single Hub



This kind of topology is effective for services in which one site needs to communicate with all other sites, but communication among spokes is not required. For example, the hub site might house corporate headquarters, while each of the spoke sites is a region.

[Figure 12 on page 61](#) shows a point-to-multipoint service with two hubs. In this case, all spokes connect to both hubs.

Figure 12: Point-to-Multipoint VPLS Service with Multiple Hubs



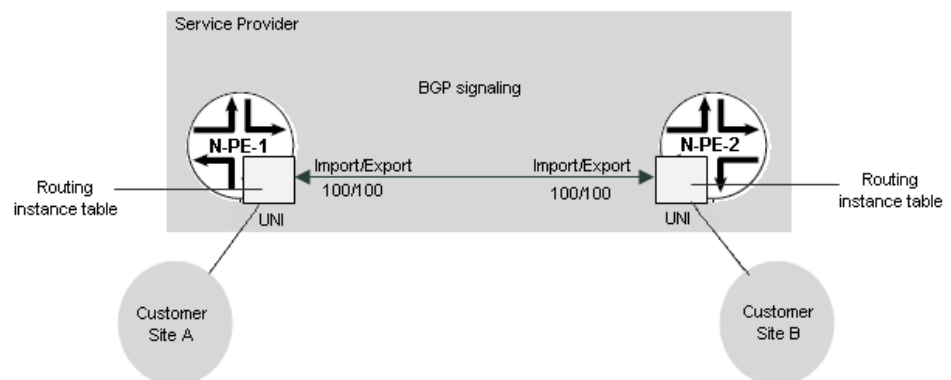
Typical use for dual hub routers is to provide redundancy in case of failure. For example, a data center might be duplicated at customer sites A and B, requiring access to both sites from each spoke for effective redundancy.

For all VPLS topologies, route targets and route distinguishers designate the multipoint connectivity among the participating endpoints.

Service Autodiscovery

BGP uses autodiscovery to establish connectivity among the N-PE routers quickly and efficiently. Figure 13 on page 61 shows an example.

Figure 13: Autodiscovery of Service Connectivity

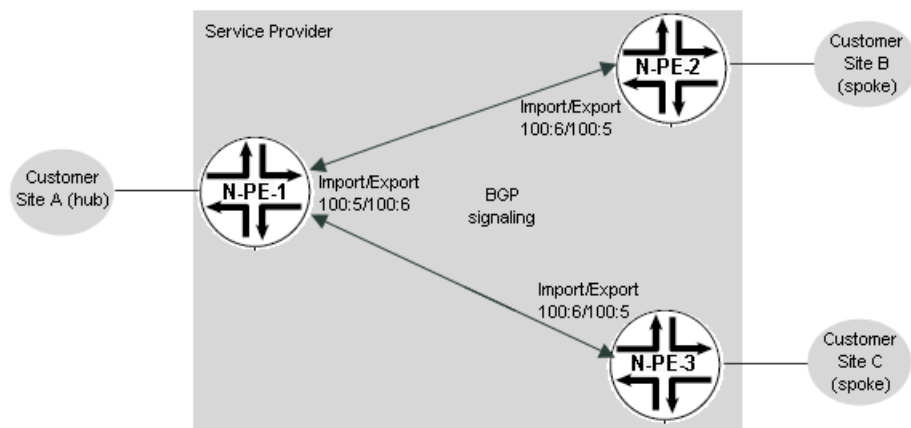


In this example, device N-PE-1 is the first to be added to the service. It exports route target 100 and imports route target 100. When N-PE-2 is added to the service, it also exports

and imports route target 100. The Junos OS on the device automatically makes the association and creates the connectivity path between the two devices. Similarly, when you add a third device to the service, so long as it exports/imports the same route targets as the N-PE devices in the existing service, the new device is added to the service and connectivity with both existing N-PE devices is established automatically.

For a point-to-multipoint service, route target/route distinguisher pairs have different values for import and export. These values for import and export are the same for all spokes, but reversed for the hub, thereby enabling communication between each spoke and the hub, but not among spokes. [Figure 14 on page 62](#) shows an example. In this case, device N-PE-1 (the hub router) exports route target:route distinguisher pair 100:6 and imports 100:5. Each spoke imports 100:6 and exports 100:5 enabling communication with the hub, but not with each other.

Figure 14: Autodiscovery in a Point-to-Multipoint Service



VPLS and Normalization

Similar to point-to-point Ethernet services, the UNIs of VPLS services can be port-to-port, 802.1Q, or Q-in-Q. The type of VLAN mapping—or normalization—is specified in the service definition. VLAN normalization applies only to MX Series devices.

Normalization supports automatic mapping of VLANs. Normalization performs operations on VLAN tags to achieve the desired translation. The Connectivity Services Director application supports the following forms of VLAN normalization:

- **Normalize to VLAN all**—The customer VLAN ID is preserved across the network. That is, the broadcast domain includes the interfaces that have the same VLAN ID across the VPLS service. For double-tagged packets (Q-in-Q interfaces), a pop operation at ingress strips the service VLAN ID from the packet. A corresponding push operation at egress inserts the service VLAN ID known at the local site. Hence, the service VLAN ID at egress does not have to match the service VLAN ID at ingress.

For single-tagged packets (802.1Q interfaces), “Normalize to VLAN all” has no effect, because the packet has no service VLAN ID to pop or push.

- **Normalize to VLAN none**—The customer VLAN ID is not preserved across the network. The broadcast domain includes all VLANs at any site provisioned in the service. For

single-tagged packets (802.1Q interfaces), a pop operation at ingress removes the customer VLAN ID from the packet. A corresponding push operation at egress adds a local customer VLAN ID.

For double-tagged packets (Q-in-Q interfaces), both customer VLAN ID and service VLAN ID are popped from the packet at ingress and pushed at egress.

- **Normalize to Dot1q tag**—The VLAN tag is preserved across the network. The broadcast domain includes all VLANs at any site provisioned in the service. For information about how frames are translated to provide the required VLAN tags for interfaces with different tag heights, see the section “VLAN Mapping for VPLS Services” in [“Understanding VLAN Manipulation \(Normalization and VLAN Mapping\) on Ethernet Services” on page 88](#).
- **Normalize to QinQ tags**—The inner VLAN tag and outer VLAN tag are preserved across the network. The broadcast domain includes all VLANs at any site provisioned in the service. For information about how frames are translated to provide the required VLAN tags for interfaces with different tag heights, see the section “VLAN Mapping for VPLS Services” in [“Understanding VLAN Manipulation \(Normalization and VLAN Mapping\) on Ethernet Services” on page 88](#).

Normalization works well with automatically assigned VLAN IDs, because the service provider does not need to specify the VLAN IDs that are popped and pushed. Without normalization, the service provider must specify explicitly the customer VLAN ID and the service VLAN ID.

- **Normalization not required**—If normalization is not used, then all customer VLAN IDs and all service VLAN IDs must match to be part of the same broadcast domain.



NOTE: For information on the VLAN normalization requirements for each Ethernet interface option, see the table in the topic [“Specifying Connectivity Information When Signaling Is BGP” on page 615](#)

Related Documentation

- [Junos Space Layer 3 Services Overview on page 64](#)
- [Provisioning Process Overview on page 65](#)
- [Seamless MPLS Support in Junos Space Overview on page 69](#)
- [Service Attributes Overview on page 71](#)

Junos Space Layer 3 Services Overview

To configure Layer 3 virtual private network (VPN) functionality, you must enable VPN support on the provider edge (PE) router. You must also configure any provider (P) routers that service the VPN, and you must configure the customer edge (CE) routers so that their routes are distributed into the VPN.

This topic covers:

- [Overview on page 64](#)
- [Layer 3 VPN Platform Support on page 64](#)
- [Layer 3 VPN Attributes on page 64](#)
- [Device Configuration for a Layer 3 VPN on page 65](#)

Overview

RFC 4364 VPNs are also known as BGP/MPLS VPNs because BGP is used to distribute VPN routing information across the provider's backbone, and MPLS is used to forward VPN traffic across the backbone to remote VPN sites.

Customer networks, because they are private, can use either public addresses or private addresses, as defined in RFC 1918, Address Allocation for Private Internets. When customer networks that use private addresses connect to the public Internet infrastructure, the private addresses might overlap with the same private addresses used by other network users. MPLS/BGP VPNs solve this problem by adding a VPN identifier prefix to each address from a particular VPN site, thereby creating an address that is unique both within the VPN and within the public Internet. In addition, each VPN has its own VPN-specific routing table that contains the routing information for that VPN only.

For this release, Junos Space Connectivity Services Director application enables you to provision Layer 3 VPN full mesh services.

For more information about Layer 3 VPNs, see the *Junos Software VPNs Configuration Guide*.

Layer 3 VPN Platform Support

Layer 3 VPNs are supported on most combinations of Juniper Networks routing platforms and PICs that are capable of running the Junos Software.

MX Series routers configured in Ethernet services mode can support some of the Junos OS Layer 3 VPN features. For Layer 3 VPNs, Ethernet services mode supports configuring a loopback interface for a VPN routing and forwarding (VRF) instance. You can configure up to two VRF instances in Ethernet services mode. Each VRF instance can handle up to 10,000 routes. The **ping mpls l3vpn** operational mode command is also supported.

Layer 3 VPN Attributes

Connectivity Services Director application supports the following Layer 3 VPN attributes. For more information, see the *Junos OS VPNs Configuration* technical documentation.

- **Target VPN**—Identifies a set of sites with a VPN to which a PE router distributes routes. This attribute is also called the *route target*. A PE egress router uses the route target to determine whether a received route is destined for a VPN that the router services.
- **Route distinguisher**—a 6-byte number that you can specify using one of the following formats:
 - *as-number:number*, where *as-number* is an AS number (a 2-byte value) and *number* is any 4-byte value. The AS number can be in the range 1 through 65,535. We recommend that you use an Internet Assigned Numbers Authority (IANA)-assigned, nonprivate AS number, preferably the Internet service provider's (ISP's) own or the customer's own AS number.
 - *ip-address:number*, where *ip-address* is an IP address (a 4-byte value) and *number* is any 2-byte value. The IP address can be any globally unique unicast address. We recommend that you use the address that you configure in the router-id statement, which is a nonprivate address in your assigned prefix range.

Device Configuration for a Layer 3 VPN

To implement Layer 3 VPNs in the JUNOS Software, you configure one routing instance for each VPN. You configure the routing instances on PE routers only. Each VPN routing instance consists of the following components:

- **VRF table**—On each PE router, you configure one VRF table for each VPN.
- **Set of interfaces that use the VRF table**—The logical interface to each directly connected CE router must be associated with a VRF table. You can associate more than one interface with the same VRF table if more than one CE router in a VPN is directly connected to the PE router.
- **Policy rules**—These control the import of routes into and the export of routes from the VRF table.
- **One or more routing protocols that install routes from CE routers into the VRF table**—You can use the BGP and OSPF routing protocols and static routes.

Related Documentation

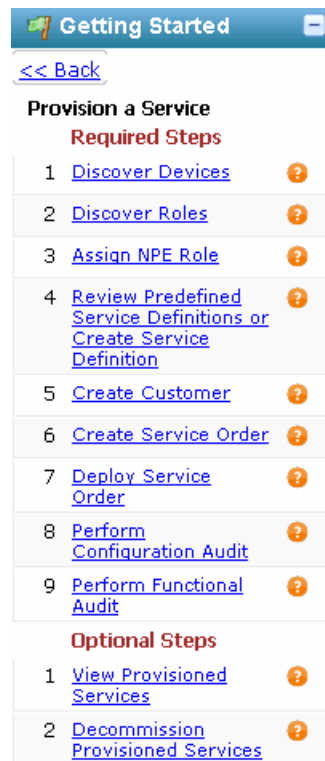
- [Junos Space Layer 2 Services Overview on page 55](#)
- [Provisioning Process Overview on page 65](#)
- [Seamless MPLS Support in Junos Space Overview on page 69](#)
- [Service Attributes Overview on page 71](#)

Provisioning Process Overview

Provisioning is a multistep process that makes services available to customers.

The following figure describes the steps involved in provisioning a service, including not only the provisioning work itself (steps 4 through 9), but also the steps that are necessary before you can begin the provisioning process (steps 1 through 3). The example in the figure shows the Service Provisioning operations.

Dividing the provisioning process into distinct activities allows you to use role-based access control to configure which type of user is allowed to perform each step.



Steps in the sequence are often performed by users with different levels of privilege. The Junos Space software provides predefined administrator roles that provide the necessary privilege for each step in the sequence:

- The Device Manager role allows an administrator to discover devices (step 1).
- The Service Manager role allows an administrator to perform device prestaging actions including discovering and assigning device roles (steps 2 and 3).
- The Service Designer role allows an administrator to create and publish a service definition (step 4).
- The Service Activator (less privileged) role allows an administrator to perform provisioning tasks including creating and managing customers, service orders, and services (steps 5 through 9).

For details about predefined administrator roles, see *Predefined Roles Overview* in the *Junos Space Network Application Platform User Guide*.

Network Operator Tasks—Provisioning Prerequisites

Network operators are usually responsible for performing the prerequisite tasks before the following service designer or service provisioner can perform their tasks:

- Discovering devices

- Launching role discovery
- Assigning N-PE roles

Discovering devices is the process for bringing your network devices under Junos Space management. Network operators who are assigned the Device Manager role can perform this task. See *Device Discovery Overview* in the *Junos Space Network Application Platform User Guide* for more information about discovering devices.

Launching role discovery and assigning N-PE roles are collectively known as prestaging tasks. Prestaging finds the N-PE devices among those already under Junos Space management and assigns appropriate MPLS N-PE roles to these devices and user-to-network interface (UNI) roles to their interfaces. Once these roles are established, the devices are ready for provisioning. Users who are assigned the Service Manager role can perform device role discovery and role assignment. See *Prestaging Devices Overview* for more information about prestaging devices.

Service Designer Tasks

The service designer is responsible for the creation and management of the service definitions that the service provisioner uses as the basis for creating a service order.

A service definition specifies the attributes that are common among a group of service orders that have similar service requirements. For example, a service definition might specify a port-to-port service, whether the associated VCID should be assigned automatically from a predefined pool or specified by the user, and what range of bandwidths can be assigned in the service order. The service definition also defines which attributes of the service can be edited in the service order.

The Junos Space Connectivity Services Director product provides several standard service definitions which support most needs. If the standard service definitions do not support your needs, then the service designer needs to create new, customized service definitions.

Users who are assigned the Service Designer role can create and manage service definitions.

Service Provisioner Tasks

Service provisioner tasks include the following:

- Creating the customer.
- Creating the service order.
- Deploying the service.
- Performing a configuration audit.
- Performing a functional audit.

A service order is an instance of the service definition that completes the definition for a specific customer's use. The service order always specifies the customer and the endpoints that link the customer sites through the MPLS network. For each endpoint, the service provisioner specifies the N-PE device and the UNI on that device that connects the

customer site to the N-PE device. The service order can also specify any additional attributes that are configured in the service definition as editable in the service order. These attributes might include the VCID, MTU for the UNI, MTU for the connection across the network, VLAN-ID, and bandwidth.

Deployment of a service order pushes a service to the network devices. Before deployment completes, a series of pre-validation checks takes place. If the pre-validation checks indicate that the service is valid, the deployment proceeds. If the pre-validation checks indicate an invalid service, the service provisioner must re-create the service order correctly before trying again to deploy it.

After the service is deployed, a functional audit establishes whether the service is up or down. If the functional audit reports that the service is up, the customer can begin using the service.

Once the service is active, the service provisioner can monitor the health of the service by running a functional audit or a configuration audit.

Users assigned the Service Activator role can perform these service provisioning tasks.

**Related
Documentation**

- *Discovering Devices* in the *Junos Space Network Application Platform User Guide*
- [Junos Space Layer 2 Services Overview on page 55](#)
- [Junos Space Layer 3 Services Overview on page 64](#)
- [Seamless MPLS Support in Junos Space Overview on page 69](#)
- [Service Attributes Overview on page 71](#)
- *Predefined Roles Overview* in the *Junos Space Network Application Platform User Guide*

Seamless MPLS Support in Junos Space Overview

MPLS-based Layer 2 services are growing in demand among enterprise and service providers, creating new challenges related to interoperability between Layer 2 and Layer 3 services for service providers who want to provide end-to-end value-added services. Service providers are able to expand service offerings, support multiple Layer 2 services and protocols at the same time, and to expand geographically by stitching different Layer 2 services to one another and to Layer 3 services, moving toward a seamless MPLS environment..

Interconnecting a Layer 2 VPLS network with a Layer 3 network enables the sharing of a service provider's core network infrastructure between IP and Layer 2 services, reducing the cost of providing those services. A Layer 2 MPLS circuit allows service providers to create a Layer 2 circuit service over an existing IP and MPLS backbone.

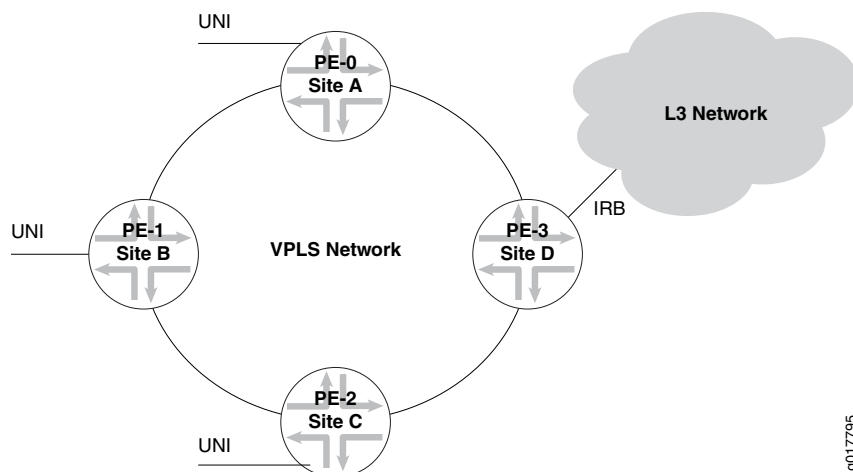
Service providers do not have to invest in separate Layer 2 equipment to provide Layer 2 services. A service provider can configure a provider edge router to run any Layer 3 protocol in addition to the Layer 2 protocols. Customers who prefer to maintain control over most of the administration of their own networks want Layer 2 circuit connections with their service provider instead of a Layer 3 VPN connection.

Using MPLS pseudowires makes it possible to encapsulate Layer 2 packets and extend Layer 2 services into Layer 3 networks. Junos Space supports the trend toward accomplishing Seamless MPLS with these two features:

- VPLS Access Into Layer 3 Networks
- Pseudowire Access Into a Layer 3 VPN

VPLS Access Into Layer 3 Networks

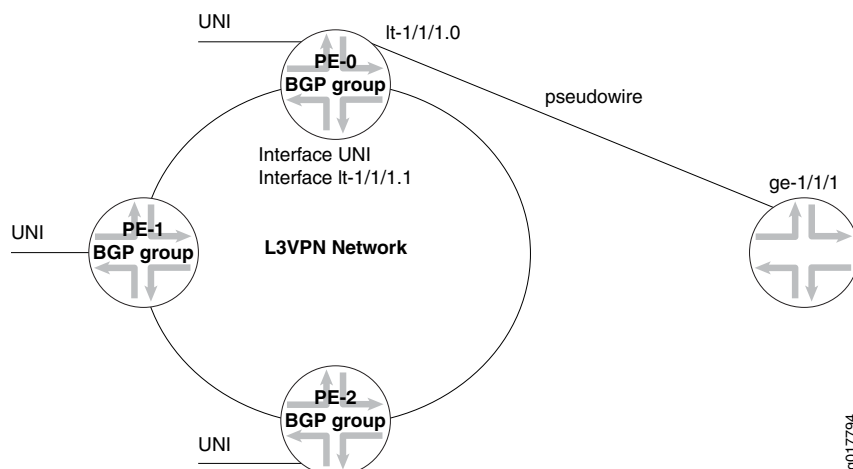
Integrated Routing and Bridging (IRB) provides simultaneous support for Layer 2 bridging and Layer 3 routing within the same bridge domain, and as well as in the same routing instance. If the IRB interface configured as a Layer 3 interface is being used in a routing instance, that routing instance will specifically declare it as routing-interface rather than regular VPLS interface (which acts like the interface on a specific VPLS Site). This feature requires a normalized VLAN (vlan-id=xxx which is the same as the unit name on which the inet4 address is specified)



Junos Space uses the two peer subinterfaces of the IRB to create the link between an existing VLAN and the Layer 3 network. An extra VPLS node is required to support the IRB interface which allows the rest of the VPLS nodes to be able to access all Layer 3 networks reachable through that interface. Providing the VPLS access into Layer 3 networks enhances basic VPLS services. Because this feature requires a normalized VLAN, it is available only on the Juniper Networks MX 3D Router series.

Pseudowire Access Into Layer 3 VPNs

While technically not a VPLS feature, Junos Space uses pseudowires, also known as pseudowire stitching, to link Layer 2 services together and to Layer 3 services. Pseudowire access into the L3 VPN enhances the standard Eline LDP and point-to-point services. The link into the L3VPN network can be port-based or VLAN-based. At least one node in the peer must be a logical tunnel (LT) interface. The peer must appear in the L3VPN configuration.



In Junos, this Layer 2 access into Layer 3 VPNs is accomplished by using a tunnel PIC to create a peer link between pseudowire and a Layer 3 network interface.

- Related Documentation**
- [Creating a Service Definition for VPLS Access into Layer 3 Networks on page 705](#)
 - [Creating a Service Order for VPLS Access into Layer 3 Networks on page 930](#)
 - *Example: Interconnecting a Layer 2 Circuit with a Layer 3 VPN*

Service Attributes Overview

A service is defined by a set of attributes. Some attributes are common to all service instances created from one service definition, and are therefore set during service definition time. Other attributes are specific to a service instance and must be set in the service order. Some attributes can be set either in the service definition or in the service order; in such cases it is up to the service designer to determine when the attribute will be set.

The Connectivity Services Director user interface groups service attributes as follows:

- **General attributes**—General information about the service, such as whether the service is point-to-point, multipoint-to-multipoint (full mesh VPLS), or point-to-multipoint VPLS, what signaling mechanism is used in the network core, whether quality of service (QoS) is enabled on the service, and who the enterprise customer is who uses the service.
- **Connectivity settings**—Information about connectivity among customer sites through the network. For point-to-point Ethernet services in a network with LDP switching in the network core, these settings include the VC ID. For multipoint Ethernet (or VPLS) services, these settings include the route target and route distinguisher.
- **Advanced settings**—Information about advanced connectivity among customer sites through the network. For multipoint Ethernet (or VPLS) services, these settings include tunnel services, local switching, fast-reroute-priority, label block size, and connection type.
- **UNI settings**—Information about each customer site, including the N-PE device and interface the site uses to connect to the network, the encapsulation method used (physical and logical), MTU, customer VLAN ID and range, service VLAN ID, bandwidth limiting, and so on.

General Attributes

The following general attributes are defined for each service:

- [Service Type on page 72](#)
- [Signaling on page 72](#)
- [Comments on page 72](#)
- [Service Template on page 72](#)
- [Threshold Alarm Profile on page 72](#)
- [Interface Type on page 72](#)
- [Enabling Additional Features on page 72](#)

- [Customer on page 73](#)
- [Enable QoS on page 73](#)

Service Type

The **Service type** attribute specifies a network topology to include in the service definition.

The service type is the first attribute to be determined during service definition. It can be one of the following values:

- Point-to-point Ethernet—Virtual circuit between two customer sites in the network core.
- Multipoint-to-multipoint Ethernet (VPLS) —Virtual private LAN service (VPLS) among multiple customer sites in the network core to provide full mesh connectivity.
- Point-to-multipoint Ethernet (VPLS) —VPLS among multiple customer sites in the network core to provide connectivity between a hub site and multiple spoke sites.

Signaling

The **Signaling** attribute specifies the protocol that controls signaling in the network core. You can select BGP or LDP.

Comments

The **Comments** attribute .

Service Template

The **Service Template** attribute .

Threshold Alarm Profile

The **Threshold Alarm Profile** attribute.

Interface Type

The **Interface type** attribute . You can specify one of the following:

- Ethernet
- TDM
- ATM

Enabling Additional Features

In addition to the interface type, depending on the **Service type** topology and **Signaling** you specify, you can enable the following features for a service:

- **Static pseudowire**—For networks that do not support LDP or do not have LDP enabled. You define pseudowires by configuring static values for the inbound and outbound labels of the connection.
- **Enable PW access to L3 VPN networks**

- **Enable L3 Access**
- **Enable PW Extension**
- **Enable PW Resiliency**
- **Decouple Service Status from Port Status**—Isolates events related to an interface in the OpenNMS database. Only traps related to pseudowires are monitored.

Customer

This attribute specifies the enterprise customer who will use the service instance. This attribute is always specified in the service order.

Enable QoS

This attribute specifies whether QoS is enabled on the service to divide traffic into classes and offer various levels of throughput and packet loss when congestion occurs. When you enable QoS in the service definition, the QoS Settings box appears when you configure the service order.



NOTE: When you enable QoS in the service definition, bandwidth settings are also configurable in the service order.



NOTE: A QoS profile that specifies a level-three scheduler is not supported on port-to-port services. Only non-hierarchical port scheduler profiles are supported.

UNI Settings

The following attributes are defined for the service endpoints or customer sites that are connected by the service:

- [Ethernet Options on page 74](#)
- [Interface on page 74](#)
- [MTU on page 74](#)
- [Customer Traffic Type on page 74](#)
- [Customer VLAN ID on page 75](#)
- [Service VLAN ID and VLAN ID Range on page 75](#)
- [Physical Encapsulation on page 75](#)
- [Logical Encapsulation on page 76](#)
- [Rate Limiting and Bandwidth on page 77](#)
- [UNI Settings for TDM Interfaces on page 77](#)
- [UNI Settings for ATM Interfaces on page 77](#)

Ethernet Options

This attribute identifies the interface type at the endpoint by defining the level of packet tagging for the UNI. It can have the following values:

- asymmetric tag depth

Allows port-based, 802.1Q and Q-in-Q interfaces for UNIs to coexist in a service.

- port-port

Transfers all data from the UNI to the other end of the LSP trunk.

- dot1q

An 802.1Q interface that tags each packet with a VLAN ID, thus allowing a specific VLAN to traverse the network.

- qinq

A Q-in-Q interface that double tags each frame. The inner tag is added by the service provider. The service provider can use this inner tag to differentiate among services. For example, you can configure VLANs for a customer's intranet with a different inner tag from VLANs used for working with providers or partners.

Interface

Specifies the physical interface on the N-PE device that connects the customer site or CE device to the N-PE device.

MTU

The maximum transmission unit (MTU) represents the largest frame size, in bytes, that passes through the UNI. MTU is configurable.



.....
NOTE: This value is distinct from the MTU assigned to the connectivity in the network core.
.....

Customer Traffic Type

This attribute places restrictions on the traffic that can be transported across the network by the associated service. It can have the following values:

- Transport single VLAN

Restricts the associated service to transporting just one VLAN across the network. You can use this option with 802.1Q and Q-in-Q interface types.

- Transport VLAN range

Allows the associated service to transport a range of VLANs across the network. You can use this option with 802.1Q and Q-in-Q interface types.

- Transport all traffic

Allows the associated service to transport all traffic across the network. You can use this option with Q-in-Q interface types only.

The traffic type attribute is not applicable to port-to-port services. Port-to-port services always transport all traffic.

Customer VLAN ID

Specifies a VLAN ID that is attached to each packet to permit VLANs to be shared across the network.

This attribute can be used only with 802.1Q and Q-in-Q interface types.

Service VLAN ID and VLAN ID Range

The service VLAN ID (VLAN ID) specifies a second level of tagging to segregate groups of VLANs.

The VLAN range specifies a range of VLANs to be transported across the network by associating them with a service VLAN ID.

These options are configurable only for Q-in-Q interfaces.

Physical Encapsulation

Specifies the physical link-layer encapsulation type.

- **flexible-ethernet-services**—Offers the most flexibility, depending on the characteristics of the N-PE device and its line modules.

For Gigabit Ethernet IQ interfaces and Gigabit Ethernet PICs with small form-factor pluggable transceivers (SFPs) only, use flexible Ethernet services encapsulation when you want to configure multiple per-unit Ethernet encapsulations. This encapsulation type allows you to configure any combination of route, TCC, CCC, and VPLS encapsulations on a single physical port. Aggregated Ethernet bundles cannot use this encapsulation type. If you configure flexible Ethernet services encapsulation on the physical interface, VLAN IDs from 1 through 511 are no longer reserved for normal VLANs.

In the Junos Space Connectivity Services Director product, you can use this encapsulation type with 802.1Q interfaces and Q-in-Q interfaces in point-to-point Ethernet services and in multipoint Ethernet services.

- **vlan-ccc**—You can use Ethernet VLAN encapsulation on CCC interfaces. This option restricts the range of available VLAN IDs to 512 through 4094. VLAN IDs 1 through 511 are reserved for internal use.

In the Junos Space Connectivity Services Director product, you can use this encapsulation type with 802.1Q interfaces and Q-in-Q interfaces in point-to-point services.

- **extended-vlan-ccc**—Use extended VLAN encapsulation on CCC interfaces with Gigabit Ethernet interfaces that must accept packets carrying 802.1Q values.

In the Junos Space Connectivity Services Director product, you can use this encapsulation type with 802.1Q interfaces and Q-in-Q interfaces in point-to-point services.

- **ethernet-vpls**—Use Ethernet VPLS encapsulation on Ethernet interfaces that have VPLS enabled and that must accept packets carrying standard TPID values.

In the Junos Space Connectivity Services Director product, this encapsulation is used only for dedicated port interface types in multipoint Ethernet services.

Logical Encapsulation

Specifies the logical link-layer encapsulation type. Logical encapsulation with 802.1Q interfaces allows you to route multiple services through the same physical interface.

- **vlan-ccc**—Use Ethernet virtual LAN (VLAN) encapsulation on CCC interfaces. When you use this encapsulation type, you can configure the family ccc only.
- **extended-vlan-ccc**—Use extended VLAN encapsulation on CCC interfaces with Gigabit Ethernet interfaces that must accept packets carrying 802.1Q values.
- **vlan-vpls**—Use VLAN VPLS encapsulation on Ethernet interfaces with VLAN tagging and VPLS enabled. Interfaces with VLAN VPLS encapsulation accept packets carrying standard Tag Protocol (TPID) values only.

[Table 6 on page 76](#) defines the logical encapsulation types that are valid for each physical encapsulation type in a point-to-point Ethernet service.

Table 6: Physical and Logical Encapsulation Compatibilities in Point-to-Point Ethernet Services

Physical Encapsulation	Logical Encapsulation	Valid Interface Types
flexible-ethernet-services	vlan-ccc	802.1Q and Q-in-Q
vlan-ccc	vlan-ccc	802.1Q and Q-in-Q
extended-vlan-ccc	extended-vlan-ccc	802.1Q and Q-in-Q
ethernet-ccc	not applicable	dedicated port

[Table 7 on page 76](#) defines the logical encapsulation types that are valid for each physical encapsulation type in multipoint Ethernet services.

Table 7: Physical and Logical Encapsulation Compatibilities in Multipoint Ethernet (VPLS) Services

Physical Encapsulation	Logical Encapsulation	Valid Interface Types
flexible-ethernet-services	vlan-vpls	802.1Q and Q-in-Q
ethernet-vpls	not applicable	dedicated port

Rate Limiting and Bandwidth

Rate limiting allows you to specify the maximum bandwidth permitted for a service.

The burst rate is automatically calculated as two times the MTU of the UNI.



NOTE: When a service is QoS enabled, you can also configure rate limiting and bandwidth in the service.

UNI Settings for TDM Interfaces

The following TDM options are configurable for TDM interfaces:

- **Physical IF encapsulation**—satop or cesopsn
- **Jitter buffer**
M Series: 1 through 340
- **Idle pattern**—0 through 255
- **Excessive packet loss rate**—1 through 100%
- **Payload size**
M Series: 64 through 1024

UNI Settings for ATM Interfaces

The following ATM options are configurable for ATM interfaces:

- **Physical IF encapsulation**—The type of encapsulation to apply to the interface. Use atm-ccc-cell-relay for ATM cell relay encapsulation. Use atm-ccc-cell-mux for ATM VC for CCC.
- **VPI selection**—The virtual path identifier
- **VCI selection**—This integer uniquely identifies the virtual circuit that the service uses.
- **Cell bundle size**—Cell bundle size can be 1 through 34.

Connectivity Settings

The following attributes are defined for the connectivity among UNI endpoints across the network:

- [Virtual Private LAN Service Identifier \(VPLS ID\) on page 78](#)
- [Auto Discovery on page 78](#)
- [Virtual Circuit Identifier \(VCID\) \(Point-to-Point Services Only\) on page 78](#)
- [Route Targets and Route Distinguishers on page 78](#)
- [Normalized VLAN \(Multipoint Services Only\) on page 78](#)
- [MAC Learning on page 79](#)

Virtual Private LAN Service Identifier (VPLS ID)

This VPLS ID is available if the signaling is LDP and the Auto Discovery check box is disabled. The VPLS ID can be selected automatically or manually. The VPLS ID identifies the virtual circuit identifier used for the VPLS routing instance.

Auto Discovery

The Auto Discovery check box is available only if the signaling is LDP. If you enable Auto Discovery, the attributes Route target, Route distinguisher, and VPN ID appear and are provisionable.

Virtual Circuit Identifier (VCID) (Point-to-Point Services Only)

This unique identifier can be assigned automatically from a pool of VCIDs or can be manually specified. It uniquely identifies a point-to-point virtual circuit through the network and is provided for all switched point-to-point services.

Route Targets and Route Distinguishers

Route targets and route distinguishers are applied to point-to-point services in which BGP controls the connections in the network core.

Route targets and route distinguishers are always automatically generated by the Junos Space software for multipoint Ethernet (VPLS) services. Route targets and route distinguishers designate the multipoint connectivity among the participating endpoints of a multipoint service. They identify the members of the virtual LAN.

Normalized VLAN (Multipoint Services Only)

Similar to point-to-point Ethernet services, the UNIs of VPLS services can be port-to-port, 802.1Q, or Q-in-Q. The type of VLAN mapping—or normalization—is specified in the service definition. VLAN normalization applies only to MX Series devices.

Normalization supports automatic mapping of VLANs and performs operations on VLAN tags to achieve the desired translation. The Connectivity Services Director application supports the following forms of VLAN normalization:

- **Normalize to VLAN all**—The customer VLAN ID is preserved across the network. That is, the broadcast domain includes the interfaces that have the same VLAN ID across the VPLS service. For double-tagged packets (Q-in-Q interfaces), a pop operation at ingress strips the service VLAN ID from the packet. A corresponding push operation at egress inserts the service VLAN ID known at the local site. Hence, the service VLAN ID at egress does not have to match the service VLAN ID at ingress.

For single-tagged packets (802.1Q interfaces), "Normalize to VLAN All" has no effect, because the packet has no service VLAN ID to pop or push.

- **Normalize to VLAN none**—The customer VLAN ID is not preserved across the network. The broadcast domain includes all VLANs at any site provisioned in the service. For single-tagged packets (802.1Q interfaces), a pop operation at ingress removes the customer VLAN ID from the packet. A corresponding push operation at egress adds a local customer VLAN ID.

For double-tagged packets (Q-in-Q interfaces), both customer VLAN ID and service VLAN ID are popped from the packet at ingress and pushed at egress.

- **Normalize to Dot1q tag**—The VLAN tag is preserved across the network. The broadcast domain includes all VLANs at any site provisioned in the service. For information about how frames are translated to provide the required VLAN tags for interfaces with different tag heights, see the section “VLAN Mapping for VPLS Services” in *Understanding VLAN Manipulation (Normalization and VLAN Mapping) on Ethernet Services*.
- **Normalize to QinQ tags**—The inner VLAN tag and outer VLAN tag are preserved across the network. The broadcast domain includes all VLANs at any site provisioned in the service. For information about how frames are translated to provide the required VLAN tags for interfaces with different tag heights, see the section “VLAN Mapping for VPLS Services” in *Understanding VLAN Manipulation (Normalization and VLAN Mapping) on Ethernet Services*.
- **Normalization not required**—For port-to-port services only. Specifies that normalization is not used.

If normalization is not used, then all customer VLAN IDs and all service VLAN IDs must match to be part of the same broadcast domain. Services with dedicated port interfaces cannot use normalization.

Normalization works well with automatically assigned VLAN IDs, because the service provider does not need to specify the VLAN IDs that are popped and pushed. Without normalization, the service provider must specify explicitly the customer VLAN ID and the service VLAN ID.



NOTE: For a description of how the Connectivity Services Director application manipulates VLANs, see *Understanding VLAN Manipulation (Normalization and VLAN Mapping) on Ethernet Services*.

MAC Learning

You can enable MAC learning for a virtual switch, for a bridge domain, for a specific logical interface in a bridge domain, or for a set of bridge domains associated with a Layer 2 trunk port. MAC learning is enabled by default.

When MAC learning is enabled, you can configure the following settings:

Interface MAC Limit

You can specify the maximum number of media access control (MAC) addresses that can be learned by the VPLS routing instance. You can configure the same limit for all interfaces configured for a routing instance. You can also configure a limit for a specific interface. The default is 1024 addresses. The range is 16 through 65,536 MAC addresses. This option is supported for MX-series routers only.

MAC Statistics

You can enable MAC accounting either for a specific bridge domain, or for a set of bridge domains associated with a Layer 2 trunk port. MAC statistics is disabled by default. This option is supported for MX-series routers only.

MAC Table Size

You can modify the size of the MAC address table for the bridge domain, a set of bridge domains associated with a trunk port, or a virtual switch. The default is 5120 MAC addresses.

Advanced Settings

The following attributes are defined for advanced connectivity among UNI endpoints across the network:

- [Tunnel Services on page 80](#)
- [Local Switching on page 80](#)
- [Fast Reroute Priority on page 80](#)
- [Label Block Size on page 81](#)
- [Connectivity Type on page 81](#)

Tunnel Services

You can enable tunnel services to specify that traffic for particular VPLS routing instances be forwarded to specific virtual tunnel (VT) interfaces, allowing you to load-balance VPLS traffic among all the available VT interfaces on the router.

Tunnel services are disabled by default.

Local Switching

In local switching mode, you can terminate multiple Layer 2 circuit pseudowires at a single VPLS mesh group.

Local switching is disabled by default.



NOTE: In a point-to-multipoint topology, you must enable local switching on the hub router and disable local switching on the spokes.

Fast Reroute Priority

Specify the fast reroute priority for a VPLS routing instance. You can configure high, medium, or low fast reroute priority to prioritize specific VPLS routing instances for faster convergence and traffic restoration. Because the router repairs next hops for high-priority VPLS routing instances first, the traffic traversing a VPLS routing instance configured with high fast reroute priority is restored faster than the traffic for VPLS routing instances configured with medium or low fast reroute priority. The default setting is LOW.

Label Block Size

VPLS MPLS packets have a two-label stack. The outer label is used for normal MPLS forwarding in the service provider's network. If BGP is used to establish VPLS, the inner label is allocated by a PE router as part of a label block. One inner label is needed for each remote VPLS site. Four sizes are supported. We recommend using the default size of 8, unless the network design requires a different size for optimal label usage, to allow the router to support a larger number of VPLS instances.

If you allocate a large number of small label blocks to increase efficiency, you also increase the number of routes in the VPLS domain. This has an impact on the control plane overhead.

Changing the configured label block size causes all existing pseudowires to be deleted. For example, if you configure the label block size to be 4 and then change the size to 8, all existing label blocks of size 4 are deleted, which means that all existing pseudowires are deleted. The new label block of size 8 is created, and new pseudowires are established.

Four label block sizes are supported: 2, 4, 8, and 16. Consider the following scenarios:

- 2—Allocate the label blocks in increments of 2. For a VPLS domain that has only two sites with no future expansion plans.
- 4—Allocate the label blocks in increments of 4.
- 8 (default)—Allocate the label blocks in increments of 8.
- 16—Allocate the label blocks in increments of 16. A label block size of 16 enables you to minimize the number of routes in the VPLS domain. Use this setting only if the number of routes is the most important concern.

Connectivity Type

You can configure the VPLS routing instance to take down or maintain its VPLS connections depending on the status of the interfaces configured for the VPLS routing instance. By default, the VPLS connection is taken down whenever a customer-facing interface configured for the VPLS routing instance fails. This behavior is explicitly configured by specifying the `ce` option. You can alternatively specify the `irb` option to ensure that the VPLS connection remain up so long as an integrated routing and bridging (IRB) interface is configured for the VPLS routing instance.

Node Settings

Nodes refer to the devices or network elements that are used in establishing a network connection for a particular protocol. You can define configuration parameters and attributes that are common and apply to several nodes in your topology in a single, one-step task by selecting such nodes or devices and specifying the common definitions. Some of the settings need to be unique for each node, and in such cases, you can specify or modify such properties individually for each node. After you select the nodes that need to be associated with a service definition or order, you can select the interfaces corresponding to each device to define the interface-specific characteristics or capabilities. Node-wise parameters provide a quick, effective mechanism for applying configurations

on devices. You can select one or more devices from the list of displayed devices that are previously configured for management by the Connectivity Services Director database. After you select the devices and add them, they are mapped with the service definition. The following attributes can be configured as node-level settings, depending on the type of service order, such as Layer 3 VPN or VPLS:

Static Routes

Routes that are permanent fixtures in the routing and forwarding tables are often configured as static routes. These routes generally do not change, and often include only one or very few paths to the destination. To create a static route in the routing table, you must, at minimum, define the route as static and associate a next-hop address with it. The static route in the routing table is inserted into the forwarding table when the next-hop address is reachable. All traffic destined for the static route is transmitted to the next-hop address for transit. You can specify options that define additional information about static routes that is included with the route when it is installed in the routing table. All static options are optional. A router uses static routes in the following scenarios:



NOTE: Although you can configure next-hop tables using service templates, you can configure only next-hop addresses in the service order.

When it does not have a route to a destination that has a better (lower) preference value.

When it cannot determine the route to a destination.

When it is forwarding unroutable packets.

For the destination prefix of the static route, you must specify the destination of the route (in route destination-prefix) in one of the following ways:

network/mask-length, where network is the network portion of the IP address and mask-length is the destination prefix length.

default if this is the default route to the destination. This is equivalent to specifying an IP address of 0.0.0.0/0.



NOTE: IPv4 packets with a destination of 0.0.0.0 (the obsoleted limited broadcast address) and IPv6 packets with a destination of 0::0 are discarded by default. To forward traffic destined to these addresses, you can add a static route to 0.0.0.0/32 for IPv4 or 0::0/128 for IPv6.

For the next-hop portion of the static route, you must configure the IPv4, IPv6, or ISO network address of the next hop or the name of the interface on which to configure an independent metric or preference for a static route.

PIM Settings

Protocol Independent Multicast (PIM) emerged as an algorithm to overcome the limitations of dense-mode protocols such as the Distance Vector Multicast Routing

Protocol (DVMRP), which was efficient for dense clusters of multicast receivers, but did not scale well for the larger, sparser, groups encountered on the Internet. The Core Based Trees (CBT) Protocol was intended to support sparse mode as well, but CBT, with its all-powerful core approach, made placement of the core critical, and large conference-type applications (many-to-many) resulted in bottlenecks in the core. PIM was designed to avoid the dense-mode scaling issues of DVMRP and the potential performance issues of CBT at the same time. PIM operates in several modes: bidirectional mode, sparse mode, dense mode, and sparse-dense mode. In sparse-dense mode, some multicast groups are configured as dense mode (flood-and-prune, [S,G] state) and others are configured as sparse mode (explicit join to rendezvous point [RP], [*G] state). To join the shared tree, or rendezvous-point tree (RPT) as it is called in PIM sparse mode, the router must do the following: Determine the IP address of the RP for that group. Determining the address can be as simple as static configuration in the router, or as complex as a set of nested protocols.

- Build the shared tree for that group. The router executes an RPF check on the RP address in its routing table, which produces the interface closest to the RP. The router now detects that multicast packets from this RP for this group need to flow into the router on this RPF interface.
- Send a join message out on this interface using the proper multicast protocol (probably PIM sparse mode) to inform the upstream router that it wants to join the shared tree for that group. This message is a (*G) join message because S is not known. Only the RP is known, and the RP is not actually the source of the multicast packets. The router receiving the (*G) join message adds the interface on which the message was received to its outgoing interface list (OIL) for the group and also performs an RPF check on the RP address. The upstream router then sends a (*G) join message out from the RPF interface toward the source, informing the upstream router that it also wants to join the group.

You can specify the following attributes: PIM mode on the interface. The choice of PIM mode is closely tied to controlling how groups are mapped to PIM modes, as follows: bidirectional-sparse—Use if all multicast groups are operating in bidirectional, sparse, or SSM mode. bidirectional-sparse-dense—Use if multicast groups, except those that are specified in the dense-groups statement, are operating in bidirectional, sparse, or SSM mode. dense—Use if all multicast groups are operating in dense mode. sparse—Use if all multicast groups are operating in sparse mode or SSM mode. sparse-dense—Use if multicast groups, except those that are specified in the dense-groups statement, are operating in sparse mode or SSM mode

Name of the interface on which PIM must be enabled. Specify the full interface name, including the physical and logical address components.

Configure the routing device as an actual or potential rendezvous point (RP). A routing device can be an RP for more than one group.

Name of the interface on the device that functions as the RP.

Address ranges for the multicast groups for which the routing device is the RP. By default, a routing device running PIM is eligible to be the RP for all IPv4 or IPv6 groups (224.0.0.0/4

or FF70::/12 to FFF0::/12). The following example limits the groups for which this routing device can be the RP.

MVPN Settings

Multiprotocol BGP-based multicast VPNs (also referred to as next-generation Layer 3 VPN multicast) constitute the next evolution after dual multicast VPNs (draft-rosen) and provide a simpler solution for administrators who want to configure multicast over Layer 3 VPNs. For MBGP MVPNs (also referred to as next-generation Layer 3 multicast VPNs), the default mode of operation supports only intersite shortest-path trees (SPTs) for customer PIM (C-PIM) join messages. It does not support rendezvous-point trees (RPTs) for C-PIM join messages. The default mode of operation provides advantages, but it requires either that the customer rendezvous point (C-RP) be located on a PE router or that the Multicast Source Discovery Protocol (MSDP) be used between the C-RP and a PE router so that the PE router can learn about active sources advertised by other PE routers. If the default mode is not suitable for your environment, you can configure RPT-SPT mode (also known as shared-tree data distribution), as documented in section 13 of the BGP-MVPN draft (draft-ietf-l3vpn-2547bis-mcast-bgp-00.txt). RPT-SPT mode supports the native PIM model of transmitting (*,G) messages from the receiver to the RP for intersite shared-tree join messages. This means that the type 6 (*,G) routes get transmitted from one PE router to another. In RPT-SPT mode, the shared-tree multicast routes are advertised from an egress PE router to the upstream router connected to the VPN site with the C-RP. The single-forwarder election is performed for the C-RP rather than for the source. The egress PE router takes the upstream hop to advertise the (*,G) and sends the type 6 route toward the upstream PE router. To send the data on the RPT, either inclusive or selective provider tunnels can be used. After the data starts flowing on the RPT, the last-hop router switches to SPT mode, unless you include the spt-threshold infinity statements in the configuration.

You can specify the following parameters:

- Indicate whether the shared-tree data distribution mode or the shortest path tree only (SPT-only) mode of MVPN must be enabled to learn about active multicast sources using multicast VPN source-active routes. the default mode of operation is shortest path tree only (SPT-only) mode. In SPT-only mode, the active multicast sources are learned through multicast VPN source-active routes. This mode of operation is described in section 14 of the BGP-MVPN draft (draft-ietf-l3vpn-2547bis-mcast-bgp-00.txt).
- Specify the export and import targets specified specifically for sender sites or receiver sites, or can be borrowed from a configured unicast route target. Note that a sender site export route target is always advertised when security association routes are exported. By default, the VPN routing and forwarding (VRF) import and export route targets (configured either using VRF import and export policies or using the vrf-target statement) are used for importing and exporting routes with the MBGP MVPN network layer reachability information (NLRI). You can use the export-target and import-target options to override the default VRF import and export route targets.
- Specify the export target to enable you to override the Layer 3 VPN import and export route targets used for importing and exporting routes for the MBGP MVPN network layer reachability information (NLRI).
- Specify the target value when importing sender and receiver site routes.

- Specify a unicast target community as the import target while importing sender and receiver site routes.
- Specify if you want to enable automatic selection of an export target if a configuration is not provided. An imported automatic discovery route is treated as belonging to both the sender site set and the receiver site set.
- Specify the export and import target community names.
- Specify the provider tunnel name to configure virtual private LAN service (VPLS) flooding of unknown unicast, broadcast, and multicast traffic using point-to-multipoint LSPs. Also configure point-to-multipoint LSPs for MBGP MVPNs.
- Specify the site type of the MBGP MVPN. An MBGP MVPN defines two types of site sets, a sender site set and a receiver.
- Configure the upstream multicast hop (UMH) to denote a router to use the unicast route preference to determine the single forwarder election.

MAC Settings

You can specify the following attributes related to the MAC application of a node:

Enable or disable MAC learning for all logical interfaces in a specified bridge domain, or for a specific logical interface in a bridge domain. Disabling dynamic MAC learning prevents the specified interfaces from learning source MAC addresses. A limit on the number of MAC addresses learned from a specific bridge domain or from a specific logical interface that belongs to a bridge domain. For an access port, the default limit on the maximum number of MAC addresses that can be learned on an access port is 1024. For a trunk port, the default limit on the maximum number of MAC addresses that can be learned on a trunk port is 8192.

Enable or disable packet accounting either for a router or switch as a whole or for a specific VLAN. After you enable packet accounting, the Junos OS maintains packet counters for each MAC address learned. By default, MAC accounting is disabled. Size of the MAC address table for each VLAN. The default table size is 5120 addresses. The minimum you can configure is 16 addresses, and the maximum is 1,048,575 addresses. If the MAC table limit is reached, new addresses can no longer be added to the table. Unused MAC addresses are removed from the MAC address table automatically. This frees space in the table, allowing new entries to be added.

Topology Settings

Automatically assign a route distinguisher to the routing instance. Alternatively, specify the route distinguisher manually by specifying an identifier attached to a route, enabling you to distinguish to which VPN or VPLS the route belongs. Each routing instance must have a unique route distinguisher associated with it. The route distinguisher is used to place bounds around a VPN so that the same IP address prefixes can be used in different VPNs without having them overlap.

Related Documentation

- [Junos Space Layer 2 Services Overview on page 55](#)
- [Junos Space Layer 3 Services Overview on page 64](#)

- [Provisioning Process Overview on page 65](#)
- [Seamless MPLS Support in Junos Space Overview on page 69](#)

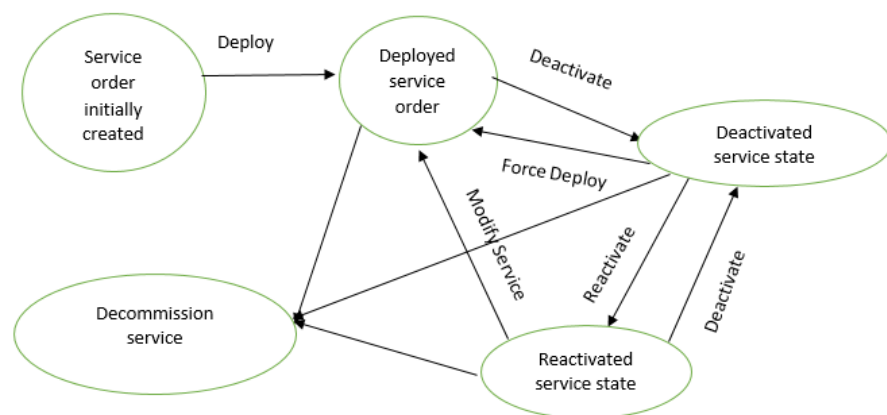
Service Order States and Service States Overview

Service provisioners create service orders which are requests to provision a service, validate a service, or decommission a service. The service order for provisioning a service defines all the service attributes.

Service Order States

Before a service order can affect a service, it must transition through several states as shown in [Figure 15 on page 86](#).

Figure 15: Service Order States and State Transitions



When the service provisioner has created the service order, but has not yet attempted to deploy it or schedule it for deployment, the service order is in the Draft state (also, formerly, called Requested state).

After the service provisioner has scheduled the service order for deployment, the service order transitions to the Scheduled state. If the service provisioner schedules the service order for immediate deployment, then the service order will be in the Scheduled state only briefly. However, if the service provisioner has scheduled a later deployment, the service order could be in this state for several hours or days.

When a scheduled service order reaches its time for deployment, it transitions to the transitory In Progress state. From this state, the Junos Space software attempts to deploy the service. Successful deployment transitions the service order to the Completed state.

If the Junos Space software cannot deploy the service because of invalid information in the service order itself, the service order enters the Invalid state. The service provisioner

must resolve the issues that cause the failure before re-creating the service order and rescheduling it for deployment.

If the device is down or the Junos Space software is unable to push the service configuration to the device, the service order transitions to the Failed Deploy state. A network operator might need to resolve the problem before the service provisioner reschedules the service order.

After you disable a service order to deactivate the configuration settings on devices mapped to the service, you might require the service settings to be reenabled after you have modified the service parameters, either directly on the device or using the Connectivity Services Director application. In such a case, you can use the reactivation functionality to revive and activate the service properties on devices. To disable a service, the service must not contain any pending or uncommitted changes. Also, the service must be in the Deactivated state. By disabling a service, the traffic processing for the traversed packets is impacted.

In certain network topologies, you might require a service-related settings to be disabled for a certain period to perform troubleshooting or modification to the traffic-handling method, and you might want to reactivate a disabled service later when you have completed network maintenance and analysis work. In such a case, it might be beneficial to use the deactivation functionality for a service order. When you disable a service order, the configuration attributes associated with such a service order are deactivated and commented out in the device settings. The deactivated service is propagated to the devices associated with the service order. To disable a service, the service must not contain any pending or uncommitted changes. Also, the service must be in the Deployed or Re-Activated state.

When you cancel a job, the service order may not fail, but changes the service order state to **Scheduled**. When the job state is **In Progress** and until the device responds, the service order state is **Scheduled**. When the job is **Cancelled**, the job state becomes **Cancelled** and the service order state is **Scheduled**. As a result, the service order cannot be deleted or edited. However, you can move the service order state to **Draft** by right-clicking any service order or by clicking **Actions** at the header of the grid and selecting **Cancel Order** option. The **Cancel Order** option is enabled or disabled, depending on the state of the service order. This option is enabled only when the service order state is **Scheduled** and the job state is **Cancelled** while it is disabled for all the other service order states. When the state of the service order is **Draft**, you can modify and deploy or delete the service order.

The Deployed-Active or Active state denotes a service that has been deployed and is in an active state (enabled). The Deployed-Inactive or Inactive state denotes a service that has been deployed and is in a deactivated state (disabled). The Deployment-Pending or Pending state denotes a service for which deployment of the service to a device is pending to be performed.

Service States

A service is created when a service order to provision a service reaches the Completed state.

If a service exists, it is in the Deployed state. If a new service fails to deploy, the service does not exist.

If an attempt to modify a service fails, the service enters the Fail Deploy state. When a service is in the Fail Deploy state, you can attempt to redeploy it, or you can delete it.

The service also has an audit state of Up or Down, depending on whether the service passed or failed functional audit.

If you modify a service order and successfully redeploy the service, the modified service will operate according to the updated configuration.

**Related
Documentation**

- [Publishing a Custom Service Definition on page 647](#)
- [Unpublishing a Custom Service Definition on page 648](#)
- [Deactivating a Service on page 860](#)
- [Reactivating a Service on page 862](#)

Understanding VLAN Manipulation (Normalization and VLAN Mapping) on Ethernet Services

To effectively manage Ethernet frames that are transported across bridge domains and VPLS routing instances, frames are processed and, if necessary, translated to provide the required VLAN tags. When the customer sites participating in a VPLS domain send traffic of different tag heights (untagged, single tagged, or dual tagged packets) across a service, Internet service providers (ISPs) need to provide a network environment to transport traffic of different tag heights. The Connectivity Services Director application supports VLAN manipulation on VPLS services. VLAN manipulation allows transport of traffic with different tag heights between different customer access sites while preserving the customer traffic profiles that are transported over an MPLS core. You can also use VLAN manipulation for the following purposes:

- Specify different normalized values for outer and inner VLAN tags while troubleshooting packet captures to identify wrong inner/ outer VLAN tag configuration issues.
- Simplify provisioning across a BGP/LDP scenario because VLAN tag manipulation is performed on customer facing interfaces only.
- Simplify the process for troubleshooting predetermined tag values.
- Enable end-to-end communication between clients employing different VLAN topologies.
- Provide ISPs the flexibility to enforce their own QoS policies through metro area and core networks because customer traffic classification is not impacted.



NOTE: To support all access types (port-based [untagged], single-tag, and dual-tag) in a VPLS instance, we recommend that normalization is based on a two-tag operation. However, when only port-based or single-tag access is required, normalizing traffic to a single tag might be sufficient.

For Ethernet services and Ethernet services with flexible VLAN tagging (asymmetric tag height), the type of VLAN manipulation applied depends on the type of device sending and receiving packets. MX Series devices can use VLAN mapping or normalization to translate VLANs tags. M Series devices use only VLAN mapping to translate VLAN tags.

VLAN Translation (Normalization) for VPLS Services

A packet received on a physical port is only accepted for processing if the VLAN tags of the received packet match the VLAN tags associated with one of the logical interfaces configured on the physical port. The VLAN tags of the received packet are translated only if they are different than the normalized VLAN tags. For the translation case, the VLAN identifier tags specify the normalized VLAN.

The VLAN tags of a received packet are compared with the normalized VLAN tags specified with either the **vlan-id** or **vlan-tags** statements. If the VLAN tags of the received packet are different from the normalized VLAN tags, then appropriate VLAN tag operations (such as push-push, pop-pop, pop-swap, swap-swap, swap, and others) are implicitly made to convert the received VLAN tags to the normalized VLAN tags. Then, the source MAC address of a received packet is learned based on the normalized VLAN configuration. For output packets, if the VLAN tags associated with an egress logical interface do not match the normalized VLAN tags within the packet, then appropriate VLAN tag operations (such as push-push, pop-pop, pop-swap, swap-swap, swap, and others) are implicitly made to convert the normalized VLAN tags to the VLAN tags for the egress logical interface. For more information about these operations, see the *Junos OS Routing Protocols Configuration Guide*.

VLAN Mapping for VPLS Services

For Ethernet services and Ethernet services with flexible VLAN tagging (asymmetric tag depth), the Connectivity Services Director application uses the VLAN configuration data that you specified in the service order to apply the appropriate VLAN tags to the input and output VLAN maps for the ingress and egress logical interfaces, respectively. The following steps outline the process of bridging a packet received over a Layer 2 logical interface when a normalizing VLAN identifier (**vlan-id number** or **vlan-tags** statement) is specified for a bridge domain or VPLS routing instance:

1. When a packet is received on a physical port, it is accepted only if the VLAN identifier of the packet matches the VLAN identifier of one of the logical interfaces configured on that port.
2. The VLAN tags of the received packet are then compared with the normalizing VLAN identifier. If the VLAN tags of the packet are different from the normalizing VLAN identifier, the VLAN tags are rewritten, as described in [Table 8 on page 90](#).

3. If the source MAC address of the received packet is not present in the source MAC table, it is learned based on the normalizing VLAN identifier.
4. The packet is then forwarded toward one or more outbound Layer 2 logical interfaces based on the destination MAC address. A packet with a known unicast destination MAC address is forwarded only to one outbound logical interface. For each outbound Layer 2 logical interface, the normalized VLAN identifier configured for the bridge domain or VPLS routing instance is compared with the VLANs tags that are configured on that logical interface. If the VLAN tags associated with an outbound logical interface do not match the normalizing VLAN identifier that is configured for the bridge domain or VPLS routing instance, the VLAN tags are rewritten, as described in [Table 9 on page 91](#).

[Table 8 on page 90](#) and [Table 9 on page 91](#) show how VLAN tags are applied when traffic is sent to and from the bridge domain, depending on how the VLAN IDs and VLAN tags (inner and outer) are configured for the bridge domain and on how VLAN identifiers are configured for the logical interfaces in a bridge domain or VPLS routing instance. Depending on the configuration of the Ethernet services that you create in Connectivity Services Director, the following rewrite operations are performed on VLAN tags:

- **pop**—Remove the VLAN tag from the top of the VLAN tag stack.
- **pop/pop**—Remove both the outer and inner VLAN tags of the frame.
- **pop/swap**—Remove the outer VLAN tag of the frame and replace the inner VLAN tag of the frame.
- **swap**—Replace the inner VLAN tag of the frame.
- **push**—Add a new VLAN tag to the top of the VLAN stack.
- **push/push**—Push two VLAN tags in front of the frame.
- **swap/push**—Replace the VLAN tag of the frame and add a new VLAN tag to the top of the VLAN stack.
- **swap/swap**—Replace both the outer and inner VLAN tags of the frame.

No operation means that the VLAN tags of the inbound or outbound packet are not translated for the specified output logical interface or input logical interface. **NA** means not applicable.

Table 8: VLAN Tag Rewrite Operations at UNI Ingress for Ethernet Services

VLAN Identifier of Logical Interface	vlan-id none	vlan-id 200	vlan-id all	vlan tags outer 100, inner 300
none	no operation	push 200	NA	push 100, push 300
200	pop 200	no operation	no operation	swap 200 to 300, push 100
1000	pop 1000	swap 1000 to 200,	no operation	swap 1000 to 300, push 100

Table 8: VLAN Tag Rewrite Operations at UNI Ingress for Ethernet Services (continued)

vlan-tags outer 2000, inner 300	pop 2000, pop 300	pop 2000, swap 300 to 200	pop 200	swap 2000 to 100
vlan-id range 10-100	NA	NA	no operation	NA
vlan-tags outer 200, inner range 10-100	NA	NA	pop 200	NA

Table 9: VLAN Tag Rewrite Operations at UNI Egress for Ethernet Services

VLAN Identifier of Logical Interface	vlan-id none	vlan-id 200	vlan-id all	vlan tags outer 100, inner 300
none	no operation	pop 200	NA	pop 100, pop 300
200	push 200	no operation	no operation	pop 200, swap 300 to 200
1000	push 1000	swap 200 to 1000	no operation	pop 100, swap 300 to 1000
vlan-tags outer 2000, inner 300	push 2000, push 300	swap 200 to 300, push 3000	push 2000	swap 100 to 2000
vlan-id range 10-100	NA	NA	no operation	NA
vlan-tags outer 200, inner range 10-100	NA	NA	push 200	NA

Sample VLAN Configuration on MX Series and M Series PE Routers

MX Series devices can use VLAN mapping or normalization to translate VLANs tags. M Series devices use only VLAN mapping to translate VLAN tags. The following sample configurations show the VLAN and VPLS routing-instance configurations for an MX960 PE interface and M320 PE interface.

MX960 PE Interface Configuration

M320 PE Interface Configuration

```
interfaces {
  ge-0/0/0 {
    unit 1 {
      encapsulation vlan-vpls;
      vlan-tags outer 5 inner 5;
      ##normalizing the inner and outer tags
      towards the core with Push/Push operations##
    }
  }
  family vpls
}
```

```
interfaces {
  ge-1/1/1 {
    unit 1 {
      encapsulation vlan-vpls;
      vlan-tags outer 22 inner 2;
      ## Q-in-Q tags configured on the PE interface ##
    }
  }
  input-vlan-map {
    swap-swap;
    ##normalizing the inner and outer tags towards the core
    by swapping both tags##
    vlan-id 2;
    inner-vlan-id 1;
  }
  output-vlan-map swap-swap;
  ## Put the original tags back for the packets towards the
  VPLS CE ##
  family vpls
}
```

- Related Documentation**
- [Creating a Multipoint-to-Multipoint VPLS Service Order on page 881](#)
 - [Creating a Point-to-Multipoint VPLS Service Order on page 905](#)

VLAN Pool Profiles Overview

A VLAN pool profile specifies the ranges of valid VLAN IDs that are available for use on MX Series devices, on each physical interface. The maximum theoretical pool of VLAN IDs contains 4096 VLAN IDs—IDs 0 through 4095.

VLAN ID 0 and VLAN ID 4095 are never valid VLAN IDs.

The Connectivity Services Director system provides the following predefined VLAN pool profiles:

- **maximum-range**—Any VLAN ID pool created using the maximum-range profile allows any VLAN ID from 1 through 4094. This is the default VLAN profile.
- **vlan-ccc**—Any VLAN ID pool created using the vlan-ccc profile allows any VLAN IDs from 512 through 4094 available for use. VLAN IDs 1 through 511 are reserved for use by Juniper Networks.

For each physical interface that Junos Space recommends as a UNI, the system attempts to determine the best VLAN pool profile. For example, if a UNI has the vlan-ccc encapsulation setting, the rules recommend the vlan-ccc pool profile for that interface. When the correct VLAN pool profiles have been assigned to each UNI, Connectivity Services Director creates a VLAN ID pool for each UNI containing only the allowed VLAN IDs specified in the VLAN pool profile for that UNI.

If the device interface is already running encapsulation before being brought under Junos Space management, the Connectivity Services Director application assigns the appropriate VLAN range.

For details about encapsulation, see the *Junos OS VPNs Configuration Guide*.

Related Documentation

- [Adding a UNI on page 371](#)
- [Unassigning Device Roles on page 372](#)
- [Deleting UNIs on page 373](#)
- [Discovering Device Roles on page 374](#)
- [Excluding Devices from N-PE Role Assignment on page 375](#)

Redundant Pseudowires for Layer 2 Circuits and VPLS

A redundant pseudowire can act as a backup connection between PE routers and CE devices, maintaining Layer 2 circuit and VPLS services after certain types of failures. This feature can help improve the reliability of certain types of networks (metro for example) where a single point of failure can interrupt service for multiple customers. Redundant pseudowires cannot reduce traffic loss to zero. However, they provide a way to gracefully recover from pseudowire failures in such a way that service can be restarted within a known time limit.

When you configure redundant pseudowires to remote PE routers, you configure one to act as the primary pseudowire over which customer traffic is being transmitted and you configure another pseudowire to act as a backup in the event the primary fails. You configure the two pseudowires statically. A separate label is allocated for the primary and backup neighbors.

The following sections provide an overview of redundant pseudowires for Layer 2 circuits and VPLS:

- [Types of Redundant Pseudowire Configurations on page 94](#)
- [Pseudowire Failure Detection on page 95](#)

Types of Redundant Pseudowire Configurations

You can configure redundant pseudowires for Layer 2 circuits and VPLS in either of the following manners:

- You can configure a single active pseudowire. The PE router configured as the primary neighbor is given preference and this connection is the one used for customer traffic. For the LDP signaling, labels are exchanged for both incoming and outgoing traffic with the primary neighbor. The LDP label advertisement is accepted from the backup neighbor, but no label advertisement is forwarded to it, leaving the pseudowire in an incomplete state. The pseudowire to the backup neighbor is completed only when the primary neighbor fails. The decision to switch between the two pseudowires is made by the device configured with the redundant pseudowires. The primary remote PE router is unaware of the redundant configuration, ensuring that traffic is always switched using just the active pseudowire.
- Alternatively, you can configure two active pseudowires, one to each of the PE routers. Using this approach, control plane signaling is completed and active pseudowires are established with both the primary and backup neighbors. However, the data plane forwarding is done only over one of the pseudowires (designated as the active pseudowire by the local device). The other pseudowire is on standby. The active pseudowire is preferably established with the primary neighbor and can switch to the backup pseudowire if the primary fails.

The decision to switch between the active and standby pseudowires is controlled by the local device. The remote PE routers are unaware of the redundant connection, and so both remote PE routers send traffic to the local device. The local device only accepts traffic from the active pseudowire and drops the traffic from the standby. In addition,

the local device only sends traffic to the active pseudowire. If the active pseudowire fails, traffic is immediately switched to the standby pseudowire.

Pseudowire Failure Detection

When a failure is detected, traffic is switched to the redundant pseudowire, which is then also designated as the active pseudowire. The switch is nonreversible, meaning that once traffic has been switched to the redundant pseudowire, it remains active unless it also fails unless the switch to the redundant pseudowire is never done unless there is a failure in the currently active pseudowire. For example, a primary pseudowire has failed and traffic has been successfully switched to the redundant pseudowire. After a period of time, the cause of the failure of the primary pseudowire has been resolved and it is now possible to reestablish the original connection. However, traffic is not switched back to the original pseudowire unless a failure is detected on the now active pseudowire.

Related Documentation

- [Creating a Point-to-Point Ethernet Service Definition on page 625](#)
- [Creating a Multipoint-to-Multipoint VPLS Service Definition on page 653](#)
- [Creating a Point-to-Multipoint VPLS Service Definition on page 678](#)

VPLS over GRE Overview

Generic routing encapsulation (GRE) is one of the tunneling mechanisms that uses IP as the transport protocol. The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel destination addresses at each endpoint.

The primary use of GRE is to carry non-IP packets through an IP network. GRE also carries IP packets such as IP broadcast, IP multicast through an IP cloud. A GRE tunnel has the following characteristics:

- GRE tunnel is stateless, and offers no flow control mechanisms.
- GRE is multiprotocol and can tunnel any OSI Layer 3 protocol.
- GRE enables routing protocols to travel through the tunnel.
- GRE has weak security features.
- GRE provides no reliability or sequencing. Such features are typically handled by upper-layer protocols.
- GRE tunnels carry multicast traffic.

The VPLS over GRE feature allows you to combine flow-based and packet-based services in a single device. You can deploy large-scale VPLS over GRE.

To better understand this configuration, consider the following scenarios:

In the first scenario, pseudowires enable the creation of point-to-point circuits between two endpoints carried over the MPLS network. Ignoring the signaling protocols for this discussion, these connections are just point-to-point connections. Using this approach

provides an end-to-end wire between sites. This is beneficial from a traffic processing point of view because the gateways do not need to learn MAC addresses; they simply forward anything they receive to the pseudowire. Deploying this configuration can be difficult when trying to provide connectivity to multiple branch offices.

In the second scenario, VPLS provides a Layer 2 network abstraction. With VPLS, endpoints typically negotiate LSPs and pseudowires with every other endpoint (that is, they are fully meshed). When a node receives an Ethernet frame from one of its LAN interfaces, the source MAC address is learned, if it is not already known, and flooded using every pseudowire connecting to all other branch nodes. However, if the destination has been previously learned, then the frame is sent to the appropriate destination. When an Ethernet frame is received through one of the pseudowires (that is, from the MPLS network), source MAC address learning is performed. The next time a frame is sent to that MAC it does not need to be flooded and the frame is flooded to every single LAN interface in the node, but not over the pseudowires. The network acts as a distributed Layer 2 switch providing any-to-any Ethernet connectivity between the devices connected to the different nodes in the network.

While the second scenario provides significant advantages (any-to-any connectivity, automated provisioning, and simple abstraction), it is more complex. Every PE node has to perform Layer 2 learning and flooding of traffic, which can cause problems when either multiple broadcast/multicast or frames to unknown MAC addresses are used. For example, in a topology with a thousand branch offices, each office that receives a broadcast packet must replicate it 999 times, encapsulate each copy in GRE, and forward the resulting traffic. Additionally, because each node performs Layer 2 learning, the maximum number of MAC addresses that each node can learn is limited, limiting the total number of nodes in the domain.

**Related
Documentation**

- [Creating a Multipoint-to-Multipoint VPLS Service Definition on page 653](#)
- [Creating a Point-to-Multipoint VPLS Service Definition on page 678](#)

Junos Space Network Topology Overview

Network topology is the arrangement of various elements including nodes and links. It is the graphical representation of physical devices and their interconnection. The topology has the following three components:

1. Physical topology
2. Link topology
3. IP connectivity

Each application registers itself to the topology framework so that you can view and change topology on the application layer. To view the network topology, select **Network Management Platform > Network Monitoring > Topology**.

In a network topology, you can:

- Monitor the status and configurations of the discovered devices and their interconnections.
- View source and destination information for the device interconnections that exist within the discovered topologies.
- Select a service and view all the devices associated with the service.
- Discover IS-IS configuration devices.

The network topology helps you to understand and visualize the physical and logical interconnection between the network devices and the services. It also enables you to view the end-to-end network and zoom into the segments of the network for management and troubleshooting.

Related Documentation

- [Creating a Service Order on page 815](#)
- [Creating a Point-to-Point ATM or TDM Pseudowire Service Order on page 816](#)
- [Creating a Point-to-Point Service Order on page 829](#)
- [Creating a Multipoint-to-Multipoint VPLS Service Order on page 881](#)
- [Creating a Point-to-Multipoint VPLS Service Order on page 905](#)
- [Creating a Full Mesh Layer 3 VPN Ethernet Service Order on page 941](#)
- [Creating a Hub-and-Spoke Layer 3 VPN Service Order on page 964](#)

Service Recovery Overview

The Service Recovery operation recovers services that are present on devices that Junos Space is not managing. The missing entity can be an entirely new service or the missing component of an existing service.

The Service Recovery operation has two parts. First, you select one or more devices for which services are to be recovered. Service Recovery recovers and identifies the missing services and displays the result. Second, you select a service to be managed, providing any missing information about the recovered service. When you provide missing information for a service, the recovered service is converted to a managed service.

The Connectivity Services Director application supports Service Recovery for point-to-point services, VPLS services, and Layer 3 VPN services. You can perform Service Recovery only using the Services Activation Director GUI and not using the Connectivity Services Director GUI.

Besides the supported capabilities of recovery of new services and new endpoints for existing services, recovery of CFM profiles attached to services is also supported. Also, the Service Recovery task enables you to recover modifications made to existing endpoints associated with services and recover deleted endpoints for services.

The Service Recovery task is displayed in the Connectivity tree node under Network Services root node of the View pane. Recovery of services is supported only for

point-to-point, Layer 3 VPN, and VPLS services. The following tasks are available under the Service Recovery section of the Tasks pane:

- **Recover Services**—Enables you to create or modify a service recovery request. You can also initiate the recovery operation for a request that you created. The Create Service Recovery Request wizard is available to create a service recovery request. The Recover Services button enables you to initiate the recovery job. You can also view the recovered status of services.
- **Recover OutOfBand Changes**—Enables you to recover out-of-band changes that are performed on previously deployed service. A network managed by Connectivity Services Director has three repositories of information about the configuration of a network device—the configuration stored on the device itself, the device configuration record maintained by Junos Space, and the Build mode configuration maintained by Connectivity Services Director. When the configuration contained in all three repositories match, the device configuration state is shown as In Sync in Connectivity Services Director. When the repositories do not match, the configuration state is shown as Out of Sync. A common cause for this state is out-of-band configuration changes—that is, configuration changes made to a device outside of Connectivity Services Director.
- **Rejected Services**—Displays the services that were rejected during service recovery process with the reject reason.

**Related
Documentation**

- [Creating and Handling a Service Recovery Request on page 406](#)

Multicast L3VPN Overview

The Junos Space Connectivity Services Director application uses Multiprotocol-BGP (MBGP) Multicast L3VPNs (MVPN) to implement MVPNs because it is simpler. This method does not require a service provider to configure multicast in its provider backbone to connect PE routers.

For the control plane, MBGP MVPN uses the intra-autonomous system (AS) next-generation BGP. The data plane is configured with Protocol Independent Multicast (PIM) sparse mode. Connectivity Services Director maintains PIM state information using the same architecture that is used for unicast VPNs.

The MBGP MVPN method avoids potential control and data plane scaling problems that can occur with the requirement to maintain two routing and forwarding mechanisms, one for VPN unicast and one for VPN multicast.

The Connectivity Services Director application addresses aspects of published standards as follows:

- Layer 3 VPN service, as defined by RFC 4364, is supported to enable service providers to implement IP multicast for L3VPN services.
- The architecture defined by RFC 4364 for unicast VPNs is supported to enable service providers to configure BGP for the control plane between PE routers.

- Unicast with extensions for intra-Autonomous System (AS) and inter-AS communication, as defined by RFC 4364, is supported.

For MVPNs, Connectivity Services Director enables you to configure two site sets, a sender site set and a receiver site set. Site sets have the following properties:

- Hosts within a sender site can originate multicast traffic for receivers in a receiver site set.
- Receivers outside the receiver site set should not be able to receive traffic sent from the sender site.
- Hosts within the receiver site set can receive multicast traffic originated from any host in the sender site set.
- Hosts within the receiver site set should not be able to receive multicast traffic originated from any host that is not in the sender site set.

A host can be in both the sender site set and the receiver site set. Therefore, such a host can both originate and receive multicast traffic. For example, the sender site set could be the same as the receiver site set. In this case, all hosts could both originate and receive multicast traffic from one another.

Administrative policies define an MBGP MVPN. The policies define both the sender site set and receiver site set. Customers establish the policies but the policies are implemented by service providers, which use the existing BGP and MPLS VPN infrastructure.

Multi-Chassis Automatic Protection Switching Overview

Automatic protection switching (APS) is a linear protection scheme designed to protect VLAN-based Ethernet networks.

With APS, a protected domain is configured with two paths: a working path and a protection path. Both working and protection paths can be monitored. Normally, traffic is carried on the working path (that is, the working path is the active path), and the protection path is disabled. If the working path fails, its protection status is marked as degraded (DG) and APS switches the traffic to the protection path, then the protection path becomes the active path.

APS uses two modes of operation: linear 1+1 protection switching architecture and linear 1:1 protection switching architecture. The linear 1+1 protection switching architecture operates with either unidirectional or bidirectional switching. The linear 1:1 protection switching architecture operates with bidirectional switching.

Related Documentation

- [Creating a Point-to-Point ATM or TDM Pseudowire Service Definition on page 618](#)

Inverse Multiplexing for ATM Overview

The Inverse multiplexing for ATM (IMA) protocol defines a technique for transporting ATM traffic over a bundle of T1 or E1 interfaces. IMA processes traffic differently from multiplexing. While multiplexing combines multiple signals into a single signal, IMA divides a data stream into multiple concurrent streams that are transmitted at the same time across separate channels (such as T1 or E1 interfaces). The data streams are reconstructed into the original data stream at the far end. IMA speeds up the flow of data across a slower interface, such as a T1 or E1 interface, by load balancing the data stream across multiple T1 or E1 interfaces, which increases the line capacity.

You can deploy IMA on Juniper Networks M7, MX and ACX devices. IMA includes the following operational features:

- **Aggregated device count**—A device count is the number of IMA group interfaces created on a CT1 or CE1 interface. As part of an IMA group, a logical ATM interface is identified by the naming format: *at-fpc/pic/port*. The port number is derived from the last port on the MIC plus 1.

For example, for an ACX2000 router with a 16-port built-in T1/E1 TDM MIC, IMA group interface numbering starts with *at-0/0/16*. That interface number is incremented by 1 to *at-0/0/17*, and so on. For an ACX1000 router with an 8-port built-in T1/E1 TDM MIC, IMA group interface numbering starts with *at-0/0/8*. That interface number is incremented by 1 to *at-0/0/9*, and so on.

- **Framing mode**—An emulation mechanism duplicates the essential attributes of a service, such as T1 or E1, over a packet-switched network. On the ACX Series routers, you can configure the built-in channelized T1 and E1 interfaces (CT1 and CE1) to work in either T1 or E1 mode. You can configure these child T1 and E1 interfaces to carry ATM services over the packet-switched network.
- **Built-in channelized interface**—The Juniper Networks devices that support ATM IMA are deployed with one full T1 or E1 interface on the channelized CT1 or CE1 interface. You cannot configure the built-in interface. However, on the built-in interface, you configure the parameters for a child T1 or E1 interface.
- **T1 or E1 interface member of IMA group for IMA link**—Each child T1 or E1 interface of a channelized CT1 or CE1 interface is the physical interface over which the ATM signals are transmitted. To ensure that the IMA link operates correctly, you specify the T1 or E1 interface to be a member of an IMA group.
- **IMA group interface configuration**—To ensure proper operation, you must configure each IMA group interface (*at-fpc/pic/g*) with all ATM properties, which include the logical link-layer encapsulation type and the circuit cross-connect protocol suite. Further, you must dedicate the entire ATM device to the ATM cell relay circuit.

Related Documentation

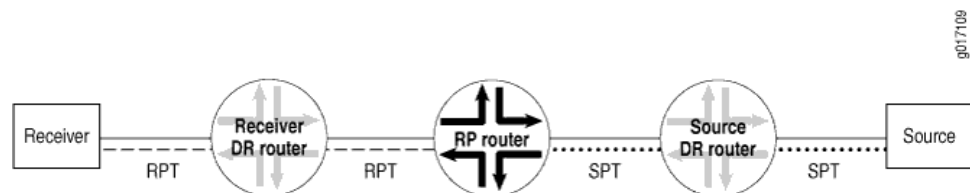
- [Inverse Multiplexing for ATM Overview on page 100](#)
- [Viewing Functional Audit Results for an Inverse Multiplexing for ATM Service on page 1106](#)

Rendezvous Point

The RP router serves as the information exchange point for the other routers. All routers in a PIM domain must provide mapping to an RP router. It is the only router that needs to know the active sources for a domain—the other routers just need to know how to get to the RP. In this way, the RP matches receivers with sources.

The RP router is downstream from the source and forms one end of the SPT. As shown in [Figure 16 on page 101](#), the RP router is upstream from the receiver and thus forms one end of the RPT.

Figure 16: Rendezvous Point as Part of the RPT and SPT



The benefit of using the RP as the information exchange point is that it reduces the amount of state in non-RP routers. No network flooding is required to provide non-RP routers information about active sources.

Related Documentation

- [Understanding Multicast Rendezvous Points, Shared Trees, and Rendezvous-Point Trees on page 101](#)
- [Understanding PIM Sparse Mode on page 103](#)
- [Configuring Shared-Tree Data Distribution Across Provider Cores for Providers of MBGP MVPNs on page 106](#)
- [Configuring SPT-Only Mode for Multiprotocol BGP-Based Multicast VPNs on page 107](#)
- [Configuring VRF Route Targets for Routing Instances for an MBGP MVPN on page 109](#)

Understanding Multicast Rendezvous Points, Shared Trees, and Rendezvous-Point Trees

In a shared tree, the root of the distribution tree is a router, not a host, and is located somewhere in the core of the network. In the primary sparse mode multicast routing protocol, Protocol Independent Multicast sparse mode (PIM SM), the core router at the root of the shared tree is the rendezvous point (RP). Packets from the upstream source and join messages from the downstream routers “rendezvous” at this core router.

In the RP model, other routers do not need to know the addresses of the sources for every multicast group. All they need to know is the IP address of the RP router. The RP router discovers the sources for all multicast groups.

The RP model shifts the burden of finding sources of multicast content from each router (the (S,G) notation) to the network (the (*,G) notation knows only the RP). Exactly how

the RP finds the unicast IP address of the source varies, but there must be some method to determine the proper source for multicast content for a particular group.

Consider a set of multicast routers without any active multicast traffic for a certain group. When a router learns that an interested receiver for that group is on one of its directly connected subnets, the router attempts to join the distribution tree for that group back to the RP, not to the actual source of the content.

To join the shared tree, or *rendezvous-point tree (RPT)* as it is called in PIM sparse mode, the router must do the following:

- Determine the IP address of the RP for that group. Determining the address can be as simple as static configuration in the router, or as complex as a set of nested protocols.
- Build the shared tree for that group. The router executes an RPF check on the RP address in its routing table, which produces the interface closest to the RP. The router now detects that multicast packets from this RP for this group need to flow into the router on this RPF interface.
- Send a join message out on this interface using the proper multicast protocol (probably PIM sparse mode) to inform the upstream router that it wants to join the shared tree for that group. This message is a (*,G) join message because S is not known. Only the RP is known, and the RP is not actually the source of the multicast packets. The router receiving the (*,G) join message adds the interface on which the message was received to its outgoing interface list (OIL) for the group and also performs an RPF check on the RP address. The upstream router then sends a (*,G) join message out from the RPF interface toward the source, informing the upstream router that it also wants to join the group.

Each upstream router repeats this process, propagating join messages from the RPF interface, building the shared tree as it goes. The process stops when the join message reaches one of the following:

- The RP for the group that is being joined
- A router along the RPT that already has a multicast forwarding state for the group that is being joined

In either case, the branch is created, and packets can flow from the source to the RP and from the RP to the receiver. Note that there is no guarantee that the shared tree (RPT) is the shortest path tree to the source. Most likely it is not. However, there are ways to “migrate” a shared tree to an SPT once the flow of packets begins. In other words, the forwarding state can transition from (*,G) to (S,G). The formation of both types of tree depends heavily on the operation of the RPF check and the RPF table.

Related Documentation

- [Rendezvous Point on page 101](#)
- [Understanding PIM Sparse Mode on page 103](#)
- [Configuring Shared-Tree Data Distribution Across Provider Cores for Providers of MBGP MVPNs on page 106](#)
- [Configuring SPT-Only Mode for Multiprotocol BGP-Based Multicast VPNs on page 107](#)

- [Configuring VRF Route Targets for Routing Instances for an MBGP MVPN on page 109](#)

Understanding PIM Sparse Mode

A Protocol Independent Multicast (PIM) sparse-mode domain uses reverse-path forwarding (RPF) to create a path from a data source to the receiver requesting the data. When a receiver issues an explicit join request, an RPF check is triggered. A (*,G) PIM join message is sent toward the RP from the receiver's designated router (DR). (By definition, this message is actually called a join/prune message, but for clarity in this description, it is called either join or prune, depending on its context.) The join message is multicast hop by hop upstream to the ALL-PIM-ROUTERS group (224.0.0.13) by means of each router's RPF interface until it reaches the RP. The RP router receives the (*,G) PIM join message and adds the interface on which it was received to the outgoing interface list (OIL) of the rendezvous-point tree (RPT) forwarding state entry. This builds the RPT connecting the receiver with the RP. The RPT remains in effect, even if no active sources generate traffic.



NOTE: State—the (*,G) or (S,G) entries—is the information used for forwarding unicast or multicast packets. S is the source IP address, G is the multicast group address, and * represents any source sending to group G. Routers keep track of the multicast forwarding state for the incoming and outgoing interfaces for each group.

When a source becomes active, the source DR encapsulates multicast data packets into a PIM register message and sends them by means of unicast to the RP router.

If the RP router has interested receivers in the PIM sparse-mode domain, it sends a PIM join message toward the source to build a shortest-path tree (SPT) back to the source. The source sends multicast packets out on the LAN, and the source DR encapsulates the packets in a PIM register message and forwards the message toward the RP router by means of unicast. The RP router receives PIM register messages back from the source, and thus adds a new source to the distribution tree, keeping track of sources in a PIM table. Once an RP router receives packets natively (with S,G), it sends a register stop message to stop receiving the register messages by means of unicast.

In actual application, many receivers with multiple SPTs are involved in a multicast traffic flow. To illustrate the process, we track the multicast traffic from the RP router to one receiver. In such a case, the RP router begins sending multicast packets down the RPT toward the receiver's DR for delivery to the interested receivers. When the receiver's DR receives the first packet from the RPT, the DR sends a PIM join message toward the source DR to start building an SPT back to the source. When the source DR receives the PIM join message from the receiver's DR, it starts sending traffic down all SPTs. When the first multicast packet is received by the receiver's DR, the receiver's DR sends a PIM prune message to the RP router to stop duplicate packets from being sent through the RPT. In turn, the RP router stops sending multicast packets to the receiver's DR, and sends a PIM prune message for this source over the RPT toward the source DR to halt multicast packet delivery to the RP router from that particular source.

If the RP router receives a PIM register message from an active source but has no interested receivers in the PIM sparse-mode domain, it still adds the active source into the PIM table. However, after adding the active source into the PIM table, the RP router sends a register stop message. The RP router discovers the active source's existence and no longer needs to receive advertisement of the source (which utilizes resources).



NOTE: If the number of PIM join messages exceeds the configured MTU, the messages are fragmented in IPv6 PIM sparse mode. To avoid the fragmentation of PIM join messages, the multicast traffic receives the interface MTU instead of the path MTU.

The major characteristics of PIM sparse mode are as follows:

- Routers with downstream receivers join a PIM sparse-mode tree through an explicit join message.
- PIM sparse-mode RPs are the routers where receivers meet sources.
- Senders announce their existence to one or more RPs, and receivers query RPs to find multicast sessions.
- Once receivers get content from sources through the RP, the last-hop router (the router closest to the receiver) can optionally remove the RP from the shared distribution tree (*;G) if the new source-based tree (S,G) is shorter. Receivers can then get content directly from the source.

The transitional aspect of PIM sparse mode from shared to source-based tree is one of the major features of PIM, because it prevents overloading the RP or surrounding core links.

There are related issues regarding source, RPs, and receivers when sparse mode multicast is used:

- Sources must be able to send to all RPs.
- RPs must all know one another.
- Receivers must send explicit join messages to a known RP.
- Receivers initially need to know only one RP (they later learn about others).
- Receivers can explicitly prune themselves from a tree.
- Receivers that never transition to a source-based tree are effectively running Core Based Trees (CBT).

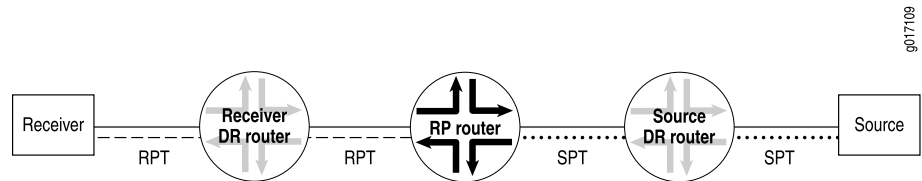
PIM sparse mode has standard features for all of these issues.

Rendezvous Point

The RP router serves as the information exchange point for the other routers. All routers in a PIM domain must provide mapping to an RP router. It is the only router that needs to know the active sources for a domain—the other routers just need to know how to reach the RP. In this way, the RP matches receivers with sources.

The RP router is downstream from the source and forms one end of the shortest-path tree. As shown in [Figure 16 on page 101](#), the RP router is upstream from the receiver and thus forms one end of the rendezvous-point tree.

Figure 17: Rendezvous Point as Part of the RPT and SPT



The benefit of using the RP as the information exchange point is that it reduces the amount of state in non-RP routers. No network flooding is required to provide non-RP routers information about active sources.

RP Mapping Options

RPs can be learned by one of the following mechanisms:

- Static configuration
- Anycast RP
- Auto-RP
- Bootstrap router

We recommend a static RP mapping with anycast RP and a bootstrap router (BSR) with auto-RP configuration, because static mapping provides all the benefits of a bootstrap router and auto-RP without the complexity of the full BSR and auto-RP mechanisms.

Protocol Independent Multicast (PIM) sparse mode is the most common multicast protocol used on the Internet. PIM sparse mode is the default mode whenever PIM is configured on any interface of the device. However, because PIM must not be configured on the network management interface, you must disable it on that interface.

Each any-source multicast (ASM) group has a shared tree through which receivers learn about new multicast sources and new receivers learn about all multicast sources. The rendezvous point (RP) router is the root of this shared tree and receives the multicast traffic from the source. To receive multicast traffic from the groups served by the RP, the device must determine the IP address of the RP for the source.

You can configure a static rendezvous point (RP) configuration that is similar to static routes. A static configuration has the benefit of operating in PIM version 1 or version 2. When you configure the static RP, the RP address that you select for a particular group must be consistent across all routers in a multicast domain.

One common way for the device to locate RPs is by static configuration of the IP address of the RP. A static configuration is simple and convenient. However, if the statically defined RP router becomes unreachable, there is no automatic failover to another RP router. To remedy this problem, you can use anycast RP.

- Related Documentation**
- [Rendezvous Point on page 101](#)
 - [Understanding Multicast Rendezvous Points, Shared Trees, and Rendezvous-Point Trees on page 101](#)
 - [Configuring Shared-Tree Data Distribution Across Provider Cores for Providers of MBGP MVPNs on page 106](#)
 - [Configuring SPT-Only Mode for Multiprotocol BGP-Based Multicast VPNs on page 107](#)
 - [Configuring VRF Route Targets for Routing Instances for an MBGP MVPN on page 109](#)

Configuring Shared-Tree Data Distribution Across Provider Cores for Providers of MBGP MVPNs

For MBGP MVPNs (also referred to as next-generation Layer 3 multicast VPNs), the default mode of operation supports only intersite shortest-path trees (SPTs) for customer PIM (C-PIM) join messages. It does not support rendezvous-point trees (RPTs) for C-PIM join messages. The default mode of operation provides advantages, but it requires either that the customer rendezvous point (C-RP) be located on a PE router or that the Multicast Source Discovery Protocol (MSDP) be used between the C-RP and a PE router so that the PE router can learn about active sources advertised by other PE routers.

If the default mode is not suitable for your environment, you can configure RPT-SPT mode (also known as *shared-tree data distribution*), as documented in section 13 of the BGP-MVPN draft (draft-ietf-l3vpn-2547bis-mcast-bgp-00.txt). RPT-SPT mode supports the native PIM model of transmitting (*G) messages from the receiver to the RP for intersite shared-tree join messages. This means that the type 6 (*G) routes get transmitted from one PE router to another. In RPT-SPT mode, the shared-tree multicast routes are advertised from an egress PE router to the upstream router connected to the VPN site with the C-RP. The single-forwarder election is performed for the C-RP rather than for the source. The egress PE router takes the upstream hop to advertise the (*G) and sends the type 6 route toward the upstream PE router. To send the data on the RPT, either inclusive or selective provider tunnels can be used. After the data starts flowing on the RPT, the last-hop router switches to SPT mode, unless you include the **spt-threshold infinity** statements in the configuration.



NOTE: The MVPN single-forwarder election follows the rule documented in section 9.1.1 of the BGP-MVPN draft (draft-ietf-l3vpn-2547bis-mcast-bgp-00.txt). The single-forwarder election winner is based on the following rules:

- If the active unicast route to the source is through the interface, then this route is used to determine the upstream multicast hop (UMH).
 - If the active unicast route to the source is a VPN route, MVPN selects the UMH based on the highest IP address in the route import community for the VPN routes, and the local master loopback address for local VRF routes.
-

The switch to SPT mode is performed by PIM and not by MVPN type 5 and type 6 routes. After the last-hop router switches to SPT mode, the SPT (S,G) join messages follow the same rules as the SPT-only default mode.

The advantage of RPT-SPT mode is that it provides a method for PE routers to discover sources in the multicast VPN when the C-RP is located on the customer site instead of on a PE router. Because the shared C-tree is established between VPN sites, there is no need to run MSDP between the C-RP and the PE routers. RPT-SPT mode also enables egress PE routers to switch to receiving data from the PE connected to the source after the source information is learned, instead of receiving data from the RP.

In Junos OS Release 15.1 and later, in RPT-SPT mode, PIM SSG Joins are created on the egress PE even if no directly-connected receivers are present.



CAUTION: When you configure RPT-SPT mode, receivers or sources directly attached to the PE router are not supported. As a workaround, place a CE router between any receiver or source and the PE router.

Related Documentation

- [Rendezvous Point on page 101](#)
- [Understanding Multicast Rendezvous Points, Shared Trees, and Rendezvous-Point Trees on page 101](#)
- [Understanding PIM Sparse Mode on page 103](#)
- [Configuring SPT-Only Mode for Multiprotocol BGP-Based Multicast VPNs on page 107](#)
- [Configuring VRF Route Targets for Routing Instances for an MBGP MVPN on page 109](#)

Configuring SPT-Only Mode for Multiprotocol BGP-Based Multicast VPNs

For MBGP MVPNs (also referred to as next-generation Layer 3 multicast VPNs), the default mode of operation is shortest path tree only (SPT-only) mode. In SPT-only mode, the active multicast sources are learned through multicast VPN source-active routes. This mode of operation is described in section 14 of the BGP-MVPN draft (draft-ietf-l3vpn-2547bis-mcast-bgp-00.txt).

In contrast to SPT-only mode, rendezvous point tree (RPT)-SPT mode (also known as shared-tree data distribution) supports the native PIM model of transmitting (*,G) messages from the receiver to the RP for intersite shared-tree join messages.

In SPT-only mode, when a PE router receives a (*, C-G) join message, the router looks for an active source transmitting data to the customer group. If the PE router has a source-active route for the customer group, the router creates a source tree customer multicast route and sends the route to the PE router connected to the VPN site with the source. The source is determined by MVPN's single-forwarder election. When a receiver sends a (*,G) join message in a VPN site, the (*,G) join message only travels as far as the PE router. After the join message is converted to a type 6 multicast route, which is

equivalent to a (S,G) join message, the route is installed with the no-advertise community setting.



NOTE: The MVPN single-forwarder election follows the rule documented in section 9.1.1 of the BGP-MVPN draft (draft-ietf-l3vpn-2547bis-mcast-bgp-00.txt). The single-forwarder election winner is based on the following rules:

- If the active unicast route to the source is through the interface, then this route is used to determine the upstream multicast hop (UMH).
- If the active unicast route to the source is a VPN route, MVPN selects the UMH based on the highest IP address in the route import community for the VPN routes, and the local master loopback address for local VRF routes.

Single-forwarder election guarantees selection of a unique forwarder for a given customer source (C-S). The upstream PE router might differ for the source tree and the shared tree because the election is based on the customer source and C-RP, respectively. Although the single-forwarder election is sufficient for SPT-only mode, the alternative RPT-SPT mode involves procedures to prevent duplicate traffic from being sent on the shared tree and the source tree. These procedures might require administrator-configured parameters to reduce duplicate traffic and reduce blackholes during RPT to SPT switch and the reverse.

In SPT-only mode, when a source is active, PIM creates a register state for the source both on the DR and on the C-RP (or on a PE router that is running Multicast Source Discovery Protocol [MSDP] between itself and the C-RP). After the register states are created, MVPN creates a source-active route. These type 5 source-active routes are installed on all PE routers. When the egress PE router with the (*G) join message receives the source-active route, it has two routes that it can combine to produce the (S,G) multicast route. The type 6 route informs the PE router that a receiver is interested in group G. The source active route informs the PE router that a source S is transmitting data to group G. MVPN combines this information to produce a multicast join message and advertises this to the ingress PE router, as determined by the single-forwarder election.

For some service providers, the SPT-only implementation is not ideal because it creates a restriction on C-RP configuration. For a PE router to create customer multicast routes from (*, C-G) join messages, the router must learn about active sources through MVPN type 5 source-active routes. These source-active routes can be originated only by a PE router. This means that a PE router in the MVPN must learn about all PIM register messages sent to the RP, which is possible only in the following cases:

- The C-RP is colocated on one of the PEs in the MVPN.
- MSDP is run between the C-RP and the VRF instance on one of the PE routers in the MVPN.

If this restriction is not acceptable, providers can use RPT-SPT mode instead of the default SPT-only mode. However, because SPT-only mode does not transmit (*,G)

routes between VPN sites, SPT-only mode has the following advantages over RPT-SPT mode:

- Simplified operations by exchanging and processing only source-tree customer multicast routes among PE routers
- Simplified operations by eliminating the need for the service provider to suppress MVPN transient duplicates during the switch from RPT to SPT
- Less control plane overhead in the service provider space by limiting the type of customer multicast routes exchanged, which results in more scalable deployments
- More stable traffic patterns in the backbone without the traffic shifts involved in the RPT-SPT mode
- Easier maintenance in the service provider space due to less state information

**Related
Documentation**

- [Rendezvous Point on page 101](#)
- [Understanding Multicast Rendezvous Points, Shared Trees, and Rendezvous-Point Trees on page 101](#)
- [Understanding PIM Sparse Mode on page 103](#)
- [Configuring Shared-Tree Data Distribution Across Provider Cores for Providers of MBGP MVPNs on page 106](#)
- [Configuring VRF Route Targets for Routing Instances for an MBGP MVPN on page 109](#)

Configuring VRF Route Targets for Routing Instances for an MBGP MVPN

By default, the VPN routing and forwarding (VRF) import and export route targets (configured either using VRF import and export policies or using the **vrf-target** statement) are used for importing and exporting routes with the MBGP MVPN network layer reachability information (NLRI).

You can use the **export-target** and **import-target** statements to override the default VRF import and export route targets. Export and import targets can also be specified specifically for sender sites or receiver sites, or can be borrowed from a configured unicast route target. Note that a sender site export route target is always advertised when security association routes are exported.



NOTE: When you configure an MBGP MVPN routing instance, you should not configure a target value for an MBGP MVPN specific route target that is identical to a target value for a unicast route target configured in another routing instance.

Specifying route targets in the MBGP MVPN NLRI for sender and receiver sites is useful when there is a mix of sender only, receiver only, and sender and receiver sites. A sender site route target is used for exporting automatic discovery routes by a sender site and for importing automatic discovery routes by a receiver site. A receiver site route target is

used for exporting routes by a receiver site and importing routes by a sender site. A sender and receiver site exports and imports routes with both route targets.

A provider edge (PE) router with sites in a specific MBGP MVPN must determine whether a received automatic discovery route is from a sender site or receiver site based on the following:

- If the PE router is configured to be only in a sender site, route targets are imported only from receiver sites. Imported automatic discovery routes must be from a receiver site.
- If the PE router is configured to be only in a receiver site, route targets are imported only from sender sites. Imported automatic discovery routes must be from a sender site.
- If a PE router is configured to be in both sender sites and receiver sites, these guidelines apply:
 - Along with an import route target, you can optionally configure whether the route target is from a receiver or a sender site.
 - If a configuration is not provided, an imported automatic discovery route is treated as belonging to both the sender site set and the receiver site set.

**Related
Documentation**

- [Rendezvous Point on page 101](#)
- [Understanding Multicast Rendezvous Points, Shared Trees, and Rendezvous-Point Trees on page 101](#)
- [Understanding PIM Sparse Mode on page 103](#)
- [Configuring Shared-Tree Data Distribution Across Provider Cores for Providers of MBGP MVPNs on page 106](#)
- [Configuring SPT-Only Mode for Multiprotocol BGP-Based Multicast VPNs on page 107](#)

Static Pseudowire Provisioning for VPLS Services

A virtual private LAN service (VPLS) domain consists of a set of PE routers that act as a single virtual Ethernet bridge for the customer sites connected to these routers. By configuring static pseudowires for the VPLS domain, network providers do not need to configure the LDP or BGP protocols that are normally used for signaling. Static pseudowires require that you configure a set of in and out labels for each pseudowire configured for the VPLS domain. You still need to configure a VPLS identifier and neighbor identifiers for a static VPLS domain. You can configure both static and dynamic neighbors within the same VPLS routing instance.

The manual configuration of a static pseudowire in MPLS requires configuring many parameters at the two PE sides. We recommend that you configure the parameters on both sides the same to make the pseudowire operational. A mismatch in one or more parameters on either end can cause the pseudowire not to operate correctly. In the case of a dynamic pseudowire, these parameters are negotiated at either end through a

signaling session. For static pseudowire, there is no such signaling session and therefore parameters must be pre-selected and configured on both PE ends.

To enable static VPLS on a router, you need either to configure a virtual tunnel interface (requires the router to have a tunnel services PIC) or to configure a label-switching interface (LSI).

To configure an LSI, include the **no-tunnel-services** statement at the **[edit protocols vpls static-vpls]** hierarchy level.



NOTE: This **Enable Static PW Labels** option is available in the Point-to-Multipoint and Multipoint-to-Multipoint service types when the signaling type is LDP and only in the Point-to-Multipoint service type when the signaling type is BGP.

Related Documentation

- [Creating a Multipoint-to-Multipoint VPLS Service Definition on page 653](#)
- [Creating a Point-to-Multipoint VPLS Service Definition on page 678](#)
- [Creating a Service Definition for VPLS Access into Layer 3 Networks on page 705](#)

PART 2

Getting Started With Connectivity Services Director

- [Understanding Connectivity Services Director System Administration and Preferences on page 115](#)

CHAPTER 4

Understanding Connectivity Services Director System Administration and Preferences

- [Understanding Connectivity Services Director User Administration on page 115](#)
- [Understanding the System Tasks Pane on page 117](#)
- [Audit Logs Overview on page 117](#)
- [Viewing Audit Logs From Connectivity Services Director on page 117](#)
- [Managing Jobs on page 118](#)
- [Collecting Logs for Troubleshooting on page 120](#)
- [Setting Up User and System Preferences on page 122](#)

Understanding Connectivity Services Director User Administration

Connectivity Services Director uses the user administration features of the Junos Space platform on which it runs. Using these features, you can add, delete, and edit user accounts and roles and changing user passwords. Refer to the *Junos Space Network Application Platform User Guide* for more information about user administration.

When Connectivity Services Director is installed, some additional user administration options are available in Junos Space, which are specific to Connectivity Services Director:

In addition to the Super Administrator role, the following predefined roles are available to Connectivity Services Director users:

- The Device Manager role allows an administrator to discover devices.
- The Service Manager role allows an administrator to perform device pre-staging actions including discovering and assigning device roles.
- The Service Designer roles allows an administrator to create and publish a service definition.
- The Service Activator (less privileged) role allows an administrator to perform provisioning tasks including creating and managing customers, service orders, and services.

You can also create custom roles to grant users different access rights to the Connectivity Services Director modes. Connectivity Services Director modes—Deploy, Monitor, Fault, and Build—are available to assign to custom user roles in the list of application workspaces and associated tasks.



NOTE: The tasks listed under the Connectivity Services Director modes are disabled. Access is controlled at the mode level, so if you grant a role access to a mode, the role has access to all tasks in that mode, regardless of which tasks you select.



NOTE: For the Service Manager, Service Designer, and Service Activator user roles in Services Activation Director, the roles are migrated with additional access privileges to enable access to the different lifecycle modes of Connectivity Services Director after upgrading to Connectivity Services Director, Release 2.0.

If you try to log in to Connectivity Services Director by using an account that does not have access rights to any Connectivity Services Director modes, you are redirected to Junos Space instead.



NOTE: Access to Connectivity Services Director system preferences is controlled by user access rights. For more information, see [“Setting Up User and System Preferences” on page 122](#).

Related Documentation

- [Connectivity Services Overview on page 3](#)
- [Benefits of a Unified User Interface for Routing and Tunnel Services with Connectivity Services Director on page 6](#)
- [Connectivity Services Director Overview on page 8](#)
- [Understanding the Connectivity Services Director User Interface on page 10](#)
- [Understanding the Usage and Layout of Connectivity Services Director Views and Tasks on page 21](#)
- [Understanding the Management Lifecycle Modes in Connectivity Services Director on page 22](#)
- [Logging In to Connectivity Services Director on page 25](#)
- [Logging Out of Connectivity Services Director on page 30](#)

Understanding the System Tasks Pane

The System Tasks pane provides tasks for viewing audit logs of Connectivity Services Director user activities, for managing jobs, and for collecting troubleshooting logs.

To access the System Tasks pane, click **System** in the Connectivity Services Director banner. The tasks are described in [Table 10 on page 117](#).

Table 10: System Tasks

Task	Description
View Audit Logs	View a history of user activities on Connectivity Services Director, including log in, log out, and task initiation and completion.
Manage Jobs	View all jobs that are scheduled to run or have been run by Connectivity Services Director. You can cancel jobs that are in progress or scheduled to run in the future.
Collect Jobs for Troubleshooting	Download a zip file containing logs and troubleshooting data from both Connectivity Services Director and Junos Space.

Audit Logs Overview

Audit logs provide a record of login history and user-initiated tasks that are performed from the user interface. From the Audit Logs page, you can monitor user login–logout activity over time, track device management tasks, view services that were provisioned on devices, and so forth. Audit logging does not record non-user initiated activities, such as device-driven activities, and is not designed for debugging purposes.

Administrators can sort and filter on audit logs to determine which users performed what actions on what objects at what time. For example, an administrator can use audit log filtering to track the user accounts that were added on a specific date, track configuration changes across a particular type of device, view services that were provisioned on specific devices, or monitor user login–logout activity over time.

Over time, Connectivity Services Director will archive a large volume of log entries. Such log entries might or might not be reviewed, but they must be retained for a period of time.

The audit logs can be saved to a local server (the server that functions as the active node for Connectivity Services Director) or a remote network host or media.

Viewing Audit Logs From Connectivity Services Director

Audit logs are generated for login activity and tasks that are initiated from the Connectivity Services Director application. The Audit Logs page displays the logs for all user-initiated activities.

You can do the following on the Audit Logs page:

- Sort, filter, and search the log entries using the standard table manipulation features in Connectivity Services Director.
- Obtain more information about a log entry by double-clicking the entry or by selecting the entry and clicking **Show Details**. The Audit Log Details window is displayed.
- For a user-initiated task that runs as a job, you can obtain more information about the job by clicking the job ID in the Job ID column.

To display the Audit Logs page:

1. Click **System** in the Connectivity Services Director banner.
2. Select **View Audit Logs** from the Tasks pane.

The Audit Logs page is displayed with the fields listed in [Table 11 on page 118](#).

Table 11: Audit Logs Page Fields

Field	Description
User Name	The login ID of the user that initiated the task
User IP	The IP address of the client computer from which the user initiated the task
Task	The name of the task that triggered the audit log
Time	The data and time when the user initiated the task
Result	The execution result of the task that triggered the audit log: <ul style="list-style-type: none">• Success—Job completed successfully• Failure—Job failed and was terminated• Job Scheduled—Job is scheduled but has not yet started
Description	A description of the audit log
Job ID	The job ID for any task that runs as a job

Managing Jobs

Connectivity Services Director enables you to view and manage jobs. You can view the status of completed jobs and cancel the jobs that are scheduled to execute at a later time or jobs that are in progress.

The Job Management page, accessible as a System task, enables you to view and manage all jobs. In addition, Connectivity Services Director enables you to view special pre-filtered versions of this page from various other tasks, such as View Discovery Status or View Image Deployment Jobs. These pages contain the same fields (although some fields might be hidden) and have the same functionality as the Job Management page, but they list only those jobs relevant to particular tasks.

Job ID	Name	Percent	State	Summary	Parameters	Scheduled Start Time	Actual Start Time	End Time	User
458759	Cloud Infrastructure Event Purge...	0	SCHEDULED			Sep 04, 2015 05:30:00 AM IST	-	-	
622654	Vtpe-Test-scale Deployment	0	CANCELLED	Job was cancelled by user super		Sep 03, 2015 09:45:00 PM IST	-	-	super
622655	Auto Resynchronize devices-62...	100	SUCCESS	Number of Reconciled Devices: 1 Number of Reconciled succeeded: 1 Number of Reconciled failed: 0	Device(s): junos-mx80-2-space	Sep 03, 2015 03:37:27 PM IST	Sep 03, 2015 03:37:29 P...	Sep 03, 2015 03:37:50 P...	
622653	Auto Resynchronize devices-62...	100	FAILURE	Number of Reconciled Devices: 1 Number of Reconciled succeeded: 0 Number of Reconciled failed: 1	Device(s): junos-mx240-space	Sep 03, 2015 03:25:17 PM IST	Sep 03, 2015 03:25:19 P...	Sep 03, 2015 03:25:22 P...	
622679	Auto Resynchronize devices-62...	100	FAILURE	Number of Reconciled Devices: 1 Number of Reconciled succeeded: 0 Number of Reconciled failed: 1	Device(s): RouterZ1-re	Sep 03, 2015 03:21:49 PM IST	Sep 03, 2015 03:21:49 P...	Sep 03, 2015 03:21:50 P...	
622675	vtpa-bgp-res-lst Deployment	100	SUCCESS	Deployed On Device [RouterZ1-...		Sep 03, 2015 03:19:08 PM IST	Sep 03, 2015 03:19:08 P...	Sep 03, 2015 03:19:17 P...	super
622674	007_P2P_RESValidate Service O...	100	SUCCESS	Validated On Device [PE9_re] O...		Sep 03, 2015 03:14:43 PM IST	Sep 03, 2015 03:14:43 P...	Sep 03, 2015 03:14:55 P...	super
622673	006_P2P_RESValidate Service O...	100	SUCCESS	Validated On Device [PE9_re] O...		Sep 03, 2015 03:11:59 PM IST	Sep 03, 2015 03:12:00 P...	Sep 03, 2015 03:12:12 P...	super
622672	005_P2P_RESValidate Service O...	100	FAILURE	Validating On Device [400R4_EP...] lock Success. edit-config Failed. protocol operation-failed error invalid input at '132' in tp addr...		Sep 03, 2015 03:08:25 PM IST	Sep 03, 2015 03:08:25 P...	Sep 03, 2015 03:08:46 P...	super
622671	004_P2P_RESValidate Service O...	100	SUCCESS	Validated On Device [400R4_EP_...		Sep 03, 2015 03:06:26 PM IST	Sep 03, 2015 03:06:26 P...	Sep 03, 2015 03:06:38 P...	super
622670	003_P2P_RESValidate Service O...	100	SUCCESS	Validated On Device [PE8_re] O...		Sep 03, 2015 02:58:43 PM IST	Sep 03, 2015 02:58:44 P...	Sep 03, 2015 02:58:57 P...	super
622664	Auto Resynchronize devices-62...	100	SUCCESS	Number of Reconciled Devices: 1 Number of Reconciled succeeded: 1 Number of Reconciled failed: 0	Device(s): PE9_re	Sep 03, 2015 02:56:39 PM IST	Sep 03, 2015 02:56:44 P...	Sep 03, 2015 02:56:45 P...	
622666	002_P2P_RESValidate Service O...	100	SUCCESS	Validated On Device [400R4_EP_...		Sep 03, 2015 02:56:30 PM IST	Sep 03, 2015 02:56:31 P...	Sep 03, 2015 02:56:43 P...	super

To display the Job Management page:

1. Click **System** on the Connectivity Services Director banner.
2. Select **Manage Jobs** from the Tasks pane. The Job Management page appears.
3. To view the details of a job, select a row and click **Show Details** or double-click a row.
4. To cancel a scheduled job, select a job that is scheduled for a later time or a job that is in progress and click **Cancel**.

The fields in the Job Management page are described in [Table 12 on page 119](#). To view any hidden column, keep the mouse on any column heading and select the down arrow and then click Columns. Select the check box to display the hidden columns.



NOTE: You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the View Deployment Jobs option in the task pane.



NOTE: Details of jobs initiated from Connectivity Services Director will be available only from Connectivity Services Director. These jobs will not be listed in the Job Management pane in Junos Space platform and vice-versa.

Table 12: Job Management Page Fields

Field	Description
Job ID	The unique ID assigned to the job
Name	The name of the job

Table 12: Job Management Page Fields (continued)

Field	Description
Percent	The percentage of completion of the job
State	The status of the job: <ul style="list-style-type: none"> • Success—Job completed successfully • Failure—Job failed and was terminated • Job Scheduled—Job is scheduled but has not yet started • In progress—Job is has started, but not completed • Cancelled—Job is cancelled
Job Type	The type of the job
Summary	Summary of the job scheduled and executed with status
Scheduled Start Time	The time when the job is scheduled to start
Actual Start Time	The actual time when the job started
End Time	The time when the job was completed
User	The login ID of the user that initiated the task
Recurrence	The recurrent time when the job will be restarted.

Related Documentation

- [Managing Service Configuration Deployment Jobs on page 1003](#)
- [Deploying Services Configuration to Devices on page 1005](#)

Collecting Logs for Troubleshooting

Connectivity Services Director enables you to collect logs and other data from both Connectivity Services Director and Junos Space that can assist in managing and monitoring Connectivity Services Director servers.

Connectivity Services Director collects the logs and troubleshooting data into a compressed file that you can download. This file is named **troubleshoot_yyyy-mm-dd_hh-mm-ss.zip**—for example, **troubleshoot_2012-12-21_11-25-12.zip**. The date and time in the file name is the server Coordinated Universal Time (UTC) date and time.

To retrieve troubleshooting data and log files, follow these steps:

1. Click **System** on the Connectivity Services Director banner.
2. From the Tasks pane, click **Collect Logs for Troubleshooting**. The Collect Logs for Troubleshooting page appears.
3. Click the **Download troubleshooting data and logs from Connectivity Services Director and Junos Space** link.

Connectivity Services Director begins collecting the logs and data. It can take a few minutes for Connectivity Services Director to collect the information and create the zip file.

4. When the standard file download window for your browser opens, save the **troubleshoot_yyyy-mm-dd_hh-mm-ss.zip** file.
5. When you contact the Juniper Technical Assistance Center, describe the problem you encountered and provide the JTAC representative with the **troubleshoot.zip** file.

[Table 13 on page 121](#) lists the files included in the **troubleshoot_yyyy-mm-dd_hh-mm-ss.zip** file.

Table 13: Log Files in the troubleshooting.zip File

Description	Location
Jboss log files	<code>/var/log/jboss/servers/server1</code>
Connectivity Services Director application log files	<code>/var/log/jboss/CSD.log</code>
Connectivity Services Director monitoring log files	<code>/var/log/jboss/CSDMoniotring.log</code>
MSS OS adapter log files	<code>/home/jmp/mssosadpater/var/errorLog/</code>
Daemon log files	<code>/opt/opennms/logs/daemon/</code>
Platform log files	<code>/var/log/platform</code>
Access Log Files	<code>/var/log/httpd</code>
Log files for Apache, NMA, Webproxy	<code>/var/log/httpd/</code>
Watchdog log file	<code>/var/log/</code>

Setting Up User and System Preferences

Depending on your system authority, Preferences page can display either user settings or a combination of user settings and system settings. One or more of these preference tabs appear when you open the Preferences page:

- **User**—All users can choose whether monitors and reports display local time or server time.
- **Search**—Administrators can configure options for search indexing.
- **Monitoring**—Network Administrators can change the polling interval for data collection for Monitor mode monitors and enable or disable the internal processes used for data collection.
- **Fault**—Network Administrators can enable or disable alarms. They can also set the retention period for alarms and the number of events per alarm.
- **Report**—Network Administrators can specify length of time Connectivity Services Director reports are retained.
- **Topology**—Network Administrators can specify the topology server to which the Connectivity Services Director application can establish a connection. Also, you can specify settings for the automatic update and refresh of the topology. In addition, you can define a retention period for the deleted links in Topology.
- **Service Activation**—Network Administrators can modify the configuration settings for services activation-related components or functionalities of the Connectivity Services Director application.
- **Optical**—Network Administrators can enable or disable optical performance monitoring.

This topic describes:

- [Accessing the Preferences page on page 122](#)
- [Choosing Server Time or Local Time on page 123](#)
- [Specifying Search Preferences on page 123](#)
- [Retaining Connectivity Services Director Reports on page 123](#)
- [Modifying Services Activation Parameter Settings on page 123](#)
- [Specifying Topology Preferences on page 128](#)
- [Changing Monitor Mode Settings on page 129](#)
- [Changing Alarm Settings on page 131](#)
- [Disabling Optical Performance Monitoring on page 153](#)

Accessing the Preferences page


To open the Preferences page, click  in the Connectivity Services Director banner and select **Preferences** as shown in [Figure 18 on page 123](#).

Figure 18: Accessing the Preferences Page



The Preferences page opens with User Preferences as the default tab.

Choosing Server Time or Local Time

All users can specify whether Connectivity Services Director displays local time or the server's time in monitors and reports on the User Preferences tab. The default setting is to display local time. To change the setting to display the server's time:

1. In the Preferences page, select **Use Server Time** from the list.
2. Click **OK** to save your changes or click **Cancel** to close Preferences.

Specifying Search Preferences

Connectivity Services Director indexes the device inventory data periodically to enable users to perform efficient searches. You can specify a time interval after which Connectivity Services Director initiates the next indexing on the Search tab. You can also specify to stop indexing while devices are imported into Connectivity Services Director. If you are running short of system memory, selecting this option can help save some memory and speed up the discovery and import of new devices. By default this option is selected and the search index update interval is set to 900 seconds.

Retaining Connectivity Services Director Reports

By default, Connectivity Services Director keeps reports for 30 days. However, Network Administrators can change the retention period from 0 to 365 days. To change the setting, move the slider right or left on the Report tab of Preferences to the new setting. Click **OK** to save the setting.

Modifying Services Activation Parameter Settings

To understand the parameters of the services-activation settings, such as the attributes and functionalities that apply to the management, provisioning, and monitoring of point-to-point, Layer 3 VPN, RSVP LSP, and VPLS services, refer to [Table 14 on page 123](#).

Table 14: Parameters in the Services Activation Tab

Fields	Description
Deployment	
Check service version	Select this check box to validate the version of the service being configured.

Table 14: Parameters in the Services Activation Tab (continued)

Fields	Description
Deploy configuration to the device	Select this check box to deploy the configuration to the device.
Enable service alarms	Select this check box to enable the service alarms. Enabling the service alarms causes a GUI impact on the Connectivity Services Director application. When you select the check box and deploy the service, the interface goes down, resulting in the failure to update the fault status. When you right-click Service and select View Service Alarms , the latter does not appear in the results.
Save configuration in XML format	Select this check box to save the configuration of the device in XML format.
Show configuration in set format	Select this check box to display the configuration in set format.
Use two-phase commit for service provisioning	Select this check box to push the configuration on all the network elements automatically, making either one or all successful.
Use vlan maps for E-Line services	When this check box is selected, normalization of VLAN tags is performed using the input or output VLAN maps. This check box is selected by default.
Use vlan maps for flexible tagged services instead of normalized vlan (VPLS)	When this check box is cleared, normalization of VLAN tags is performed using normalized tags under routing instance. This check box is cleared by default.
Block deployment on pending notifications	Select this check box to cause a validation to be performed to determine if any of the selected devices have pending out-of-band notification, before deploying a service order. If a pending out-of-band notification exists for a device, deployment is blocked with the following message: Cannot deploy service order, since pending notification exists for device(s) : <dev-1>, <dev-2>,<dev-3>
Audit	
Enable Functional Audit after deployment	Select this check box to perform the functional audit automatically, after the service is deployed successfully. By default, the functional audit is not checked. Extra time is taken to complete both the functional audit and deployment.
Functional Audit Waiting Time after deployment	Specify the initial wait time to auto-schedule a functional audit job after deployment. If the entered value is greater than 30 minutes, it is reset to 30 minutes. If the entered value is less than 1 minute, the wait time is ignored. The range is from 1 minute through 30 minutes.
Perform Functional Audit on Control plane only	Select this check box to make the functional audit ignore the data plane verification and to consider only the control plane.
User Interface	

Table 14: Parameters in the Services Activation Tab (continued)

Fields	Description
Allow template modification for service	Select this check box to allow the templates to be changed during the service modification.
Bandwidth Combo Items Count	<p>Specify the bandwidth combo items count.</p> <p>In Create P2P service order page, if the bandwidth range exceeds the bandwidth combo items count, then the bandwidth input is taken in text field.</p> <p>The default value is 100.</p>
Service Detail Wait Time (sec)	Specify the period of time in seconds as the wait period for retrieving service details during service template modification.
Monitoring	
Perform Monitoring on Failed Functional Audit	Select this check box to perform monitoring if the functional audit fails.
Pseudowire Redundancy Transition TimeDelay	<p>Select this check box to dump the configuration files.</p> <p>Specify the time delay to issue the remote procedure call (RPC) call for redundancy service. Since there is no support for the fault management for redundancy service, it should not update the fault status as down, when the interface goes down as the service will be running with the help of backup device. The RPC is issued to check the status of the service. If the value of this time delay is 2 seconds and the interface goes down, it waits for 2 seconds to check whether the service is up, with the help of the backup device and correspondingly updates the fault status.</p> <p>The default value is 2 seconds.</p>
Statistics Aggregation Reporting	<p>Specify the manner in which the aggregated results are returned for a query that polls and retrieves data from devices. Two aggregation values are supported:</p> <ul style="list-style-type: none"> • Total: Sum of the number of packets received in the interval • Average: Average of the total number of packets received in the interval
Logging	
Dump Configuration Files	By default, the configuration files are not dumped into the log directory. This is enabled, if there is a need to provide troubleshooting to Juniper Networks Technical Assistance Center (JTAC).
Dump Deployment Data	Select this check box to write the configlets and error response from the JUNOS devices into the log directory..
Log Directory	Specify the default path of the log directory: <code>/var/tmp/jboss</code>
Prestage Devices	

Table 14: Parameters in the Services Activation Tab (continued)

Fields	Description
Pre-stage Wait Time (Sec)	Specify the number of seconds for which the task to trigger a job for prestaging devices must wait after receiving the first notification for prestaging devices. For example, if you specify the prestage wait time as 20 seconds, the prestaging task waits for a period of 20 seconds, after receiving the first notification for prestaging devices, and then initiates the prestaging-devices job.
Pre-stage Idle Time (Sec)	Specify the number of seconds after which the job for prestaging devices is initiated, if no notification is received during the idle period. For example, if you specify the prestage idle time as 10 seconds and if no notification for prestaging devices is received within this period, the job for prestaging devices is triggered immediately after 10 seconds. The prestage idle time value takes precedence over the prestage wait time value.
Loopback Unit	Specify the logical unit of the loopback interface that must be used as the default loopback logical interface for all provisioning tasks that are initiated from Connectivity Services Director. The default logical unit for the loopback interface is 0.
Route Target	
BeginIndex	<p>Specify the least value in the preferred range of numbers, among which a certain number is assigned for each BGP service. Route target allows you to distribute VPN routes to only the routers that need them. When a route target value is entered manually, it should be either of the following two formats: Autonomous System number format or IPv4 format. For Autonomous System number format, the pattern is as-number:2-byte-number. For example, target:100:200.</p> <p>Range: The Autonomous System number format number can be in the range from 1 through 65,535.</p> <p>The IPv4 format is ip-address:2-byte-number. For example, target:10.1.1.1:2.</p>
EndIndex	<p>Specify the greatest value in the preferred range of numbers, among which a certain number is assigned for each BGP service. Route target allows you to distribute VPN routes to only the routers that need them. When a route target value is entered manually, it should be either of the following two formats: Autonomous System number format or IPv4 format. For Autonomous System number format, the pattern is as-number:2-byte-number. For example, target:100:200.</p> <p>Range: The Autonomous System number format number can be in the range from 1 through 65,535.</p> <p>The IPv4 format is ip-address:2-byte-number. For example, target:10.1.1.1:2. The EndIndex value should be lesser than the maximum assigned value.</p>
Virtual Circuit ID	

Table 14: Parameters in the Services Activation Tab (continued)

Fields	Description
BeginIndex	<p>Specify the least value in the preferred range of numbers, among which a certain number is assigned as the VirtualCircuitID to the new circuit created. This VCID can be manually chosen by the customer or auto-generated by the system. For example, if BeginIndex = 100 and EndIndex = 200, then the VCID would be somewhere between 100 and 200.</p> <p>Minimum: 1</p> <p>The value of BeginIndex should be less than or equal to EndIndex value.</p> <p>The range is from 0 through 200000.</p>
EndIndex	<p>Specify the greatest value in the preferred range of numbers, among which a certain number is assigned as the VirtualCircuitID to the new circuit created. This VCID can be manually chosen by the customer or auto-generated by the system. For example, if BeginIndex = 100 and EndIndex = 200, then the VCID would be somewhere between 100 and 200.</p> <p>Maximum: 2147483647.</p> <p>The range is from 0 through 200000.</p>
Performance Monitoring	
DataSetSize	<p>DataSetSize is the size of the performance monitoring data set in days. This field indicates the number of days of performance monitoring data could be stored for display.</p> <p>The default value is 2880.</p>
Enable Performance Monitoring through scripts	<p>Select the check box to collect the performance data through scripts and opennms will store the data in its database. If this check box is not selected, then performance data such as one-way delay, two-way delay, and frame loss are collected through RPC and stored in the application database.</p>
OSS Config Parameters	
Alcatel Primary Server IP	Specify the IP address of the primary server.
Alcatel Primary Server Port	Specify the port number of the primary server.
Backup Server IP	Specify the IP address of the backup server.
Backup Server Port	Specify the port number of the backup server.
HTTP Connection Timeout	Specify the duration of HTTP connection before the time-out elapses.
Maximum API Requests	Specify the maximum number of simultaneous API requests permitted.
OSS Log Directory	Specify the directory path of the OSS log directory.
OSS Log Filename	Specify the OSS log filename.
OSS User Name	Specify the user name for accessing the OSS server.

Table 14: Parameters in the Services Activation Tab (continued)

Fields	Description
OSS User Password	Specify the hashed password for accessing the OSS server.
Synchronize OSS Inventory daily at given time	Sets the daily time at which the CPP system synchronizes third-party devices, added or deleted from the CPP system, with the OSS server.
Use primary server	If the check box is enabled, the CPP system communicates with the primary OSS server.
Service Decommission	
Device Sync Wait Time	Specify the device synchronization waiting time. This is the maximum wait time to complete the device synchronization. After this time duration, irrespective of the device synchronization status, the resources are released. The default value is 60 seconds. The range is from 30 seconds through 300 seconds.
Wait for Device Sync Before Releasing Resource	Select this check box to wait for the device synchronization before resources are released. To revert the decommissioning to the normal behavior, clear this check box.
Service Recovery	
OutofBand Notification	Select either of the following options from the OutofBand Notification Action list to specify the action you want to be performed when an OutOfBand notification is received by Connectivity Services Director: <ul style="list-style-type: none"> • Make Device OutOfSync—Causes the device to be made OutOfSync and disables subsequent provisioning on that device until it changes to the In Sync state again • Ignore Notification—Causes the notification to be ignored and device will remain InSync
Store OutofBand Notification XML	Select the check box to enable the storage of OutOfBand notification XML in the Connectivity Services Director database. By default, this check box is not selected, which disables the saving of OutofBand notification XML in the Connectivity Services Director database.

Specifying Topology Preferences

From the **Topology** tab of the Preferences page (which you can launch by clicking the down arrow beside the System button on the Connectivity Services Director banner and selecting Preferences), you can specify the topology server IP and the credentials for enabling the Connectivity Services Director to connect to the topology server.

For Layer 2 topology settings, you can also disable the automatic updates to the topology and, instead, enable the topology updates to be manually triggered by selecting the **Disable Autoupdate of Topology** check box. In the **Deleted Link Retention Period (Days)** field, drag the square over the line to specify the number of days that you might want to retain the deleted link.

For Layer 3 topology settings, you can select or clear the **Use PCEP** check box. Select the **Use PCEP** check box to use the Path Computation Element Protocol (PCEP) for discovery of LSPs. PCEP enables communication between a PCC and the CSD-Topology to learn

about the network and LSP path state and communicate with the Path Computation Clients (PCCs). By default, this check box is not selected.

Enter the server IP address in the Topology Server field, and the authentication credentials in the Username and Password fields.

In the **Refresh Topology Interval (days)** field, drag the square over the line to specify the frequency in number of days at which the Layer 3 topology must be refreshed and displayed in the Topology View. By default, the topology is refreshed once every day. Drag the square to the leftmost end of the line to disable the refresh of topology. Drag the square to the rightmost end of the line to enable the refresh of topology once every 365 days or a year, which is the largest frequency you can specify for the refresh setting.

Changing Monitor Mode Settings

The Monitoring tab of Preferences has three tabs under it. These are:

- **Monitor Settings**—Enables you to change the default polling interval for data collection for Monitor mode monitors. You can also disable or reen able the internal processes used for data collection on this sub-tab.
- **Client Session History**—Enables you to set the retention period for history records and the frequency that these records are checked for deletion.

This section describes:

- [Disabling Data Collection for Monitors on page 129](#)
- [Changing the Polling Interval on page 130](#)
- [Specifying Database History Retention on page 131](#)

Disabling Data Collection for Monitors

Connectivity Services Director internally gathers data for monitors by using a set of data collection processes. You can disable these data collectors if they do not pertain to your installation. For example, if you do not use Virtual Chassis, you can disable the data collection processes used for Virtual Chassis.

The data collection processes are divided into the following categories:

- Equipment
- FM
- Traffic

One data collector can be used by multiple monitors. Likewise, some monitors can be supported by multiple data collectors. These data collectors are enabled by default. To ensure proper data collection, if you enable the equipment data collectors, you must also enable the traffic collectors..

To disable or reen able a data collector:

1. Determine which monitors are used by the data collectors. Use [Table 15 on page 130](#) to determine the relationship between the data collectors and the monitors.

Table 15: Monitor Mapping for Data Collectors

Monitor	Data Collector	Category
Show Interface Statistics	ProvisioningMonitorInterfaceStatsCollector	Equipment
Show Interface Status	ProvisioningMonitorInterfaceStatusCollector	Equipment
Service Traffic, Service Summary, Service Transport	ProvisioningMonitorServiceStatusCollector	Equipment
LSP Statistics	ProvisioningMonitorLSPStatsCollector	Equipment
LDP Statistics	ProvisioningMonitorLDPStatsCollector	Equipment
Service Performance	ProvisioningMonitorY1731PMCollector	Equipment
RFC2544 Benchmarking Tests	ProvisioningMonitoringRFC2544Poller	Equipment
Port Status (physical)	EquipmentMonitorDeviceStatusCollector	Equipment
Traffic Trend	PortTrafficMonitorCollector	Traffic
Alarms	FMAAlarmCountCollector	FM
Collection of LSPs and Service Association for Topology View	ProvisioningMonitorLSPToServiceAssociationCollector	Traffic

2. Clear the check box to disable the collector or select to enable the collector.
3. Click **Save** and **Close** to save the configuration and to close the window.

Changing the Polling Interval

The frequency at which data is collected is determined by the polling interval. [Table 16 on page 130](#) shows the default polling intervals used by each data collector.

Table 16: Default Polling Intervals

Collector	Polling Interval
ProvisioningMonitorInterfaceStatsCollector	5 minutes
ProvisioningMonitorInterfaceStatusCollector	10 minutes
ProvisioningMonitorServiceStatusCollector	10 minutes
ProvisioningMonitorLSPStatsCollector	10 minutes
ProvisioningMonitorLDPStatsCollector	5 minutes

Table 16: Default Polling Intervals (continued)

Collector	Polling Interval
ProvisioningMonitorY1731PMCollector	5 minutes
ProvisioningMonitoringRFC2544Poller	5 minutes
EquipmentMonitorDeviceStatusCollector	10 minutes
PortTrafficMonitorCollector	10 minutes
ProvisioningMonitorLSPToServiceAssociationCollector	5 minutes

To change the polling interval:

1. Select the polling interval for a data collector in the Monitor Settings table.
2. Type the new interval level in whole minutes. For example, do not specify 1.5 minutes. Recommended intervals are 5, 10, or 20 minutes.
3. Click **OK** and then **Yes** to verify the change to the configuration.

Specifying Database History Retention

To keep the database manageable, the system periodically checks the age of the records and retires those that have past an expiration date. By default, Connectivity Services Director ages database records off at 90 days and runs a database cleanup every 6 hours.

Use the Client Session History sub-tab to change the default values:

1. Select from the lists new values.
 - Age of history records (in days) from 1 to 365 days.
 - Cleanup job frequency (in hours) from 1 through 24 hours.
2. Click **OK** to save the changes.

Changing Alarm Settings

Use the Fault tab to enable individual alarms, set the retention period for alarms, configure alarm notifications, configure threshold alarms, and to specify the number of events to keep for each alarm. The Fault tab has multiple sections, which you can expand and collapse by clicking the arrow next to the section title:

- Global Settings, for configuring Faults settings such as global alarm notifications and alarm data retention.
- Individual Alarms and Threshold Settings, for configuring settings for individual alarms and threshold alarms.

This section describes the following tasks that you can perform by using the Fault tab:

- [Configuring Global Alarm Notifications on page 132](#)
- [Retaining Alarm History on page 132](#)
- [Specifying Event History on page 132](#)
- [Enabling Alarms on page 132](#)
- [Changing the Severity of Individual Alarms on page 152](#)
- [Configuring Threshold Alarms on page 152](#)
- [Configuring Individual Alarm Notifications on page 152](#)

Configuring Global Alarm Notifications

You can configure global e-mail notifications to be sent when any alarm with notifications enabled is generated. To configure global e-mail notifications, enter the e-mail addresses to receive global alarm notifications in the Alarm Notifications Destinations field in the Global Settings section. Separate addresses with a comma (,). For information about enabling notification for an alarm, see [“Configuring Individual Alarm Notifications” on page 152](#).

Retaining Alarm History

Use the **No. of days to keep Alarm** field in the Global Settings section to specify the number of days to keep alarm history. The default retention time is 120 days; but you can specify a period of 7 through 1000 days. Specifying a longer retention time consumes more database resources. To change the alarm retention duration, type a new value and click **OK** and **Yes** to confirm the change.

Specifying Event History

Use the **Events/Alarm** field in the Global Settings section to specify the number of event entries that are kept in the alarm history. The default setting for events is 20. To change the setting, type a new value and click **OK** and **Yes** to confirm the change.

Enabling Alarms

Ensure all devices are configured to send traps to Connectivity Services Director. This task is performed for the devices in Deploy mode through Set SNMP Trap Configuration.

Use the Individual Alarms and Threshold Settings section to disable and re-enable individual alarms or all alarms. Alarms appear on both tabs in the section: Alarm Settings and Threshold Settings. Fault alarms are preconfigured and initially enabled. To enable or disable alarms:

1. (Optional) Sort the alarms. By default, the list of alarms is sorted alphabetically within each category. You can also sort by description or alarm severity within a category by clicking a column heading.
2. Review the alarms and either select the check box in the heading to select all of the alarms or select the check box for the individual alarms you want to enable. For a full description of each of the alarms, see [Table 17 on page 133](#).

3. Click **OK** and **Yes** to confirm the alarm change.

Table 17: Alarm Descriptions

Alarm Name	Description	Device Type
<i>BFD</i>		
BfdSessionDetectionTimeAlarm	Generated when the threshold value for detection time is set and the BFD session detection-time adapts to a value greater than the threshold.	ACX, M, MX, and PTX Series routers
BfdSessionTxAlarm	Generated when the threshold value for transmit interval (in microseconds) is exceeded.	ACX, M, MX, and PTX Series routers
<i>BGP</i>		
BgpM2BackwardTransitionAlarm	Generated when the BGP FSM moves from a higher-numbered state to a lower-numbered state.	ACX, M, MX, and PTX Series routers
BgpM2EstablishedAlarm	Generated when the BGP Finite State Machine (FSM) enters the ESTABLISHED state.	ACX, M, MX, and PTX Series routers
<i>Chassis</i>		
FanFailureAlarm	Generated when the specified cooling fan or impeller has failed (is not spinning).	ACX, M, MX, and PTX Series routers
FEBSwitchoverAlarm	Generated when the Forwarding Engine Board (FEB) has switched over.	ACX, M, MX, and PTX Series routers
FRUCheckAlarm	Generated when the device has detected that a field-replaceable unit (FRU), has some operational errors and has gone into check state.	ACX, M, MX, and PTX Series routers
FRUFailedAlarm	Generated when a FRU has failed.	ACX, M, MX, and PTX Series routers
FRUInsertionAlarm	Generated when the system detects that the specified FRU is inserted into the chassis.	ACX, M, MX, and PTX Series routers
FRUOfflineAlarm	Generated when the specified FRU goes offline.	ACX, M, MX, and PTX Series routers
FRUOnlineAlarm	Generated when the specified FRU goes online.	ACX, M, MX, and PTX Series routers
FRUPowerOffAlarm	Generated when the specified FRU is powered off.	ACX, M, MX, and PTX Series routers
FRUPowerOnAlarm	Generated when the specified FRU is powered on.	ACX, M, MX, and PTX Series routers

Table 17: Alarm Descriptions (continued)

Alarm Name	Description	Device Type
FRURemovalAlarm	Generated when the system detects that the specified FRU was removed from the chassis.	ACX, M, MX, and PTX Series routers
HardDiskFailedAlarm	Generated when the hard disk for the specified routing engine has failed.	ACX, M, MX, and PTX Series routers
HardDiskMissingAlarm	Generated when the hard disk in the specified routing engine is missing from the boot device list.	ACX, M, MX, and PTX Series routers
PowerSupplyFailureAlarm	Generated when the specified power supply has failed (bad DC output).	ACX, M, MX, and PTX Series routers
RedundancySwitchOverAlarm	Generated when a graceful Routing Engine switchover (GRES) occurs on a switch with dual Routing Engines or on a Virtual Chassis.	ACX, M, MX, and PTX Series routers
TemperatureAlarm	Generated when the device has over heated.	ACX, M, MX, and PTX Series routers
<i>Cluster/Mode</i>		
Cluster Sync Failure	Generated when the cluster configuration failed to apply.	ACX, M, MX, and PTX Series routers
<i>Configuration (Configuration)</i>		
CmCfgChangeAlarm	Generated when the jnxCMCfgChgEventTable records a configuration management event.	ACX, M, MX, and PTX Series routers
CMRescueChangeAlarm	Generated when a change is made to the rescue configuration.	ACX, M, MX, and PTX Series routers
<i>Core and controllers (Controllers)</i>		
Device alarm	Generated when the device status changes (up to down or down to up).	ACX, M, MX, and PTX Series routers
<i>CoS</i>		
CoSAlmostOutOfDedicatedQueuesAlarm	Generated when only 10% of CoS queues are available.	ACX, M, MX, and PTX Series routers
CoSOutOfDedicatedQueuesAlarm	Generated when there are no more available dedicated CoS queues.	ACX, M, MX, and PTX Series routers
<i>DHCP</i>		
JdhcpLocalServerDupClientAlarm	Generated when a DHCP client is detected changing interfaces.	ACX, M, MX, and PTX Series routers

Table 17: Alarm Descriptions (continued)

Alarm Name	Description	Device Type
JdhcpLocalServerIfLimitExceededAlarm	Generated when the client limit is reached on an interface.	ACX, M, MX, and PTX Series routers
Jdhcpv6LocalServerLimitExceededAlarm	Generated when the client limit is reached on an interface for DHCPv6.	ACX, M, MX, and PTX Series routers
<i>DOM</i>		
DomAlertSetAlarm	Generated when an interface detects Digital Optical Monitor (DOM) alarm conditions.	ACX, M, MX, and PTX Series routers
<i>General</i>		
Authentication Failure Alarm	Generated when a protocol message is received that is not properly authenticated.	ACX, M, MX, and PTX Series routers
Cold Start Alarm	Generated when a device is re-initializing and its configuration might have changed.	ACX, M, MX, and PTX Series routers
Link Down Alarm	Generated when a link is down. The trap is generated when the ifOperStatus object for a communication link is about to enter the down state from another state other than notPresent. This other state is indicated by the included value of ifOperStatus.	ACX, M, MX, and PTX Series routers
Link Up Alarm	Generated when a link comes up that was previously in the down state. The trap is generated when the ifOperStatus object for a communication link left the down state and transitioned into another state other than notPresent state. This other state is indicated by the included value of ifOperStatus.	ACX, M, MX, and PTX Series routers
Warm Start Alarm	Generated when a device is re-initializing and its configuration has not changed.	ACX, M, MX, and PTX Series routers
<i>Generic (GenericEvent)</i>		
GenericEventTrapAlarm	Generated by an Op script or event policies. This notification can include one or more attribute-value pairs. The pairs are identified by the jnxEventAvAttribute and jnxEventAvValue objects.	ACX, M, MX, and PTX Series routers
<i>OTN Notification</i>		

Table 17: Alarm Descriptions (continued)

Alarm Name	Description	Device Type
FRU: OTN Admin Notification Set	Generated as a notification of an OTM alarm that is set. An alarm is triggered when an optical PIC or field-replaceable unit (FRU) is removed or reinserted, or transitions between in-service and out-of-service states.	PTX Series routers
ODU::OdukPtmAlarm	Generated as Optical Channel Payload (OPU) Payload Type Mismatch defect trigger.	PTX Series routers
ODU::OdukTcm	Generated as OC target of evaluation (TOE) security functionality (TSF) defect trigger.	PTX Series routers
ODU::OdukTcm15MinThreshBBETCA	Generated as ODU Background Block Error Threshold crossing defect trigger in the 15-minute interval threshold.	PTX Series routers
ODU::OdukTcm15MinThreshBip8TCA	Generated as ODU Bit interleaved parity for SONET section overhead defect trigger in the 15-minute interval threshold.	PTX Series routers
ODU::OdukTcm15MinThreshESTCA	Generated as ODU errored seconds threshold-crossing defect trigger in the 15-minute interval threshold.	PTX Series routers
ODU::OdukTcm15MinThreshSESTCA	Generated as ODU severely errored seconds threshold-crossing defect trigger in the 15-minute interval threshold.	PTX Series routers
ODU::OdukTcm15MinThreshUASTCA	Generated as ODU unavailable seconds threshold-crossing defect trigger in the 15-minute interval threshold.	PTX Series routers
ODU::OdukTcm15MinThreshBBETCA	Generated as ODU Background Block Error Threshold crossing defect trigger in the 15-minute interval threshold.	PTX Series routers
ODU::OdukTcm24HourThreshBip8TCA	Generated as ODU Bit interleaved parity for SONET section overhead defect trigger in the 24-hour or 1-day interval threshold.	PTX Series routers
ODU::OdukTcm24HourThreshESTCA	Generated as ODU errored seconds threshold-crossing defect trigger in the 24-hour or 1-day interval threshold.	PTX Series routers
ODU::OdukTcm24HourThreshSESTCA	Generated as ODU severely errored seconds threshold-crossing defect trigger in the 24-hour or 1-day interval threshold.	PTX Series routers
ODU::OdukTcm24HourThreshUASTCA	Generated as ODU unavailable seconds threshold-crossing defect trigger in the 24-hour or 1-day interval threshold.	PTX Series routers

Table 17: Alarm Descriptions (continued)

Alarm Name	Description	Device Type
ODU::OdukTcmAisAlarm	Generated as ODU Alarm Indication Signal defect trigger.	PTX Series routers
ODU::OdukTcmBdiAlarm	Generated as ODU Backward Defect Indication defect trigger.	PTX Series routers
ODU::OdukTcmCSfAlarm	Generated as ODU client signal failure alarm.	PTX Series routers
ODU::OdukTcmDegAlarm	Generated as ODU degradation alarm.	PTX Series routers
ODU::OdukTcmIaeAlarm	Generated as ODU incoming alignment error alarm.	PTX Series routers
ODU::OdukTcmLTCAAlarm	Generated as ODU threshold crossing alert (TCA) alarm.	PTX Series routers
ODU::OdukTcmLckAlarm	Generated as ODU locked defect trigger.	PTX Series routers
ODU::OdukTcmOciAlarm	Generated as ODU open connection indication alarm.	PTX Series routers
ODU::OdukTcmSSfAlarm	Generated as ODU server signal failure alarm.	PTX Series routers
ODU::OdukTcmTimAlarm	Generated as ODU trace identifier mismatch alarm.	PTX Series routers
ODU::OtnOdukTcmNoAlarm	Generated as ODU no-alarm when threshold crossing alert occurs.	PTX Series routers
OTN Admin Notification Set	Generated as a notification when OTN alarm is set.	PTX Series routers
OTU::OdukTcmAisAlarm	Generated as OTU alarm indication signal trigger.	PTX Series routers
OTU::15MinThUnCorrectedWordsTCA	Generated as an alarm when OTU uncorrected words in the 15-minute threshold is exceeded.	PTX Series routers
OTU::15MinThreshBBETCA	Generated as an alarm when OTU background block error count in the 15-minute threshold is exceeded.	PTX Series routers
OTU::15MinThreshBip8TCA	Generated as an alarm when OTU bit interleaved parity count in the 15-minute threshold is exceeded.	PTX Series routers
OTU::15MinThreshESTCA	Generated as an alarm when errored seconds count in the 15-minute threshold is exceeded.	PTX Series routers

Table 17: Alarm Descriptions (continued)

Alarm Name	Description	Device Type
OTU::15MinThreshSESTCA	Generated as an alarm when severely errored seconds count in the 15-minute threshold is exceeded.	PTX Series routers
OTU::15MinThreshPreFECBERTCA	Generated as an alarm when pre-forward error correction bit error rate count in the 15-minute threshold is exceeded.	PTX Series routers
OTU::15MinThreshUASTCA	Generated as an alarm when unavailable seconds count in the 15-minute threshold is exceeded.	PTX Series routers
OTU::24HourThreshBBETCA	Generated as an alarm when OTU background block error count in the 24-hour threshold is exceeded.	PTX Series routers
OTU::24HourThreshBip8TCA	Generated as an alarm when OTU bit interleaved parity count in the 24-hour threshold is exceeded.	PTX Series routers
OTU::24HourThreshESTCA	Generated as an alarm when errored seconds count in the 24-hour threshold is exceeded.	PTX Series routers
OTU::24HourThreshPreFECBERTCA	Generated as an alarm when severely errored seconds count in the 24-hour threshold is exceeded.	PTX Series routers
OTU::24HourThreshSESTCA	Generated as an alarm when pre-forward error correction bit error rate count in the 24-hour threshold is exceeded.	PTX Series routers
OTU::24HourThreshUASTCA	Generated as an alarm when unavailable seconds count in the 24-hour threshold is exceeded.	PTX Series routers
OTU:OtnLofAlarm	Generated as an OTN loss of signal alarm.	PTX Series routers
OTU:OtnLosAlarm	Generated as an OTN loss of frame alarm.	PTX Series routers
OTU:OtnLomAlarm	Generated as an OTN loss of multiframe alarm.	PTX Series routers
OTU:OtnNoAlarm	Generated as an OTN no alarm.	PTX Series routers
OTU:OtuBdiAlarm	Generated as an OTU backward defect indication alarm.	PTX Series routers
OTU:OtuBiaeAlarm	Generated as an OTU backward error indication alarm.	PTX Series routers
OTU:OtuDegAlarm	Generated as an OTU degraded alarm.	PTX Series routers
OTU:OtuFecExcessiveErrsAlarm	Generated as an OTU excessive errors alarm.	PTX Series routers

Table 17: Alarm Descriptions (continued)

Alarm Name	Description	Device Type
OTU:OtuIaeAlarm	Generated as an OTU incoming alignment defect alarm.	PTX Series routers
OTU:OtuSsAlarm	Generated as an OTU server signal alarm.	PTX Series routers
OTU:OtuTimAlarm	Generated as an OTN trail trace identifier mismatch defect alarm.	PTX Series routers
OTU:OtuTsfAlarm	Generated as an OTU TOE security functionality (TSF) alarm.	PTX Series routers
Optical::LOS	Generated as input loss of signal alarm.	PTX Series routers
Optical::WavelengthLockErr	Generated as wavelength lock error alarm.	PTX Series routers
Optical::PowerHighAlarm	Generated as Tx high power alarm.	PTX Series routers
Optical::PowerLowAlarm	Generated as Tx low power alarm.	PTX Series routers
Optical::BiasCurrentHighAlarm	Generated as Bias Current High alarm.	PTX Series routers
Optical::BiasCurrentLowAlarm	Generated as Bias Current Low alarm.	PTX Series routers
Optical::TemperatureHighAlarm	Generated as Temperature High alarm.	PTX Series routers
Optical::TemperatureLowAlarm	Generated as Temperature low alarm.	PTX Series routers
Optical::TxPLLLockAlarm	Generated as transmitted phase-locked loop lock alarm.	PTX Series routers
Optical::RxPLLLockAlarm	Generated as received phase-locked loop lock alarm.	PTX Series routers
Optical::AvgPowerAlarm	Generated as average power alarm.	PTX Series routers
Optical::RxLossAvgPowerAlarm	Generated as Rx Loss Avg Power alarm.	PTX Series routers
Optical::LossOfACPowerAlarm	Generated as Loss of AC Power alarm.	PTX Series routers
Optical::TxPowerHighThreshAlert	Generated as transmitted temperature high threshold setting trigger.	PTX Series routers
Optical::TxPowerLowThreshAlert	Generated as transmitted temperature low threshold setting trigger.	PTX Series routers
Optical::RxPowerHighThreshAlert	Generated as received temperature high threshold setting trigger.	PTX Series routers

Table 17: Alarm Descriptions (continued)

Alarm Name	Description	Device Type
Optical::RxPowerLowThreshAlert	Generated as received temperature low threshold setting trigger.	PTX Series routers
Optical::ModuleTempHighThreshAlert	Generated as temperature high threshold setting trigger.	PTX Series routers
Optical::ModuleTempLowThreshAlert	Generated as temperature low threshold setting trigger.	PTX Series routers
Optical::24HourTxPowerHighThreshAlert	Generated as transmitted temperature high threshold setting trigger within the 24-hour period.	PTX Series routers
Optical::24HourTxPowerLowThreshAlert	Generated as transmitted temperature low threshold setting trigger within the 24-hour period.	PTX Series routers
Optical::24HourRxPowerHighThreshAlert	Generated as received temperature high threshold setting trigger within the 24-hour period.	PTX Series routers
Optical::24HourRxPowerLowThreshAlert	Generated as received temperature low threshold setting trigger within the 24-hour period.	PTX Series routers
Optical::24HourModuleTempHighThreshAlert	Generated as temperature high threshold setting trigger within the 24-hour period.	PTX Series routers
Optical::24HourModuleTempLowThreshAlert	Generated as temperature low threshold setting trigger within the 24-hour period.	PTX Series routers
Optical::RxPowerHighAlarm	Generated as received high power alarm.	PTX Series routers
Optical::RxPowerLowAlarm	Generated as received low power alarm.	PTX Series routers
Optical::TxPowerHighWarning	Generated as Rx high power warning.	PTX Series routers
Optical::TxPowerLowWarning	Generated as Rx high power warning.	PTX Series routers
Optical::RxPowerHighWarning	Generated as Rx high power warning.	PTX Series routers
Optical::RxPowerLowWarning	Generated as Rx high power warning.	PTX Series routers
Optical::ModuleTempHigh	Generated as module temperature high warning.	PTX Series routers
Optical::ModuleTempLowWarning	Generated as module temperature low warning.	PTX Series routers
Optical::RxCarrierFreqHigh	Generated as received carrier frequency high warning.	PTX Series routers
Optical::RxCarrierFreqLow	Generated as received carrier frequency low warning.	PTX Series routers

Table 17: Alarm Descriptions (continued)

Alarm Name	Description	Device Type
Optical::ChromaticDispHighWarning	Generated as chromatic dispersion high warning.	PTX Series routers
Optical::ChromaticDispLowWarning	Generated as chromatic dispersion low warning.	PTX Series routers
Optical::QLowWarning	Generated as low quality factor warning.	PTX Series routers
Optical::OSNRLowWarning	Generated as low signal-to-noise ratio warning.	PTX Series routers
Optical::CarrierFreqHighAlert	Generated as carrier frequency high threshold setting trigger.	PTX Series routers
Optical::CarrierFreqLowAlert	Generated as carrier frequency low threshold setting trigger.	PTX Series routers
Optical::24HourCarrierFreqHighAlert	Generated as carrier frequency high threshold setting trigger within the 24-hour threshold interval period.	PTX Series routers
Optical::24HourCarrierFreqLowAlert	Generated as carrier frequency low threshold setting trigger within the 24-hour threshold interval period.	PTX Series routers
<i>ILA Notification</i>		
ILA::edfaEabCalTableErr	Generated when the EDFA in the direction from optical supervisory channel (OSC) A to OSC B (Eab) has a calibration table error.	PTX Series routers
ILA::edfaEabCaseTemperature	Generated when the EDFA case temperature exceeds the configured threshold in the direction from OSC A to OSC B.	PTX Series routers
ILA::edfaEabInputLOS	Generated when the input loss of signal (LOS) is detected in the direction from OSC A to OSC B.	PTX Series routers
ILA::edfaEabOOG	Generated when the Out-of-Service Out-of-Group (OOS OOG) condition occurs in the direction from OSC A to OSC B.	PTX Series routers
ILA::edfaEabOOP	Generated when the Out-of-Policy (OOP) condition occurs in the direction from OSC A to OSC B.	PTX Series routers
ILA::edfaEabOutputLOS	Generated when an output LOS condition occurs in the direction from OSC A to OSC B.	PTX Series routers
ILA::edfaEabPump1EOL	Generated when the end-of-life (EoL) state for pump 1 of the EDFA occurs in the direction from OSC A to OSC B.	PTX Series routers

Table 17: Alarm Descriptions (continued)

Alarm Name	Description	Device Type
ILA::edfaEabPump2EOL	Generated when the end-of-life (EoL) state for pump 2 of the EDFA occurs in the direction from OSC A to OSC B.	PTX Series routers
ILA::edfaEabPump1Temperature	Generated when the temperature exceeds the threshold for pump 1 of the EDFA occurs in the direction from OSC A to OSC B.	PTX Series routers
ILA::edfaEabPump2Temperature	Generated when the temperature exceeds the threshold for pump 1 of the EDFA occurs in the direction from OSC A to OSC B.	PTX Series routers
ILA::edfaEabRFL	Generated when the radio frequency loss (RFL) occurs for the EDFA occurs in the direction from OSC A to OSC B.	PTX Series routers
ILA::edfaEbaCaliTableErr	Generated when the EDFA in the direction from optical supervisory channel (OSC) B to OSC A (Eba) has a calibration table error.	PTX Series routers
ILA::edfaEbaCaseTemperature	Generated when the EDFA case temperature exceeds the configured threshold in the direction from OSC B to OSC A.	PTX Series routers
ILA::edfaEbaInputLOS	Generated when the input loss of signal (LOS) is detected in the direction from OSC B to OSC A.	PTX Series routers
ILA::edfaEbaOOG	Generated when the Out-of-Gain (OOG) condition occurs in the direction from OSC B to OSC A.	PTX Series routers
ILA::edfaEbaOOP	Generated when the Out-of-Power (OOP) condition occurs in the direction from OSC B to OSC A.	PTX Series routers
ILA::edfaEbaOutputLOS	Generated when an output LOS condition occurs in the direction from OSC B to OSC A.	PTX Series routers
ILA::edfaEbaPump1EOL	Generated when the end-of-life (EoL) state for pump 1 of the EDFA occurs in the direction from OSC B to OSC A.	PTX Series routers
ILA::edfaEbaPump2EOL	Generated when the end-of-life (EoL) state for pump 2 of the EDFA occurs in the direction from OSC B to OSC A.	PTX Series routers
ILA::edfaEbaPump1Temperature	Generated when the temperature exceeds the threshold for pump 1 of the EDFA occurs in the direction from OSC B to OSC A.	PTX Series routers

Table 17: Alarm Descriptions (continued)

Alarm Name	Description	Device Type
ILA::edfaEbaPump2Temperature	Generated when the temperature exceeds the threshold for pump 1 of the EDFA occurs in the direction from OSC B to OSC A.	PTX Series routers
ILA::edfaEbaRFL	Generated when the radio frequency loss (RFL) occurs for the EDFA occurs in the direction from OSC B to OSC A.	PTX Series routers
ILA::ilaBoardTemperatureAbnormal	Generated when the ILA board temperature reaches an abnormal level.	PTX Series routers
ILA::ilaCommunicationAbnormal	Generated when the communication channel between the NMS system and the ILA reaches an abnormal level.	PTX Series routers
ILA::ilaACPowerAbnormal	Generated when the ILA AC power reaches an abnormal level.	PTX Series routers
ILA::ilaDCPowerAbnormal	Generated when the ILA DC power reaches an abnormal level.	PTX Series routers
ILA::ilaFan1OnlineAbnormal	Generated when the ILA fan tray controller 1 that is online reaches an abnormal level.	PTX Series routers
ILA::ilaFan1SpeedAbnormal	Generated when the speed of the ILA fan tray controller 1 reaches an abnormal level.	PTX Series routers
ILA::ilaFan2OnlineAbnormal	Generated when the ILA fan tray controller 1 that is online reaches an abnormal level.	PTX Series routers
ILA::ilaFan2SpeedAbnormal	Generated when the speed of the ILA fan tray controller 1 reaches an abnormal level.	PTX Series routers
ILA::ilaFan3OnlineAbnormal	Generated when the ILA fan tray controller 1 that is online reaches an abnormal level.	PTX Series routers
ILA::ilaFan3SpeedAbnormal	Generated when the speed of the ILA fan tray controller 1 reaches an abnormal level.	PTX Series routers
ILA::ilaSoftwareVersionAbnormal	Generated when the ILA software version reaches an abnormal level.	PTX Series routers
ILA::ilaTableErr	Generated when the ILA table error occurs.	PTX Series routers
ILA::oscaAddPowerLOS	Generated when the addition of power LOS condition occurs for the OSC A.	PTX Series routers
ILA::oscaDropPowerLOS	Generated when the dropping of power LOS condition occurs for the OSC A.	PTX Series routers

Table 17: Alarm Descriptions (continued)

Alarm Name	Description	Device Type
ILA::oscbAddPowerLOS	Generated when the addition of power LOS condition occurs for the OSC B.	PTX Series routers
ILA::oscbDropPowerLOS	Generated when the dropping of power LOS condition occurs for the OSC B.	PTX Series routers
<i>IPLC Notification</i>		
jnxlplcFpcAwgAddLosAlarm	Generated as the FPC arrayed waveguide gratings (AWG) add LOS alarm for the IPLC	PTX3000 Packet Transport Routers
jnxlplcFpcExpInLosAlarm	Generated as the FPC input LOS alarm for the express-in mode of the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcOscAddLosAlarm	Generated as the FPC add LOS alarm for the optical supervisory channel (OSC) of the IPLC. The OSC is an in-band channel used to communicate with ILAs and other optical nodes in the line system that are not directly accessible over the DCN. OSC framing logic is implemented in the FPGA.	PTX3000 Packet Transport Routers
jnxlplcFpcOscDrpLosAlarm	Generated as the FPC drop LOS alarm for the OSC of the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcLineInLosAlarm	Generated as the FPC input line-in LOS alarm for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcEdfa1RefPwAlarm	Generated as the FPC erbium doped fiber amplifier (EDFA) 1 reflect power alarm for the IPLC. EDFA1 is considered as ingress EDFA and EDFA2 is considered as egress EDFA	PTX3000 Packet Transport Routers
jnxlplcFpcEdfa1OutPwAlarm	Generated as the FPC EDFA1 output power alarm for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcEdfa1OutGain	Generated as the FPC EDFA1 output gain alarm for the IPLC	PTX3000 Packet Transport Routers
jnxlplcFpcEdfa1PumpEolAlarm	Generated as the FPC EDFA1 pump end-of-life (EoL) alarm for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcEdfa1TempAlarm	Generated as the FPC EDFA1 temperature alarm for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcEdfa1OutLosAlarm	Generated as the FPC EDFA1 output LOS alarm for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcEdfa1InLosAlarm	Generated as the FPC EDFA1 input LOS alarm for the IPLC.	PTX3000 Packet Transport Routers

Table 17: Alarm Descriptions (continued)

Alarm Name	Description	Device Type
jnxlplcFpcEdfa2RefPwAlarm	Generated as the FPC erbium doped fiber amplifier (EDFA) 1 reflect power alarm for the IPLC. EDFA1 is considered as ingress EDFA and EDFA2 is considered as egress EDFA	PTX3000 Packet Transport Routers
jnxlplcFpcEdfa2OutPwAlarm	Generated as the FPC EDFA2 output power alarm for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcEdfa2OutGainAlarm	Generated as the FPC EDFA2 output gain alarm for the IPLC	PTX3000 Packet Transport Routers
jnxlplcFpcEdfa2PumpEolAlarm	Generated as the FPC EDFA2 pump end-of-life (EoL) alarm for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcEdfa2TempAlarm	Generated as the FPC EDFA2 temperature alarm for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcEdfa2OutLosAlarm	Generated as the FPC EDFA2 output LOS alarm for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcEdfa2InLosAlarm	Generated as the FPC EDFA2 input LOS alarm for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcWssTempAlarm	Generated as the FPC wavelength selective switching (WSS) temperature alarm for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcWssVoltAlarm	Generated as the FPC WSS voltage alarm for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcInterDiagAlarm	Generated as the FPC internal diagnostic alarm for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcFwCnsistAlarm	Generated as the FPC firmware consistency alarm for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcHwFailAlarm	Generated as the FPC hardware failure alarm for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcFwFailAlarm	Generated as the FPC firmware failure alarm for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcOcmFailAlarm	Generated as the FPC optical channel module (OCM) failure alarm for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcWssFailAlarm	Generated as the FPC WSS failure alarm for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcEdfa2FailAlarm	Generated as the FPC EDFA2 failure alarm for the IPLC.	PTX3000 Packet Transport Routers

Table 17: Alarm Descriptions (continued)

Alarm Name	Description	Device Type
jnxlplcFpcEdfa1FailAlarm	Generated as the FPC EDFA1 alarm for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcPwrFailAlarm	Generated as the FPC power rail failure alarm for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcOscTxPowerHigh15minAlert	Generated as an alarm when the OSC transmitted high power exceeds the threshold within the 15-minute interval for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcOscTxPowerLow15minAlert	Generated as an alarm when the OSC transmitted low power exceeds the threshold within the 15-minute interval for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcOscRxPowerHigh15minAlert	Generated as an alarm when the OSC received high power exceeds the threshold within the 15-minute interval for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcOscRxPowerLow15minAlert	Generated as an alarm when the OSC received low power exceeds the threshold within the 15-minute interval for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcOscFiberLosHigh15minAlert	Generated as an alarm when the OSC fiber high LOS exceeds the threshold within the 15-minute interval for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcOscFiberLosLow15minAlert	Generated as an alarm when the OSC fiber low LOS exceeds the threshold within the 15-minute interval for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcLineOutVoaHigh15minAlert	Generated as the line-out Variable Optical Attenuator (VOA) high threshold setting trigger within the 15-minute period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcLineOutVoaLow15minAlert	Generated as the line-out Variable Optical Attenuator (VOA) low threshold setting trigger within the 15-minute period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcIngressEdfaInputPwHigh15minAlert	Generated as the ingress EDFA input power high threshold setting trigger within the 15-minute period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcIngressEdfaInputPwLow15minAlert	Generated as the ingress EDFA input power low threshold setting trigger within the 15-minute period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcOcmPwHigh15minAlert	Generated as the OCM module power high threshold setting trigger within the 15-minute period for the IPLC.	PTX3000 Packet Transport Routers

Table 17: Alarm Descriptions (continued)

Alarm Name	Description	Device Type
jnxlplcOcmPwLow15minAlert	Generated as the OCM module power low threshold setting trigger within the 15-minute period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcOscTxPowerHigh24hourAlert	Generated as the OSC transmitted high power threshold setting trigger within the 15-minute period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcOscTxPowerLow24hourAlert	Generated as the OSC transmitted high power threshold setting trigger within the 15-minute period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcOscRxPowerHigh24hourAlert	Generated as an alarm when the OSC received high power exceeds the threshold within the 24-hour interval for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcOscRxPowerLow24hourAlert	Generated as an alarm when the OSC received low power exceeds the threshold within the 24-hour interval for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcOscFiberLosHigh24hourAlert	Generated as an alarm when the OSC fiber high LOS exceeds the threshold within the 24-hour interval for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcOscFiberLosLow24hourAlert	Generated as an alarm when the OSC fiber low LOS exceeds the threshold within the 24-hour interval for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcLineOutVoaHigh24hourAlert	Generated as the line-out Variable Optical Attenuator (VOA) high threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcLineOutVoaLow24hourAlert	Generated as the line-out Variable Optical Attenuator (VOA) low threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcIngressEdfaInputPwHigh24hourAlert	Generated as the ingress EDFA input high power threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcIngressEdfaInputPwLow24hourAlert	Generated as the ingress EDFA input low power threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcIngressEdfaOutputPwHigh24hourAlert	Generated as the ingress EDFA output high power threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcIngressEdfaOutputPwLow24hourAlert	Generated as the ingress EDFA output low power threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers

Table 17: Alarm Descriptions (continued)

Alarm Name	Description	Device Type
jnxlplcIngressEdfaSignalPwHigh24hourAlert	Generated as the ingress EDFA signal high power threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcIngressEdfaSignalPwLow24hourAlert	Generated as the ingress EDFA signal low power threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcIngressEdfaPumpCurrentHigh24hourAlert	Generated as the ingress EDFA pump current high temperature threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcIngressEdfaPumpCurrentLow24hourAlert	Generated as the ingress EDFA pump current low temperature threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcEgressEdfaInputPwHigh24hourAlert	Generated as the egress EDFA input high power threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcEgressEdfaInputPwLow24hourAlert	Generated as the egress EDFA input low power threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcEgressEdfaOutputPwHigh24hourAlert	Generated as the egress EDFA output high power threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcEgressEdfaOutputPwLow24hourAlert	Generated as the egress EDFA output low power threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcEgressEdfaSignalPwHigh24hourAlert	Generated as the egress EDFA signal high power threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcEgressEdfaSignalPwLow24hourAlert	Generated as the egress EDFA signal low power threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcEgressEdfaPumpCurrentHigh24hourAlert	Generated as the egress EDFA pump current high temperature threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcEgressEdfaPumpCurrentLow24hourAlert	Generated as the egress EDFA pump current low temperature threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcPowerMonitorAwgAddHigh24hourAlert	Generated as the power monitor AWG add high threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers

Table 17: Alarm Descriptions (continued)

Alarm Name	Description	Device Type
jnxlplcPowerMonitorAwgAddLow24hourAlert	Generated as the power monitor AWG add low threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcPowerMonitorExpressInHigh24hourAlert	Generated as the power monitor express-in mode high threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcPowerMonitorExpressInLow24hourAlert	Generated as the power monitor express-in mode low threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcOcmPwHigh24hourAlert	Generated as the OCM module power high threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcOcmPwLow24hourAlert	Generated as the OCM module power low threshold setting trigger within the 24-hour period for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcSfpLosAlarm	Generated as the FPC SFP loss of signal (LOS) alarm for the IPLC.	PTX3000 Packet Transport Routers
jnxlplcFpcSfpLofAlarm	Generated as the FPC SFP loss of frame (LOF) alarm for the IPLC.	PTX3000 Packet Transport Routers
<i>L2ALD</i>		
L2aldGlobalMacLimitAlarm	Generated when the MAC limit is reached for the entire system. This trap is sent only once, when the limit is reached.	ACX, M, MX, and PTX Series routers
L2aldInterfaceMacLimitAlarm	Generated when the given interface reaches the MAC limit (jnxl2aldInterfaceMacLimit).	ACX, M, MX, and PTX Series routers
L2aldRoutingInstMacLimitAlarm	Generated when the MAC limit is reached for a given routing instance (jnxl2aldRoutingInst).	ACX, M, MX, and PTX Series routers
<i>L2CP</i>		
LacpTimeOutAlarm	Generated when LACP has timed out.	ACX, M, MX, and PTX Series routers
PortBpduErrorStatusChangeTrapAlarm	Generated when the port's BPDU error state (no-error or detected) changes.	ACX, M, MX, and PTX Series routers
PortLoopProtectStateChangeTrapAlarm	Generated when the port's loop-protect state (no-error or loop-prevented) changes.	ACX, M, MX, and PTX Series routers

Table 17: Alarm Descriptions (continued)

Alarm Name	Description	Device Type
PortRootProtectStateChangeTrapAlarm	Generated when the port's root-protect state (no-error or root-prevented) changes.	ACX, M, MX, and PTX Series routers
<i>MAC Forwarding Database (MACFDB)</i>		
MacChangedNotificationAlarm	Generated when MAC addresses of the monitored devices are learned or removed from the forwarding database (FDB).	ACX, M, MX, and PTX Series routers
<i>Misc.</i>		
Counter Measures Alarm	Generated when counter measures are started against a rogue device.	Wireless LAN controller
Device Configuration Saved	Generated when the running configuration of the switch is written to the configuration file.	Wireless LAN controller
Multimedia Call Failure	Generated when a multimedia call fails.	Wireless LAN controller
PoE failure	Generated when Power over Ethernet (PoE) has failed on the indicated port.	ACX, M, MX, and PTX Series routers
<i>Network Service</i>		
LSP Service	Generated when an LSP service is affected.	ACX, M, MX, and PTX Series routers
VPN Service	Generated when a VPLS service is affected.	ACX, M, MX, and PTX Series routers
<i>Passive Monitoring (PassiveMonitoring)</i>		
PMonOverloadSetAlarm	Generated when an overload condition is detected on a Passive Monitoring Interface.	ACX, M, MX, and PTX Series routers
<i>Ping</i>		
PingEgressJitterThresholdExceededAlarm	Generated when egress time jitter (jnxPingMaxEgressUs minus jnxPingResultsMinEgressUs) exceeds the configured threshold (jnxPingCtlEgressJitterThreshold) causing the egressJitterThreshold bit to be set.	ACX, M, MX, and PTX Series routers
PingEgressStdDevThresholdExceededAlarm	Generated when the standard deviation of the egress time (jnxPingResultsStddevEgressUs) exceeds the configured threshold (jnxPingCtlEgressTimeThreshold) and causes the egress bit to be set.	ACX, M, MX, and PTX Series routers

Table 17: Alarm Descriptions (continued)

Alarm Name	Description	Device Type
PingEgressThresholdExceededAlarm	Generated when the egress time (jnxPingResultsStdDevEgressUs) exceeds the configured threshold (jnxPingCtlEgressTimeThreshold) and the egress threshold bit is set in jnxPingCtlTrapGeneration.	ACX, M, MX, and PTX Series routers
PingIngressJitterThresholdExceededAlarm	Generated when ingress time jitter (jnxPingResultsMaxIngressUs minus jnxPingResultsMinIngressUs) exceeds the configured threshold (jnxPingCtlIngressJitterThreshold) and the ingressJitterThreshold bit is set in jnxPingCtlTrapGeneration.	ACX, M, MX, and PTX Series routers
PingIngressStddevThresholdExceededAlarm	Generated when the standard deviation of the ingress time (jnxPingResultsStdDevIngressUs) exceeds the configured threshold (jnxPingCtlIngressStddevThreshold) and the ingress StdDevThreshold bit is set in jnxPingCtlTrapGeneration.	ACX, M, MX, and PTX Series routers
PingIngressThresholdExceededAlarm	Generated when the ingress time jitter (jnxPingResultsIngressUs) exceeds the configured threshold (jnxPingCtlIngressTimeThreshold) and the ingress threshold bit (jnxPingIngressThresholdExceeded) is set in jnxPingCtlTrapGeneration.	ACX, M, MX, and PTX Series routers
PingRttJitterThresholdExceededAlarm	Generated when the round trip time jitter (jnxPingResultsMaxRttUs minus jnxPingResultsMinRttUs) exceeds the configured threshold (jnxPingCtlRttJitterThreshold) and the rttJitterThreshold bit is set in jnxPingCtlTrapGeneration.	ACX, M, MX, and PTX Series routers
PingRttStdDevThresholdExceededAlarm	Generated when the standard deviation of the round trip time (jnxPingResultsStdDevRttUs) exceeds the configured threshold (jnxPingCtlRTTStdDev) and the rttStdDevThreshold bit is set in jnxPingCtlTrapGeneration.	ACX, M, MX, and PTX Series routers
PingRttThresholdExceededAlarm	Generated when the round trip time (jnxPingCtlRttThreshold) exceeds the configured threshold (jnxPingCtlRttThreshold) and the rttThreshold bit is set in jnxPingCtlTrapGeneration.	ACX, M, MX, and PTX Series routers
<i>RMon</i>		
RmonAlarmGetFailureAlarm	Generated when a GET request for an alarm variable returns an error. The specific error is identified by a varbind in jnxRmonAlarmGetFailReason.	ACX, M, MX, and PTX Series routers

Changing the Severity of Individual Alarms

You can change the severity of the alarms to match your corporate procedures and guidelines. For example, at your company a DoS attack might be considered a critical alarm, while Connectivity Services Director has a default severity for DoS attacks as a major alarm. Alarms appear on both tabs in the Individual Alarms and Threshold Settings section: Alarm Settings and Threshold Settings.

To change the severity of an alarm:

1. Select the current severity in the **Severity** column. A list of the severity levels appear.
2. Select the new severity level for the alarm.
3. Click **OK** and **Yes** to confirm the change to the severity setting.

To configure alarm notifications, see [“Configuring Individual Alarm Notifications” on page 152](#).

Configuring Threshold Alarms

Threshold alarms are alarms that are generated when a monitored value crosses the configured threshold. They provide enhanced visibility into potential issues on the network. You configure and manage threshold alarms the same way as other alarms. You also have the option of setting the threshold level of individual threshold alarms.

To set threshold alarm thresholds:

1. Select the **Threshold Settings** tab in the Individual Alarms and Threshold settings section of the Fault tab.
2. Click **Edit Settings** in the Threshold Settings column of the alarm threshold you want to edit.
3. Set the threshold in the window that opens.
4. Click **Save** to save the new threshold.

To configure alarm notifications, see [“Configuring Individual Alarm Notifications” on page 152](#).

Configuring Individual Alarm Notifications

You can configure e-mail notifications to be sent when an individual alarm is generated. When you enable notification for an alarm, the notifications are sent to the e-mail addresses configured for the alarm and the addresses configured for global alarm notifications. Alarms appear on both tabs in the Individual Alarms and Threshold Settings section: Alarm Settings and Threshold Settings.

To configure e-mail notification for an alarm name:

1. Select the check box in the alarm's Notification column.
If you later want to disable notification for the alarm, clear the check box.
2. Click **Edit Notification** in the Notification column. The Alarm Notification Details window opens.
3. Enter one or more e-mail addresses in the Notification Email Addresses field. Separate addresses with a comma (,).
You can later edit the addresses to send notifications to different addresses.
4. (Optional) Enter a comment in the Comments field. This comment is included in the e-mail notification message.
5. Click **Save**.

Disabling Optical Performance Monitoring

From the **Optical** tab of the Preference page, you can disable optical performance monitoring by selecting the **Disable Optical Performance Monitoring** check box.

Select the **Disable Optical Performance Monitoring** check box, if you do not intend to store optical parameters.

PART 3

Working with the Dashboard

- [About the Dashboard on page 157](#)
- [Using the Dashboard on page 159](#)
- [Dashboard Widget Reference on page 161](#)

CHAPTER 5

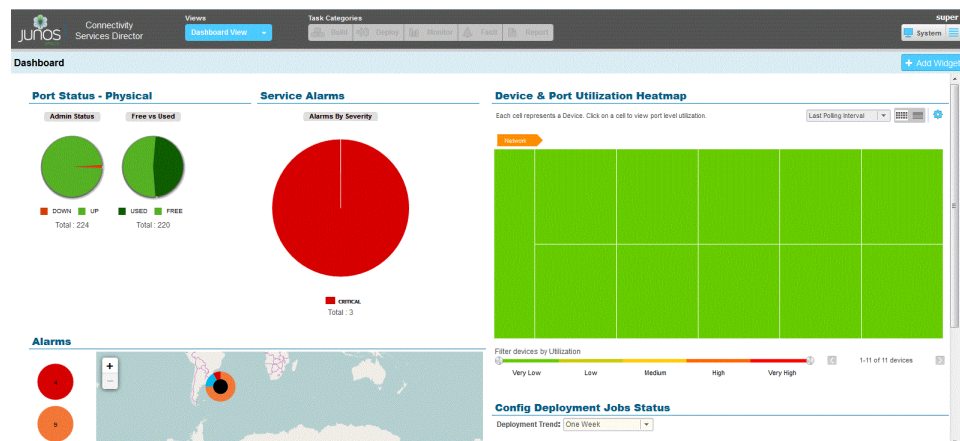
About the Dashboard

- Understanding the Dashboard on page 157

Understanding the Dashboard

When you log in to the Connectivity Services Director interface, the first page that is displayed is the Dashboard page. Service Dashboard and Monitoring provide a proactive account of the services and devices health status and working efficiency of devices in a bird's eye, comprehensive, and intuitive format at the network level and service levels. A single pane of glass (SPOG) view helps the operator to view various alarms and quickly identify and isolate issues. The dashboard and monitoring feature aggregates and correlates data from different sources such as SNMP and system event logs. The defined threshold values enable operators to specify monitoring criteria critical for service operations and administration. The performance management view also highlights the top or first three non-confirming devices and provides a historical context with time graph and additional data from the logging system.. The Dashboard page contains several monitors or frames. The following monitors are displayed on the Dashboard page:

Figure 19: Dashboard Page



The Dashboard is a customizable page to view information about the network, and is the default page that opens when you log in. You select monitoring widgets to display on the Dashboard that show various information about the network. The Dashboard is a view. To open a different view, select a view from the Views list in the Connectivity Services Director banner.

CHAPTER 6

Using the Dashboard

- [Using Dashboard Widgets on page 159](#)

Using Dashboard Widgets

The Dashboard is a customizable page for viewing information about the network. You select monitoring widgets to display on the Dashboard that show various information about the network. The Dashboard is the default view that opens when you log in. When a different view is selected, select **Dashboard View** from the Select View list in the Connectivity Services Director banner to open the Dashboard.

To select what appears on the Dashboard:

1. To add a monitor to the Dashboard:
 - a. Select **Add Widgets**. Thumbnails of the available widgets appear.
 - b. To add a widget to the Dashboard, mouse over the widget's thumbnail, then click the **Add** button that appears on the widgets.
 - c. When you are finished adding widgets, click **Done**. The new widgets appear on the Home page.
2. To refresh a widget's data, click the **Refresh** button in its title bar.
3. To see additional information for a widget, click the **Maximize** button in the widget's title bar.
4. To remove a widget from the Dashboard, click the Close button (X) in its title bar.
5. To open online help for a widget, click the Help button (?) in its title bar.
6. To move a widget, click its title bar and drag it to the new location.

Related Documentation

- [Understanding the Dashboard on page 157](#)

CHAPTER 7

Dashboard Widget Reference

- [Device Alarms Widget on page 161](#)
- [Service Alarms by Severity Widget on page 162](#)
- [Config Deployment Jobs Status Widget on page 162](#)
- [Device & Port Utilization Heatmap Widget on page 163](#)
- [Port Status - Physical Widget on page 166](#)

Device Alarms Widget

The Device Alarms widget displays summary information about alarms generated for the devices present in the network that is managed by Connectivity Services Director. The summarized way in which you can view statistical details enables you to examine the health and operating-efficiency of devices, and the performance of services. It provides a bird's eye, high-level view of parameters that enables effective and simplified troubleshooting and administration. For example, if you find that a particular device has recorded a large number of critical or major alarms, you can then navigate to the Monitoring page or the appropriate device settings page to correct and modify the attributes or diagnose the problems that might be generating the alarms.

Critical, major, and minor alarms are displayed in a pie chart with percentage values of each type of alarm. When you move the mouse over the segments of the pie chart, the total number of alarms of each type are displayed. Mouse over each segment in the pie chart to highlight and display the number of alarms for each severity level.

Alarm severity levels are:

- Critical (Red)—A critical condition exists; immediate action is necessary.
- Major (Orange)—A major error has occurred; escalate or notify as necessary.
- Minor (Yellow)—A minor error has occurred; notify or monitor the condition.
- Info (Wedgewood Blue)—An informational message; no action is necessary. Informational alarms do not necessarily indicate an error. It could indicate that a device or entity has changed state.

Service Alarms by Severity Widget

The Service Alarms by Severity widget displays comprehensive and cohesive details about the alarms generated by different devices for which services, such as point-to-point, Layer 3 VPN, RSVP LSPs, and VPLS, are configured. You can view critical, salient information about the configured devices and services in an intuitive, easily-navigable format. The summarized way in which you can view statistical details enables you to examine the health and operating-efficiency of devices, and the performance of services. These alarm details enable effective and simplified troubleshooting and administration. For example, if you find that a particular device has recorded a large number of critical or major alarms for a service, you can then navigate to the design and provisioning pages of the type of service to correct and modify the attributes or diagnose the problems that might be generating the alarms.

Critical, major, and minor alarms are displayed in a pie chart with percentage values of each type of alarm. When you move the mouse over the segments of the pie chart, the total number of alarms of each type are displayed.

Alarm severity levels are:

- Critical (Red)—A critical condition exists; immediate action is necessary.
- Major (Orange)—A major error has occurred; escalate or notify as necessary.
- Minor (Yellow)—A minor error has occurred; notify or monitor the condition.
- Info (Wedgewood Blue)—An informational message; no action is necessary.
Informational alarms do not necessarily indicate an error. It could indicate that a device or entity has changed state.

Config Deployment Jobs Status Widget

The Config Deployment Jobs Status widget provides summary and detailed information about the status of configuration deployment jobs.

This topic describes:

- [Config Deployment Jobs Status Widget Summary on page 162](#)
- [Config Deployment Jobs Status Widget Details on page 163](#)

Config Deployment Jobs Status Widget Summary

The Config Deployment Jobs Status widget displays summary information about the status of configuration deployment jobs. The information appears in a table. The vertical axis lists the job statuses. The horizontal axis shows the times when job status data was collected. You can do the following tasks:

- Select a time period to view from the **Deployment Trend** list.
- Click the **Refresh** button to refresh the information displayed.

Config Deployment Jobs Status Widget Details

To open the Config Deployment Jobs Status widget details page, click the **Maximize** button in the widget's title bar. The Config Deployment Jobs Status widget details window displays detailed information about the status of configuration deployment jobs. The page shows the same summary information table as the widget. It also shows a table of detailed configuration job status information. To close the details page, click the **Minimize** button in the title bar.

Device & Port Utilization Heatmap Widget




The Device & Port Utilization Heatmap widget provides a graphical view of device port utilization percentage. The heat map represents each device as a color-coded box. The color coding indicates the overall level of port utilization on a device. Cooler colors (for example, green) indicate lower port utilization, while hotter colors (for example, red) indicate higher port utilization.

You can view the utilization level for each port on a device by clicking on the box representing the device. A heat map is displayed that represents each port on the device as a color-coded box, with the color coding representing the level of port utilization.

- [Using the Global Controls on page 163](#)
- [Interacting with the Heat Maps on page 163](#)
- [Viewing Active Flows on a Port on page 164](#)
- [Flow Analysis Details Window on page 165](#)

Using the Global Controls

Use the controls in the upper right corner to make global changes to how the device and port heat maps are displayed. You can:

- Select the time period over which device utilization and port utilization are shown.
- Display information about the devices or the ports in either graphical heat map or tabular format by clicking either  (graphical) or  (tabular).
- Select how to organize the heat map by clicking the Settings icon (), and then selecting an option from the **Group Devices By** list. Each option creates a different view of the heat map, with device boxes grouped according to your selection.

Interacting with the Heat Maps

You can interact with the device and port heat maps as follows:

- If you have grouped the devices by location, you can drill down into the heat map's hierarchy by clicking one of the device container names (for example, a site or building). To move back up the hierarchy, click the navigation arrows above the heat map.
- Mouse over a device box to see detailed device-level port utilization information in a pop-up window. In the pop-up window, you can click the **View top 5 ports** link to view the top five ports that use the most bandwidth on the device.

- Click on a device box to display a heat map of the ports on the device. In this port-level heat map, each port is represented by a box that is color-coded to show its level of utilization. To return to the device view, click the navigation arrows above the heat map.
- Mouse over a port box to display information about the port—such as port name, status, speed, and percent utilization—in a pop-up window. For ports on devices that support Cloud Analytics Engine, you can view any existing flow analysis results on flows through the port by clicking **View active flows through this link**. See [“Viewing Active Flows on a Port” on page 164](#) for more information.
- Slide the circular controls along the bar under the heat map to Filter the devices or ports shown in the heat map by degree of port utilization..

Viewing Active Flows on a Port

For devices that support Cloud Analytics Engine, you can view the results of the most recent flow analysis traces on application flows on the port by mousing over the port and clicking **View active flows through this link**. The Current Active Flows window is displayed.

The Current Active Flows window lists only application flows for which flow analysis traces exist—there might be other active application flows on the port that are not shown. Each flow is uniquely defined by source IP address and TCP/UDP port, destination IP address and TCP/UDP port, and transport protocol. [Table 18 on page 164](#) describes the fields in this window.

Table 18: Fields in the Current Active Flows Window

Field	Description
Source IP Source Port	Source IP address and source TCP/UDP port for the flow. In the case of a flow between two VMS, the IP address is the source VTEP address. If the port is associated with a well-known service, the service name is also shown.
Destination IP Destination Port	Destination IP address and destination TCP/UDP port for the flow. In the case of a flow between two VMS, the IP address is the destination VTEP address. If the port is associated with a well-known service, the service name is also shown.
Protocol	Either TCP or UDP.
Bandwidth	Bandwidth used by the flow. This is a count of the number of packets through the port for the flow up to this point in time. For a value to be displayed in this field, flow analysis must have been performed on flow with the Capture Bandwidth option enabled.
Flow Analysis	Click View Results to see the results of the most recent flow analysis trace. The Flow Analysis Details window opens. NOTE: The View Results link is not available for VM to VM flows.


Flow Analysis Details Window

The Flow Analysis Details window provides detailed information about a flow trace.

The Flow Analysis Details window is divided into three sections:

- The flow path diagram—This diagram shows the path taken by a probe through the network. By default, the path shown is the path taken by the probe that experienced the highest per-hop latency in the trace. You can change this diagram to reflect the path taken by a different probe by selecting the probe from the top Latency Trend chart.
- Latency Trend charts—These charts show the change in latency experienced by the probes during the trace. The bars in the top chart are grouped by completed probes, with each bar in a probe group representing the latency experienced by the probe at a hop. By clicking on a probe group, you can change the flow path diagram and the Analysis Results section to reflect the results of that probe. For traces of long duration, the bar chart shows only a portion of the trace results.

The bottom area chart graphs the highest latency experienced by each probe over the entire duration of the trace. You can use the provided controls to focus on a portion of the trace—the portion you choose is reflected in the top bar chart. By default, the focus is on the portion of the trace that had the highest latency. If the trace is ongoing, a rotating circle appears at the end of the plotted area and the chart is periodically refreshed to show new results.

Both charts display a path change icon () when the path a probe takes through the network differs from the path taken by the previous probe.

- Analysis Results—This section provides details about the overall trace results and about the selected probe:
 - The Latency table provides overall latency information for the trace: the highest and lowest latency experienced at a single hop and the average latency of all hops.
 - The Latency for Selected Path table shows the latency experienced by the selected probe at each hop.

You can perform the following actions in the Flow Analysis Details window.

General actions:

- For bidirectional traces, you can select the direction for which you want results by clicking one of the arrows at the top of the window (these arrows do not appear for unidirectional traces).
- To stop an active flow analysis, click **Stop Flow Analysis** at the bottom of the window. When you stop an active flow analysis, the results up to the time you stopped the flow analysis are retained and the previously active trace is marked as complete.


On the flow path diagram, you can:

- Reposition the topology diagram by dragging it or reposition devices by dragging them.
- Zoom in or out by clicking the plus or minus signs on the left.
- Mouse over the link connecting two devices to get the connecting port names. The names are displayed in green if the link is up and in red if the link is down.
- Mouse over a device to view details about the device, such as name, connection state, and IP address. The details shown depends on the device type.

If a device in the flow path does not support Cloud Analytics Engine, it is shown in the diagram in light grey color and minimal details, such as IP address, are available.

- Display the traffic statistics for switches by mousing over the device to display the device details and clicking the **Show Traffic Data** link. If you selected the Capture Bandwidth option when you started the flow analysis, the flow bandwidth is also displayed along with the traffic statistics.
- Display the active flows associated with a VM, BMS, or virtualized host by mousing over the device and clicking **Show Active Flows** in the details box.

On the Latency Trend charts, you can:

- Mouse over a bar group in the top bar chart. A pop-up box displays the latency figures for each hop taken by the probe.
- Click a bar group in the top bar chart. The flow path diagram and the Analysis Results change to reflect the information for the probe.
- Mouse over a path change icon in the top bar chart. Information about the old and new paths is displayed.
- Change the span and position of the focus indicator on the bottom area chart:
 - To increase or decrease the time span of the focus—in other words, to zoom in or zoom out on a portion of the trace—click on one of the handle controls () and move it in either direction.
 - To change the focus to another time period, click on the arrows at either end of the slider bar.

Port Status - Physical Widget

The Port Status - Physical widget provides summary and detailed information about the status of physical ports on managed devices.

This topic describes:

- [Port Status - Physical Widget Summary on page 167](#)
- [Port Status - Physical Widget Details on page 167](#)

Port Status - Physical Widget Summary

The Port Status - Physical widget displays summary information about the status of physical ports on managed devices. It has the following pie charts:

- Admin Status pie chart—Shows the distribution of ports that are administratively up or down and states the total number of ports. Mouse over a chart segment to see more information about it.
- Free vs. Used pie chart—Shows the distribution of ports that are free or used and states the total number of ports. Mouse over a chart segment to see more information about it.

Port Status - Physical Widget Details

The Port Status - Physical widget details window has a table containing detailed information about the status of physical ports on managed devices. See *Port Status Monitor* for descriptions of the table columns.

PART 4

Working in Build Mode

- [About Build Mode on page 171](#)
- [Discovering Devices on page 177](#)
- [Creating Custom Device Groups on page 187](#)
- [Configuring Quick Templates on page 193](#)
- [Configuring Device Settings on page 201](#)
- [Configuring Class of Service \(CoS\) on page 219](#)
- [Configuring Link Aggregation Groups \(LAGs\) on page 245](#)
- [Managing Network Devices on page 251](#)

CHAPTER 8

About Build Mode

- [Understanding Build Mode in Views Other than Service View of Connectivity Services Director on page 171](#)
- [Understanding the Build Mode Tasks Pane in Views Other than Service View on page 174](#)

Understanding Build Mode in Views Other than Service View of Connectivity Services Director

In Build mode, you build the network managed by Junos Space Connectivity Services Director. It provides you with the ability to use device discovery to bring devices under Connectivity Services Director management, to customize your view of the devices, to configure devices, and to perform some common device management tasks.

This topic describes:

- [Discovering Devices on page 171](#)
- [Building the Custom View on page 172](#)
- [Configuring Devices on page 172](#)
- [Managing Devices on page 174](#)

Discovering Devices

Device discovery finds your network devices and brings them under Connectivity Services Director management. You provide Connectivity Services Director with identifying information about the devices you want Connectivity Services Director to manage—an IP address or hostname, an IP address range, an IP subnetwork, or a CSV file that contains this information. Connectivity Services Director uses the information to probe the devices by using either ping or SNMP get requests. If a device probe is successful, Connectivity Services Director then attempts to make an SSH connection to the device using the login credentials you supply. If the connection is successful and the device is a supported device, Connectivity Services Director adds the device to its database of managed devices. Connectivity Services Director uses Juniper Network's Device Management Interface (DMI), which is an extension to the NETCONF network configuration protocol, to connect to and configure its managed devices.

You can also discover devices using the device discovery feature provided by the Junos Space Network Management Platform. Devices you discover using Junos Space device

discovery are brought under Connectivity Services Director management if they are supported by Connectivity Services Director.

Besides bringing your devices under Connectivity Services Director management, device discovery:

- Reads the device configuration and saves it in the Junos Space configuration database. Connectivity Services Director uses this record of the device configuration to determine what configuration commands it needs to send to a device when you deploy the configuration on the device. For this reason, it is important for the Junos Space configuration record to match, or be in sync with, the device configuration. For more information about how the Junos Space configuration record and device configuration are kept in sync, see [“Understanding Resynchronization of Device Configuration” on page 773](#).
- Imports the device configuration into the Build mode configuration. For more information about importing device configurations, see [“Importing Device Configurations” on page 173](#).

Building the Custom View

When a device is discovered in the physical network mode, it is added to the network tree in the View pane.

The Custom Group View displays only the top level—My Network—until you create one or more custom groups. Custom group is another way of grouping your devices based on your business needs. You can create custom groups and add devices to each custom group. You can manually add devices to a custom group or you can define rules to add devices, that match the rule condition, to the custom group once they are discovered by Connectivity Services Director. You can view the custom groups and devices that are assigned to each group in the Custom Group view.



NOTE: This section does not apply to virtual devices that Connectivity Services Director manages.

Configuring Devices

In Build mode, you can define the configuration of network devices in your Physical network. To support rapid, large-scale deployment of devices, you can define much of your Build mode configuration in a set of profiles. You can reference profiles in other profiles or apply them to multiple objects in your network—devices, ports, radios, logical entities. For example, you can create a class-of-service (CoS) profile that contains settings that are appropriate for point-to-point, Layer 3 VPN, and VPLS services that you can manage, provision, and monitor in Service View of Connectivity Services Director.

In addition to creating configuration profiles, in Build mode you can configure Link Aggregation Groups (LAGs) on routers.

Deploying Device Configurations

After you build your device configurations in Build mode, you need to deploy the configurations on the devices. None of the configurations you create in Build mode affect your devices until the configurations are actually deployed on the devices.

To deploy the configuration on devices, use Deploy mode. When you change a device's configuration in Build mode, the device becomes available in Deploy mode for configuration deployment.

Importing Device Configurations

As part of device discovery, Connectivity Services Director analyzes the configuration of a newly discovered device and automatically imports the configuration into the Build mode configuration for that device.

As it imports the device configuration, Connectivity Services Director automatically creates profiles to match the configuration. It first determines whether any existing profiles match the configuration, and if so, assigns those profiles to the device. It then creates and assigns new profiles as needed. For example, if an access switch has some ports that match the configuration of an existing Port profile, Connectivity Services Director assigns the existing Port profile to those ports. For the other ports, Connectivity Services Director creates as many Port profiles as needed to match the port configurations and assigns them to the ports.

You can manage the profiles that Connectivity Services Director creates as part of device discovery in the same way that you manage user-created profiles—that is, you can modify, delete, or assign them to other devices.

Out-of-Band Configuration Changes

Out-of-band configuration changes are configuration changes made to a device outside of Connectivity Services Director. Examples include changes made by:

- Using the device CLI.
- Using the device Web-based management interface (the J-Web interface or Web View).
- Using the Junos Space Network Management Platform configuration editor.
- Using RingMaster software.
- Restoring or replacing device configuration files.

When an out-of-band change is made, the device configuration no longer matches the Build mode configuration, and the device configuration state changes to out of sync. You cannot deploy configuration on a device that is out of sync. Use the Resynchronize Device Configuration task in Deploy mode to resynchronize the device configuration. For more information about how Connectivity Services Director resolves out-of-band configuration changes and synchronizes the Build mode configuration with the device configuration, see [“Understanding Resynchronization of Device Configuration” on page 773](#).



TIP: Before you make configuration changes in Build mode, make sure that devices that will be affected are in sync. Resynchronizing the device configuration can result in losing pending Build mode configuration changes for that device.

Managing Devices

In addition to the tasks that allow you to build your network, Build mode provides a number of tasks for day-to-day device management. For example, you can:

- View a device's hardware component inventory or its installed licenses
- Reboot a device or groups of devices
- Connect to a device's CLI through SSH or to its web-based management interface
- View the profiles assigned to a device

Understanding the Build Mode Tasks Pane in Views Other than Service View

The Tasks pane in Build mode contains all the tasks you can do in Build mode. Click a specific task to begin that task.

The tasks listed in the Tasks pane depend on the scope you select in the View pane—that is, what view (Device or Custom Group) you have selected and what object you have selected. Not all tasks are available in all scopes. As you change your selections in the View pane, the contents of the Tasks pane also change.

Build mode tasks are divided into the following categories in the Tasks pane.

Connectivity Services Director enables you to perform the following tasks for devices in your physical network:

- **Device Discovery**—Before your devices can be managed by Connectivity Services Director, you must use device discovery to discover them. As Connectivity Services Director discovers devices, it adds them to your network view in the View pane. [Table 19 on page 175](#) describes the device discovery tasks.
- **Device Management**—After devices have been discovered, you can perform administrative tasks on them, such as viewing a list of the device's physical components, connecting to a device using SSH, or rebooting a device. [Table 20 on page 175](#) describes the device management tasks.
- **Wired**—You can create configuration profiles and quick templates for the different wired devices—ACX Series routers, M Series routers, MX Series routers, and PTX Series routers.
- **Profile and Configuration Management**—Connectivity Services Director provides a set of configuration profiles that you can create to provision multiple devices in your

network. [Table 22 on page 176](#) describes the profile and configuration management tasks.

- **Key Tasks**—Connectivity Services Director enables you to group the tasks that you perform frequently and create a list of key tasks. You can add any task from the Tasks pane to the Key Tasks list by selecting a task and clicking the plus (+) sign that appears adjacent to the task. For some modes, you can see that Connectivity Services Director has predefined some key tasks for you. You can modify this set of tasks to suit your requirements. This feature is available in Task pane irrespective of your current mode, scope, or view.

For more information about Build mode features, see “[Understanding Build Mode in Views Other than Service View of Connectivity Services Director](#)” on page 171.

[Table 19 on page 175](#) through [Table 22 on page 176](#) describe the tasks that you can perform in the physical network category, including the scope in the View pane that you must select to access the task.

Table 19: Device Discovery Tasks

Task	Description	Scope
Discover Devices	Discovers supported routers in the network and brings them under Connectivity Services Director management.	Any
View Discovery Status	Displays the status of device discovery jobs.	Any

Table 20: Device Management Tasks

Task	Description	Scope
Delete Devices	Deletes a device as a managed device from Connectivity Services Director. If you select a scope that contains more than one router, you can choose which devices are deleted.	View: All Object: All
Launch Web View	Launches the Web-based management interface for the selected device in a separate window: the J-Web interface for routers.	View: All Object: Individual device
Manage LAG	Creates and manages Link Aggregation Groups (LAGs).	View: All Object: Individual router
Reboot Devices	Reboots devices. If you select a scope that contains more than one router, you can choose which devices get deleted.	View: All Object: All
Show Current Configuration	Shows the running configuration on a device.	View: All Object: Individual device
SSH to Device	Launches an SSH connection to the selected device.	View: All Object: Individual device

Table 20: Device Management Tasks (continued)

Task	Description	Scope
View Inventory	Displays information about all the devices in the currently selected object and all its child objects.	View: All Object: All
View License Information	View the licenses installed on the device and their status.	View: All Object: Individual device
View Physical Inventory	Displays information about the selected device's hardware components.	View: All Object: Individual device

Table 21: Connectivity Tasks

Task	Description	Scope
View Device Connectivity	Displays the connection details of a device with its neighbors in graphical and grid views. If the selected device is connected to more than 60 devices, then the connection details are displayed only in grid view.	View: Device Object: Individual device

Table 22: Profile and Configuration Management Tasks

Task	Description	Device Family	Scope
Manage Quick Templates	Enables you to create and manage quick templates. Quick templates enable you to define your network configuration in the form of templates that you can apply to multiple devices in your network.	ACX Series M Series MX Series PTX Series	All, except wireless devices
View Deployed Templates	Enables you to view the list of quick templates that are deployed.	ACX Series M Series MX Series PTX Series	All, except wireless devices
CoS	Creates and manages CoS profiles. Use CoS profiles to configure class-of-service (CoS) attributes to be applied to interfaces or to user traffic.	ACX Series M Series MX Series PTX Series	Any
Device Common Settings	Creates and manages Device Common Settings profiles. Use Device Common Settings profiles to configure basic system settings, such as users, time and time servers, SNMP, system logging, and so on.	ACX Series M Series MX Series PTX Series	Any

CHAPTER 9

Discovering Devices

- [Discovering Devices in a Physical Network on page 177](#)
- [Troubleshooting Device Discovery Error Messages on page 184](#)
- [Viewing the Brownfield Job on page 185](#)

Discovering Devices in a Physical Network

You can discover and synchronize physical devices such as ACX Series routers, M Series routers, MX Series routers, and PTX Series routers in your network that are managed by Connectivity Services Director.



NOTE: On routers, Connectivity Services Director connects to port 22 (the default port) on the Junos Space JA2500 Appliance or the Junos Space Virtual Appliance by using SSH. You can configure port 22 on the Junos Space appliances through **Administration > Applications** in the Junos Space Platform page. Select **Network Application Platform** and click **Actions > Modify Application Settings**. Change SSH port for device connection field to 22.

Device discovery is a three-step process in which you specify the target devices, the discovery options, and the schedule options.

While in Build mode, from the Tasks pane, click **Discover Devices** from Device Discovery menu. The Discover Devices page is displayed.

This topic describes:

- [Preparing MX Series Devices for Discovery on page 178](#)
- [Specifying the Target Devices on page 178](#)
- [Specifying the Discovery Options on page 180](#)
- [Specifying the Schedule Options on page 182](#)
- [Reviewing the Device Discovery Options on page 182](#)
- [Viewing the Discovery Status on page 182](#)

Preparing MX Series Devices for Discovery

Juniper Networks MX Series 3D Universal Edge Routers—MX240, MX480, and MX960—include all standard Ethernet capabilities as well as enhanced mechanisms for service providers to provision and support large numbers of Ethernet services in addition to all Layer 3 services. You can discover these routers and manage them as devices from Connectivity Services Director. However, before discovering these MX devices from Connectivity Services Director, you must ensure that the Junos OS running on the device is at the required level and that the network service mode is set to LAN.

To prepare an MX Series device for discovery:

1. Log in to the MX Series device by using the CLI.
2. Ensure that the device is running Junos OS Release 13.2 or later. Use the operational mode command **show version** to determine the Junos OS software release. If the device is running an earlier release, upgrade to Junos OS Release 13.2 or later.
3. Set the network service mode to LAN by running the following command in the configuration mode:

```
[edit]
user@router# set chassis network-services lan
```

4. Commit your changes.

The MX Series device is now discoverable from Connectivity Services Director.

Specifying the Target Devices

You can add devices to Connectivity Services Director for device discovery by using either the Import from CSV icon or the Add icon, or both together. Use the Import from CSV icon to add devices in bulk. You can add hundreds of devices to Connectivity Services Director by using a CSV file that contains information extracted from an LDAP repository.



NOTE: If you want to discover and manage MX Series devices—MX240, MX480, and MX960—from Connectivity Services Director, you must first make these devices discoverable. For more details see [“Preparing MX Series Devices for Discovery” on page 178](#).

To specify the target devices that you want Connectivity Services Director to discover:

1. Enter a name for the device discovery job. The default name is ND Discovery.
2. To add devices in bulk, click **Import from CSV** from the Device Targets window. The Upload CSV File dialog box is displayed.
3. Click **Browse**. The File Upload dialog box is displayed.

4. Navigate to the target CSV file on your computer, select the file and click **Open**. The CSV File Upload dialog box reappears, this time displaying the name of the selected file.



NOTE: The selected CSV file must follow the same file format as that of the sample CSV file.

5. Click **Upload** to upload the selected CSV file.
6. To add individual devices by specifying the IP address credentials, click **Add** in the Device Targets table.

The Add Device Target dialog box appears.

7. Choose one of the following options to specify the target devices:
 - Select the **IP** option and enter the IP address of the device.
 - Select the **IP-Range** option and enter a range of IP addresses for the devices. The maximum number of IP addresses for an IP range target is 1024.
 - Select the **IP-Subnet** option and enter an IP subnet for the devices.
 - Select the **HostName** option and enter the hostname of the device.
 - Click **Add** to save the target devices that you specified, or click **Add More** to add more target devices. When you have added all target devices that you want Connectivity Services Director to discover, click **Add**.

The Discover Targets table displays the addresses of the configured target devices.

8.
 - To edit a target device, select a row from the Device Targets table and click **Edit**. Make the required changes and click **Add** to display the IP addresses in the Device Targets table
 - To delete a target device, select a row from the Device Targets table and click **Delete**.
 - To view and download a sample CSV file, click **CSV Sample**. The Opening Device_Discovery_CSV.csv file dialog box is displayed. You can open the sample CSV file or save the sample CSV file.
9. Click **Next** or click **Discovery Options** from the top wizard workflow to go to the Discovery Options page. Specify the options as described in [“Specifying the Discovery Options” on page 180](#).

Specifying the Discovery Options

To add the device credentials and specify the probes:

1. Add the device credentials. To add the credentials, click **Add** from the Device Credentials table.

The Add Device Credentials dialog box is displayed.



NOTE: If the credentials were specified in the CSV file, the Credentials table displays those values. If the credentials were not specified in the CSV file, then enter the values in the Add Device Credentials dialog box.

- Specify the administrator username and password, and confirm the password. The username and password must match the name and password configured on the device. The username is a mandatory field.
- Click **Add** to save the username and password that you specified or click **Add More** to add another username and password.

Click **Add** after you have finished adding all login credentials. The Device Credentials table displays the usernames that you configured.

2. Specify the probes from the Specify Probes table. Select a probe method to discover the target devices.

- Select **Use Ping** if SNMP is not configured for the device and clear the **Use SNMP** check box.

Connectivity Services Director uses the Juniper Networks Device Management Interface (DMI) to directly connect to and discover devices. DMI is an extension to the NETCONF network management protocol.

- Select **Use SNMP** if SNMP is configured for the device, and clear the **Use Ping** check box.

Connectivity Services Director uses the **SNMP GET** command to discover target devices.

- Select both the **Use Ping** and the **Use SNMP** check boxes, to enable Connectivity Services Director for faster discovery of the target devices, provided the device is pingable and also SNMP is enabled on the device.



NOTE: Connectivity Services Director uses the Juniper Networks Device Management Interface (DMI) adapter to manage devices that do not run Junos OS. However, if you enable Use SNMP, Connectivity Services Director detects whether the device is running a DMI-complaint software or not. The routers always use a DMI adapter and hence can be detected.

If you have not enabled Use SNMP, then Connectivity Services Director assumes that all devices that failed during device discovery are controllers and retry the process if the port 8889 is open.

3. Click **Add** if you have selected the Use SNMP check box.

The Add SNMP Settings dialog box is displayed.

Select either **SNMP V1/V2C** or **SNMP V3**. Based on the selection, you need to enter the details as follows:

- If you selected SNMP V1/V2C, specify a community string, which can be *public*, *private*, or a predefined string.

Click **Add** in the Add SNMP Settings dialog box or click **Add More** to add more strings to the community. If you click **Add More**, when you are done adding all the strings, click **Add** to save the SNMP settings for V1/V2C.

- If you selected SNMP V3:
 - Enter a username
 - Select the privacy type (AES 128, DES, or None).
 - Enter the privacy password (if AES 128 or DES). If you specify none for the privacy type, the privacy function is disabled.
 - Select the authentication type (MD5, SHA, or none).
 - Enter the authentication password (if MD5 or SHA). If you specify none for the authentication type, the authentication function is disabled.
 - Click **Add** to save the SNMP settings and close the dialog box, or click **Add More** to add additional configurations. If you clicked Add More, click **Add** to save the settings and close the dialog box.

The Specify Probes table displays the configured SNMP settings.

4. Click **Next** or click **Schedule Options** from the top wizard workflow to go to the Discovery Schedule Options page. Specify the options as described in the [“Specifying the Schedule Options” on page 182](#).

Specifying the Schedule Options

To specify the scheduler details:

1. Click **Run Now** if you want to discover the devices immediately or Click **Schedule at a later time** if you want to schedule the device discovery for a future time.

If you select **Schedule at a later time**, specify the date and time to run the device discovery.

2. Click **Next** or click **Review** from the top wizard workflow to view the configuration. See [“Reviewing the Device Discovery Options” on page 182](#).

Reviewing the Device Discovery Options

From this page, you can save or make changes to the device discovery options.

- To make changes to the device discovery options, click the **Edit** button associated with the configuration you want to change.

Alternatively, you can click the appropriate buttons in the profile workflow at the top of the page that corresponds to the configuration you want to change.

When you are finished with your modifications, click **Review** to return to this page.

- Click **Finish** when you are done with the configurations.

A message window opens, displaying the status of the device discovery job name and job ID. Click **OK**.

The Device Discovery Jobs page is displayed with the list of jobs scheduled.

Viewing the Discovery Status

After you have configured the device discovery options, you can view the device discovery status from the **View Discovery Status** option from the **Device Discovery** menu.

The **Device Discovery Jobs** page displays all the scheduled device discovery jobs. You can view the following details from the Device Discovery Jobs page as described in [Table 23 on page 182](#).

Table 23: Viewing Device Discover Jobs

Field	Description
Job ID	An identifier assigned to the job.
Job Name	The name of the job (user-created).
Percent	Percentage of the job that is complete.

Table 23: Viewing Device Discover Jobs (continued)

Field	Description
Status	<p>Job status. The possible states are:</p> <ul style="list-style-type: none"> • CANCELLED—The job was cancelled by a user. • FAILURE—The job failed. This state is displayed if any of the devices in the job failed. But some of the devices might have completed successfully. View the job details for the status of each device. • INPROGRESS—The job is running. • SCHEDULED—The job is scheduled but has not run yet. • SUCCESS—The job completed successfully. This state is displayed if all of the devices in the job completed successfully.
Summary	Summary of the job scheduled and executed with status.
Scheduled Start Time	The UTC time on the client computer when the job is scheduled to start.
Actual Start Time	The actual time when the job started.
End Time	The time when the job was completed.
User	The login ID of the user that initiated the job.
Recurrence	The recurrent time when the job will be restarted.

To view the details of a job, select the check box against Job ID or Job Name and click **Show Details**. The Discover Network Elements window displays details of the device discovery job.



NOTE: During device discovery, if Connectivity Services Director is unable to read the device configurations, then the status displays Failed state. For such failures, you can check the reason for failure from the Manage Jobs page in System mode. You must make the required changes to the device configuration using the CLI so that Connectivity Services Director can read the configuration. Connectivity Services Director automatically resynchronizes once you enable a device discovery job. If Connectivity Services Director cannot discover the device even after resynchronization, then you must rediscover the device after making the appropriate changes in the device configurations by using the CLI.

Troubleshooting Device Discovery Error Messages

While you are discovering devices by using Connectivity Services Director, you might encounter some issues. Connectivity Services Director enables you to detect the errors and provide solutions to the potential errors that you encounter.

Error Message	Solution
Error Messages Displayed During Discovery of Routers	
SSH connection failed. Device might not be reachable.	<p>For routers, Connectivity Services Director connects to port 22 (default port) on the JA2500 Appliance or the Junos Space Virtual Appliance by using SSH. Ensure that you have configured port 22 on the Space appliance through Administration > Applications in the Junos Space Platform page. To do this, select Network Application Platform and click Actions > Modify Application Settings. Change SSH port for device connection field to 22.</p> <p>If port 22 is open on the Junos Space Appliance, and you still get the error, then check if port 22 is open on the switch and if the switch is accepting SSH connections on port 22.</p>
User Authentication failed.	Check the read and write credentials used during device discovery.
Device is not reachable.	If ping is enabled during device discovery, then check whether the switch is reachable using the CLI command ping .
Junos Space is unable to query the device information through SNMP. Check the SNMP settings on the device to verify SNMP is not blocked and the SNMP settings specified in Junos Space match the device SNMP settings.	If the SNMP option is enabled in Connectivity Services Director during device discovery, check and ensure that SNMP is enabled on the switch. Also, check and ensure that the SNMP settings on Connectivity Services Director and Junos Space match with the SNMP settings on the switch.
General Error Messages	
Device Failed to return System information.	This message is displayed if the switch is too busy to respond to operational commands. Try discovering the device again.
Failed to configure device, Check Device state.	Check whether the Edit lock is open on the switch and close it if it is open. The configuration commit fails if the Edit lock is open.

Error Message	Solution
Device has been added, but failed to synchronize. Please try manual re-synchronization. Error while reading config from device: device_name, Detail - Fail while executing following RPC: <get-configuration database=committed><configuration></configuration></get-configuration>	Try to resynchronize the devices manually. For details, see “Resynchronizing Device Configuration” on page 778 .
Error while reading config from device: device-name Failed while executing the following RPC: <get-hardware-inventory/>	<p>Check the hardware details of the switch using the CLI command show chassis hardware detail.</p> <p>If the output displays a message error: command is not valid, then the Junos OS image on the specified switch is corrupted and you need to upgrade to the latest version of Junos OS.</p>

Viewing the Brownfield Job

Connectivity Services Director initiates the brownfield job immediately after the device discovery. The Brownfield Job window displays the job and the device details. To open the Brownfield Job window double-click the brownfield job name in the Job Management table. The following table describes the information provided in the Brownfield Job page:

Table 24: Brownfield Job Page Fields

Table Column	Description
Job Name	Job name (user-created)
Job Start Time	Job's actual start time
Job End Time	Time when the job ended
Percentage Completed	Percentage of the job that is complete
Job Status	<p>Job status. The possible states are:</p> <ul style="list-style-type: none"> CANCELLED—The job was cancelled by a user. FAILURE—The job failed. This state is applied if any of the devices in the job failed. But some of the devices might have completed successfully. View the job details for the status of each device. INPROGRESS—The job is running. SCHEDULED—The job is scheduled but has not run yet. SUCCESS—The job completed successfully. This state is applied if all of the devices in the job completed successfully.
Devices	<p>The devices section lists device details such as device name, IP address of the device, job status of the device, job start and end times and the summary of the brownfield job. For a successful job, the summary column displays the message “Brownfield is Successful”. For a job that is skipped, the summary column lists the error or warning message along with a View link. Double-click on the View link to open the Brownfield Errors page, which displays the device profile name along with the error associated with that device.</p>

CHAPTER 10

Creating Custom Device Groups

- [Understanding Custom Device Groups on page 187](#)
- [Creating Custom Device Groups on page 188](#)

Understanding Custom Device Groups

Custom group is way of grouping your devices based on your business needs. You can create custom groups and add devices to each custom group. You can manually add devices to a custom group or you can define rules to add devices, that match the rule condition, to the custom group once they are discovered by Connectivity Services Director. You can view the custom groups and devices that are assigned to each group in the Custom Group view.

A custom group can include devices such as different routing platforms. Creating custom device groups enables the configuration of multiple devices simultaneously—you can create multiple custom groups and directly associate devices at any level. Up to this point, Custom Groups are the same as selecting related items in the view tree. What makes Custom Groups unique is that you can also configure a custom group to automatically add devices after discovery. You indicate the criteria for additional devices by editing rules. Custom groups can then be created in a hierarchy up to eight levels deep. Each layer can contain up to 32 peer containers under a single parent container.

- [Where Is the Custom Group Function Located in Connectivity Services Director? on page 187](#)
- [How Do Custom Group Rules Work? on page 188](#)
- [What Happens When I Edit a Custom Group Rule? on page 188](#)
- [When Are Rules Executed? on page 188](#)

Where Is the Custom Group Function Located in Connectivity Services Director?

Connectivity Services Director has different views that you select to see different aspects of your data. You select one of these views at a time from the Select View option in the Connectivity Services Director banner. The options are Device View, Custom Group View, and Topology View. To create a Custom Group, Connectivity Services Director must be in Custom Group View. Custom Groups are created at the top level of the network—My Network.

Once Custom Groups are created, they appear in all views as options for profile assignment—assigning a profile to a Custom Group assigns that profile to all members of the group.

How Do Custom Group Rules Work?

Adding rules to a Custom group consists of creating a three part rule statement, with a rule basis, an operator, and matching criteria. Possible combinations are shown in [Table 25 on page 188](#).

Table 25: Three Options of a Rule Statement

Rule Basis	Operator	Matching Criteria
Device Type	Equals or Not Equals	Router
Serial Number	Equals or Contains	<i>You provide serial numbers or letters</i>
SKU or Model	Equals or Contains	<i>You provide model numbers or letters</i>
Management IP Address	Equals or Regex	<i>You provide IP address</i>
Device Type	Equals or Not Equals	Router
Firmware Version	Equals or Contains	<i>You provide a full or partial firmware version for devices</i>

What Happens When I Edit a Custom Group Rule?

When you edit a rule, devices that were added to the group but no longer qualify because of the rule edit are not automatically removed from the group. You must remove those devices manually. If more devices are now qualified to join the group because of your rule edit, the devices are added to the group on the next device notification change to the network.

When Are Rules Executed?

The option **Associate devices based on the rules for the custom groups while saving group information** is enabled by default. If the option is disabled, the rule engine will be activated only when there is some change in the device property. When a device property change occurs, rules are processed and devices are added to the group, if the group has a rule for those actions.

Creating Custom Device Groups

From Connectivity Services Director, you can create a custom group, then add devices, such as routers, to the group. Creating custom device groups enables the configuration of multiple devices simultaneously—you can also create multiple custom groups and directly associate devices at any level. What makes Custom Groups unique is that you can also configure a custom group to automatically add devices after discovery. You indicate the criteria for additional devices with rules. Custom groups can then be created

in a hierarchy up to eight levels deep. Each layer can contain up to 32 peer containers under a single parent container.



NOTE: A device can be part of a group at only one level in a hierarchy.

This topic describes:

- [Creating Custom Groups on page 189](#)
- [Creating a Custom Group on page 189](#)

Creating Custom Groups

To create custom groups:

1. In the top banner, under **Views**, select **Custom Group View**.
2. Click the **Build** icon in the Connectivity Services Director banner.
3. Click **Set Up Custom Group** under Key Tasks in the Tasks pane.

The Set Up Custom Group page opens, displaying a list of currently configured Custom Groups.

4. Configure the custom group, following the directions [“Creating a Custom Group” on page 189](#).
5. Click **Done**.

The new custom group appears in the Groups List.

Creating a Custom Group

Use the Set Up Custom Group page to define a group of devices that you can configure simultaneously.

To add a new custom group:

1. Type a Custom Group Name for the new group and then click **Add**.

The Custom Group tree is displayed with your new group added.

2. Click **Done** now to create the group with no child groups, devices, or rules. The Message *Data Saved Successfully* is displayed. Click **OK**.

For additional configuration, select your new group.

The options **Add Child Group**, **Assign Devices**, and **Add/Edit Rule** appear.

3. To add a child group under the new custom group:

- a. Be sure the correct custom group is selected—this group will become the parent group.

- b. Click **Add Child Group**.

The Add Child Group window opens, displaying a default child group name such as Group-0.

- c. Replace the default child group name.

- d. Click **Add**.

The new child group appears in the Custom Group list tree under the parent group.



TIP: Custom groups can be created in a hierarchy up to eight levels deep. Each layer can contain up to 32 peer containers under a single parent container.

4. To assign devices to a custom group:

- a. Select a custom group, either a parent or child group, and then click **Assign Devices**.

The Assign Devices To Custom Group window opens, displaying a list of discovered network devices, their IP addresses, and their platforms. Platforms include junos-acx, junos-m, junos-mx, and junos-ptx. These are devices that can be added to the group.

- b. Select one or more devices by adding a check mark and then click **Add**.

The devices are listed under the appropriate group in the Custom Groups List.



NOTE: A device can be part of a group at only one level in a hierarchy.

5. To add a rule that will automatically add devices to a parent or child custom group:

- a. Select a custom group, either a parent or child group, that will have devices added to it automatically when a specific rule has been met.

- b. Click **Add/Edit Rule(s)**.

The Add/Edit Rules window opens.

- c. Click **Add Rule**.

A rule statement is displayed with three columns—two columns display the words *Please select...*. The third column is blank.

- d. From the first *Please select...* option in the rule statement, select the basis for the rule. You are indicating that automatic additions to the list will be based on either **Device Type**, **Firmware Version**, **Serial Number**, **SKU/Model**, **Management IP**.
- e. From the second *Please select...* option in the rule statement, select an available operator, either **Equals**, **Not Equals**, **Like**, **Regex**, or **Contains**—the operators presented depend on the basis you selected in the first column. For example, if the basis for the rule is **SKU/Model**, then the only operator options are **Equals** and **Not Equals**.



TIP: The **Equals** operation matches all characters of the matching criteria. The **Like** operation matches the first few characters of the matching criteria.

- f. For the third option in the rule statement, provide a matching criteria. Matching criteria are indicated in the third column of the list shown in [Table 26 on page 191](#).



TIP: Some rules have no third option.

Table 26: Three Options of a Rule Statement

Rule Basis	Operator	Matching Criteria
Device Type	Equals or Not Equals	Router
Serial Number	Equals or Contains	<i>You provide serial numbers or letters</i>
SKU or Model	Equals or Contains	<i>You provide model numbers or letters</i>
Management IP	Equals or Regex	<i>You provide IP address or regular expression</i>
	TIP: Regex, a regular expression, consists of a sequence of characters that forms a search pattern.	TIP: For example, (?<=\\.) {2,} (?=[A-Z]) is a regular expression.
Firmware Version	Equals or Contains	<i>You provide a full or partial firmware version for devices.</i>

- g. Click **OK**.

Rules are executed when new devices are discovered. Devices that match the defined rules are added to the group dynamically once discovery is complete.



TIP: If you add more than one rule to a Custom Group, then all rules must be met for a device to join the group.

6. The option **Associate devices based on the rules for the custom groups while saving group information** is enabled by default. When a device property change occurs, rules are processed and devices are added to the group, if the group has a rule for those actions. If you disable the option, the rule engine will be activated only when there is some change in the device property.
7. Click **Done**.

A status window opens with either the message *Data saved successfully* or with an error message. Click **OK**.
8. To edit a rule, select the appropriate custom group and then click **Add/Edit Rule**. When you edit a rule, devices in the group that no longer qualify because of the rule change are not automatically removed from the group. You must remove those devices manually. If more devices are now qualified to join the group because of your rule edit, the devices are added to the group on the next device notification change to the network.



TIP: To delete a device from the group, select the device and then click **Delete**. To delete an entire Custom Group, select the group and then click **Delete**. You are asked to confirm the deletion—click **OK**.

Configuring Quick Templates

- [Understanding Quick Templates on page 193](#)
- [Configuring and Managing Quick Templates on page 194](#)

Understanding Quick Templates

Quick templates is a way to create a base build for the devices. This feature enables you to use a CLI-based text editor to define your network configuration in the form of a template that you can apply to multiple devices in your network in addition to the profile assignment feature. Because quick templates are driven by Device Management Interface (DMI) schema, you can use them to set all the configuration parameters for any supported device.

By using these quick templates, you can configure, for example, routing protocols such as BGP, OSPF, ISIS, or even static routes by specifying the device configuration. You can append or add the system commands or the user-defined commands in the form of the variables in the CLI-based text editor. The user-defined commands support variables in the format `$(variable_name)`, which must be populated with data when you apply a template to a device.

The variable name defined for each CLI must be unique. Otherwise, you cannot assign different values to those variables even though they are used in different CLIs. For example, if a variable say `$(description)` is used in two CLIs `set vlans $(name) description $(description)` and `set snmp description $(description)`, you will not be able to define different values to the descriptions. To define different values, you must change the variable name for one of the commands.

The [Table 27 on page 193](#) shows data types supported for the values entered for variables.

Table 27: Variable Data Types

Data Type	Description
Container	Holds other data types.
String	Contains character strings.
Integer [Number]	Specifies a numeric value without a fractional component.

Table 27: Variable Data Types (continued)

Data Type	Description
Boolean	Has two possible values: true and false. True if checked and False if unchecked.
Enumeration	Defines a variable to be a set of predefined constants. The variable is equal to one of the values that have been predefined for it.
Choice	Provides a radio button. Check the radio button to use the configuration option in the template.
String - Key [column in a table]	Identifies the uniqueness of the record in the table. If the table has a key specified, only one record with the given key could exist.

The Save option in the Create Quick Templates page enables you to save and also validate a template. If there are any conflicts in the configuration, you must resolve the conflicting variables in the configuration elements manually, before you deploy the configuration to the devices. Upon successful validation (and after you apply a template to a device), you can deploy the configurations (specified in the templates) to the devices. You can choose to deploy the configuration immediately, or at a later time. Depending upon the approval mode selected for your deployment, you can either deploy the changes directly or you can get an approval from the approver before deploying the changes. For more information about types of approval modes supported for deployments in Connectivity Services Director, see [“Setting Up User and System Preferences” on page 122](#).

Configuring and Managing Quick Templates

You can create and manage custom templates for your device configurations that are deployable through Connectivity Services Director. Unlike other features that support implementation of only some of the device configurations, quick templates enables you to set up all the configuration parameters for any supported device because it is Device Management Interface (DMI) schema-driven.

Each device type is described by a unique data model that contains all the configuration data for that device. The Schema window shows the device family that you select while you create a template and the DMI schema that lists all the possible fields and attributes for a type of device. The latest schema describe the new features associated with recent device releases. After you create a quick template, you can add or delete device configuration details to and from quick templates by loading the configuration data from the schema. You need to apply these templates to devices manually.

If you click the **More tips** link you are guided on the variable and the command syntax usages. It also provides instructions on how to issue sub-commands. When defining your network configuration in quick templates by using a particular command, ensure that you define the sub-commands individually. Stating sub-commands as a single command causes errors. For example, the commands `set snmp location xyz` and `set snmp contact admin@example.com` are valid when defined individually. However, if you combine these commands into the single command `set snmp location xyz contact admin@example.com`

schema validation treats the end command, **contact**, as an extra entry and displays an error.

To avoid any conflicts with the profile configurations while creating the template, a warning message **Please don't create any Profile conflict configuration** is displayed to indicate that you must not create a configuration as part of the template if the same configuration is available as part of the profile configuration.

The Templates page in the Quick Templates workspace lists the device templates created, in a tabular view. The [Table 28 on page 195](#) lists the columns in the table along with a description:

Table 28: Quick Templates

Column	Description
Creation Time	Date and time when the template was created.
Template Name	Name of the quick template.
Device Family	Name of the device family for which the template is created. Selecting the option Common indicates that the template is applicable for all the device families.
OS Version	Junos OS version of the device family selected.
Description	Description of the quick template.
Last Updated Time	Date and time when the template was last modified.
Last Updated By	User name of the person who created the template.

This topic describes:

- [Creating a Quick Template on page 196](#)
- [Applying Templates to Devices on page 197](#)
- [Editing a Quick Template on page 198](#)
- [Deleting a Quick Template on page 198](#)
- [Cloning a Quick Template on page 198](#)
- [Using the Quick Template Details Window on page 198](#)
- [Viewing Deployed Quick Templates on page 199](#)

Creating a Quick Template

Quick templates enable you create a template to define configurations for your devices. You can create and deploy quick templates from the Wired workspace.

To create a quick template:

1. Click the **Build** icon in the Connectivity Services Director banner.
2. Select **Wired > Tasks > Manage Quick Templates** in the Tasks pane.

The Manage Quick Template page appears.

3. Click **Create**.

The Create Quick Template page opens.

4. Specify the following details:

- **Name**—Type a name for the quick template. The quick template name is required. The quick template name must be unique and limited to 63 characters.
- **Description**—Type a description for the quick template. The description is optional and limited to 255 characters.
- **Device Family**—From the Device Family list, select an appropriate device family. Selecting the option **Common** in device family creates a generic template, which can be applied to any device family. Therefore, specify only the most common settings such as system, SNMP, or track group settings that are applicable to all the platforms. If you want to define the settings that are specific to a platform select the appropriate platform from the device family instead of the Common option. For the list of device families supported by Connectivity Services Director, see the latest [Connectivity Services Director Release Notes](#).



NOTE: ACX Series routers are listed when you select the **Common** option from the Device Family list on the Create Quick Template page. If you select the option as **MX** from the Device Family list, only MX Series routers are displayed on the Assign Quick Templates page. To apply quick templates for ACX Series routers, you must select the **Common** option as the device family type.

- **OS Version**—From the OS Version list, select an appropriate DMI Schema version running on that platform. If you are unable to locate the DMI schema for a device family, you can update the DMI schema version on the Junos Space server. For more information about updating the DMI schema on the Junos Space server, see Junos Space documentation.

The Schema window displays the device family and the OS version selected in this step.

5. Type or paste the Junos commands in the text area provided in the CLI commands section. Alternatively, you can navigate through the configuration option levels (at the left side) in Schema and double-click the configuration option you want to add to the quick template. The selected configuration option is displayed in the CLI Commands text area. The configuration options available here depend on the device family you selected.
6. Optionally, you can modify the configuration in the CLI Commands text area by using the tool bar functionalities such as undo, redo, cut, copy, paste, and find.
7. Click **Save**.

The template you created is displayed in the quick templates table.

Applying Templates to Devices

After you create a template, you can define your device configuration to be managed by using the quick templates, and apply these templates to the multiple devices.

To assign a template to a device:

1. Select the check box against the quick template for which you want to assign the profile.
2. Click **Assign**.

The Assign Quick Template : template names page opens.

3. Choose at least one device to which the profile needs to be assigned.
4. Click **Next**.
5. Choose a device and specify the quick template variables in Configure attributes page and click **Save**.

For example, when you configure a VLAN interface in a quick template, you can specify the variables VLAN and interface names for that template for a selected device.
6. Optionally, you can apply the settings specified here to all the selected devices of a device family by selecting the check box against the option **Apply above settings to all other selected devices**.
7. Click **Next** and then click **Finish**.
8. Review the profile association with the quick template and then click **Finish**.

Editing a Quick Template

You can edit a quick template to modify configurations for your devices.

To edit a quick template:

1. Select the check box against the quick template that you want to modify.
2. Click **Edit**.

The Edit Quick Template : template name page opens.

3. Make the required changes to the quick template and click **Save**.

Deleting a Quick Template

To delete a quick template:

1. Select the check box against the quick template that you want to delete.
2. Click **Delete**.

The Delete Quick Templates window opens.

3. Click **Yes** to delete the quick template; else click **No**.

Cloning a Quick Template

A cloned quick template is a copy of an existing quick template. You can use the quick template as a master copy to create clone of that template. When you clone a quick template, you create a copy of the entire device configuration, including its settings, and other contents. Cloning a quick template saves time if you are deploying device configuration that are similar to the master copy, rather than creating a template and defining configurations multiple times.

To create a copy of an existing template:

1. Select the check box against the quick template you want to clone.
2. Click **Clone**.

The cloned template named master template-clone is shown in the list of templates.

Using the Quick Template Details Window

Use the Quick Template Details window to view the details of the quick template. [Table 29 on page 199](#) describes the fields in this window.

Table 29: Quick Template Details

Field	Description
Name	Displays the name of the quick template.
Description	Provides a description of the quick template.
Device Family	Displays the device family for which quick template is created.
OS Version	Displays the Junos OS version for the selected device family.
CLI Commands	Displays the CLI commands configured for the device family.

Viewing Deployed Quick Templates

You deploy the device configurations defined in a quick template after you have applied the template to a device. The View Deployed Templates option enables an administrator or an operator to view the list of templates that are deployed to the devices.

You can mouse over the template name to view the date and time when the template was created and last modified.

The View Deployed Templates page lists the deployed templates device in a tabular view. The [Table 30 on page 199](#) lists the columns in the table along with a description.

Table 30: View Deployed Template

Column	Description
Template Name	Indicates the name of the template whose configuration is deployed to the system.
Creation Time	Indicates the date and time when the template was created.
Last Updated Time	Indicates the date and time when the template was last modified.
User Name	Indicates the user name of the person who created the template.

Depending upon the type of approval mode configured—Manual Approval or Auto Approval mode— you can either deploy the device configurations defined in the template directly or by pursuing an approval from a configuration approver for the device changes.

To view the list of quick templates that are deployed to a device:

1. Click the Build Mode icon in the Connectivity Services Director banner.
2. Select a device in the View pane.
The View Deployed Templates option appears under Wired > Tasks.
3. Click **View Deployed Templates**.

The Deployed Templates For Device: device name page displays listing the templates applied for that device.

CHAPTER 12

Configuring Device Settings

- [Understanding Device Common Settings Profiles on page 201](#)
- [Creating and Managing Device Common Settings on page 201](#)
- [Assigning Device Common Settings to Devices on page 214](#)

Understanding Device Common Settings Profiles

Connectivity Services Director enables you to configure device-level settings for routers in the Device Common Settings profile. Once you create the profiles, you can assign the profiles to a switch or a controller and you can deploy the profiles using the Deploy mode tasks.

Connectivity Services Director also creates Device Common Settings profiles when it discovers devices. It creates a Device Common Settings profile for each device it discovers, importing the device-level settings from the device into the profile.

While configuring the profiles, you can specify the basic settings, which includes the profile name, device user list, and time settings. Apart from the basic settings, you can optionally specify the management and protocol settings too.

Related Documentation

- [Creating and Managing Device Common Settings on page 201](#)
- [Assigning Device Common Settings to Devices on page 214](#)

Creating and Managing Device Common Settings

Use the Manage Device Common Settings page to create new device common settings for routing devices and to manage the existing device common settings.

This topic describes:

- [Managing Device Common Settings on page 202](#)
- [Creating a Device Common Settings Profile on page 203](#)
- [Specifying Basic Settings for Device Common Settings on page 205](#)
- [Specifying Management Settings for Routing Device Common Settings on page 208](#)
- [Specifying Protocol Settings for Routing Device Common Settings on page 211](#)

- [Reviewing and Saving a Device Common Settings Configuration on page 213](#)
- [What to Do Next on page 214](#)

Managing Device Common Settings

From the Manage Device Common Settings page, you can:

- Create a new Device Common Settings profile by clicking **Add**. For directions, see [“Creating a Device Common Settings Profile” on page 203](#).
- Modify an existing Device Common Settings profile by selecting it and clicking **Edit**.
- Assign a Device Common Settings profile to a device by selecting a profile and clicking **Assign**. For directions, see [“Assigning Device Common Settings to Devices” on page 214](#).
- Modify an existing assignment of a Device Common Settings profile by selecting the profile and clicking **Edit Assignment**.
- View information about a Device Common Settings profile by either double-clicking the profile name or by selecting the profile and clicking **Details**.
- Delete a Device Common Settings profile by selecting a profile and clicking **Delete**.



TIP: You cannot delete common settings profiles that are in use—that is, assigned to devices or used by other profiles. To see the current assignments for a profile, select the profile and click **Details**.

- Clone a Device Common Settings profile by selecting a profile and clicking **Clone**.

[Table 31 on page 202](#) describes the device information available on the Manage Device Common Settings page. This page lists all Device profiles defined for your network, regardless of your current selected scope in the network view.

Table 31: Manage Device Common Settings Settings

Field Name	Action
Profile Name	Name given to the profile when the profile was created.
Family Type	The device family; ACX Series router, M Series router, MX Series router, and PTX Series router.
Description	Description of the Device profile entered when the profile was created.
Assignment State	Displays the assignment state of the profile. A profile can be: <ul style="list-style-type: none"> • Unassigned—When the profile is not assigned to any device • Deployed—When the profile is assigned to a device and is deployed from Deploy mode • Pending Deployment—When the profile is assigned to a device, but not yet deployed in the network. For deployment directions, see Deploying Configuration to Devices.

Table 31: Manage Device Common Settings Settings (continued)

Field Name	Action
Assigned to	Displays the number of devices to which the profile assignment is done.
Creation Time	Date and time when the profile was created.
Last Updated Time	Date and time when the profile was last modified.
User Name	The username of the person who created or modified the profile.



TIP: All columns might not be displayed. To show or hide fields listed in the Manage Authorization Profiles table, click the down arrow on the field header, select **Columns**, and select or clear the check box adjacent to the field that you want to show or hide.

Creating a Device Common Settings Profile

In Connectivity Services Director, as an administrator, you can configure Device Common Settings profiles by using the Create Device Profile page for devices. You can view the summary of the configurations before saving the Device profile.

At minimum, you must specify the Device profile and profile name in the workflow. You can include additional configuration such as:

- Device users
- Management services
- Multicast, spanning-tree protocol (STP)
- Domain Name Server
- DHCP servers, DHCP Relay servers, Login Banner, and Global PoE settings for switches

You can create profiles on the basis of the device family and each Device profile is specific to a device family. After you create a Device profile, you assign the profiles to different devices.




NOTE: You can assign only one profile to a device. However, you can assign the same profile to multiple devices.

To create a Device profile:

1. Under Views, select one of these options: **Logical View**, **Device View** or **Custom Group View**.



TIP: Do not select **Dashboard View** or **Topology View**.

2. Click  in the Connectivity Services Director banner.
3. From the Tasks pane, select the type of network, the appropriate functional area, and select the name of the profile that you want to create. For example, to create a QoS profile for a device, click **Wired** > **Profiles** > **CoS**. The appropriate Manage Profile page opens.

4. Click **Add** to add a new profile.

If you chose to create a profile for the wired network, Connectivity Services Director opens the Device Family Chooser window.

- a. From the Device Family Chooser, select the device family for which you want to create a profile. The available device families are **Switching (EX)**, **Campus Switching ELS** (Enhanced Layer 2 Software), **Data Center Switching Non-ELS** and **Data Center Switching ELS**.
- b. Click **OK**.

The Create Device Common Settings wizard for the selected device family is displayed. It consists of four sections, Basic Settings, Management Settings, Protocol Settings, and Review.

If you chose to create a profile for the wireless network, Connectivity Services Director opens the Create Device Common Settings for Wireless wizard.

5. Specify the basic settings. Complete the Basic Setting wizard page as described in both the online help and in [“Specifying Basic Settings for Device Common Settings” on page 205](#).
6. When you have completed the basic settings, either click **Next** or click **Management Settings** at the top of the wizard window.
7. Complete the Management Settings described in both the online help and in the section [“Specifying Management Settings for Routing Device Common Settings” on page 208](#).
8. When you have completed the management settings, click **Next**.

- 9. Complete the protocol settings.
- 10. When you have completed the protocol settings, either click **Next** or click **Review** at the top of the wizard window.
- 11. You can either save your profile or make changes to your profile from the Review page. For more information, see “[Reviewing and Saving a Device Common Settings Configuration](#)” on page 213.
- 12. Click **Finish** to save the Device profile configuration.

The system saves the Device profile and displays the Manage Device Common Settings page. Your new or modified Device profile is listed in the table.

Specifying Basic Settings for Device Common Settings

To configure the basic settings for any Device Common Settings profile, enter the settings described in [Table 32 on page 205](#). Mandatory settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 32: Device Profile Basic Settings

Field	Action
Profile Name	Type a name for the profile.
Description	Type a description of the profile containing up to 256 characters.
Login Banner for EX Series switches, Campus Switching ELS, and Data Center Switching	Enter the banner text—this text is displayed in the banner when you log in to the device.
Country Code for wireless LAN controllers only	Select the country code for the wireless LAN controllers. Country code settings are required on the primary wireless seed controller. TIP: Do not set the country code if you plan to provision the Device profile for active secondary and member nodes that will be part of a cluster.

Device Users

Table 32: Device Profile Basic Settings (continued)

Field	Action
Task: Add a Device User	<p>To add a device user:</p> <ol style="list-style-type: none"> Click Add under Device Users. The Add User window opens. Provide a username and password. Confirm the password. Enter a combination of 6 through 128 alphanumeric characters and special characters. The password is case sensitive and must be a combination of at least two different types of characters or a combination of upper case and lower case letters. TIP: Do not create a user with the name <i>root</i>. Select a role for the user: <ul style="list-style-type: none"> For switches, the role options are: Operator, Read-only, Super-user, or Unauthorized. Operators have clear, network, reset, trace, and view privileges. Super-Users have all privileges. For wireless controllers, the role options are: Framed, Administrative, or NAS-Prompt. Framed users have network user access only. Administrative users have access to the controller, including the enabled (configuration) mode. NAS-Prompt users have administrative access to the controller, excluding enabled mode. Click OK. The user is added to the list of Device Users. TIP: To edit an entry, select a row from the Device Users table and click Edit to modify the information. To delete an entry select a row from the Device Users table and click Delete to delete the user.

Time Settings

Time settings apply to all platforms. However, the setting for offset applies exclusively to wireless.

Time Zone	Select a country and time zone from the list. For wireless, you can also change the setting for Offset.
-----------	---

Table 32: Device Profile Basic Settings (continued)

Field	Action
Add a Time Server	<p>To add a time server:</p> <ol style="list-style-type: none">1. Click Add under Time Server. The Add Time Server window opens.2. Provide an IP address and, optionally for switches only, mark the corresponding time server as Preferred. TIP: Valid IP addresses are 1.0.0.1 through 255.255.255.254 excluding 127.x.x.x and 224.0.0.0 through 239.255.255.2553. Click OK. The server is added to the list of Time Servers. TIP: To edit the settings of a time server, select it and then click Edit.

To configure management settings, click **Next** or click **Management Settings** at the top of the wizard window. To skip the management settings and protocol settings, click **Review** at the top of the wizard window.

Specifying Management Settings for Routing Device Common Settings

To configure the management settings for an Routing Device profile:

1. Enter the settings described in [Table 33 on page 209](#). All settings are optional. Default values are applied to the configuration if you skip the management settings configuration.

Table 33: Device Profile Management Settings for Routing

Task	Action
Enable Services	You can enable one or more network protocol services for this Device profile: FTP , TELNET , HTTPS , or HTTP .
Configure PoE	<p>To add Power over Ethernet (PoE) configuration for Routing, enable Configure PoE and provide these settings:</p> <p>NOTE: PoE configuration will be added only to switches that support PoE.</p> <ol style="list-style-type: none"> a. Using the arrows, adjust the Guard Band value from 0 through 19 watts. A guard band reserves a specified amount of power from the PoE power budget for the router or line card in case of a spike in PoE consumption. For routers with multiple PoE line cards, the guard band wattage is set to the specified value on all line cards, unless a line card has been explicitly configured with a different value. b. Select a Management Mode for PoE, either Class or Static: <ul style="list-style-type: none"> • Class Management—In class PoE management mode, the maximum power for an interface is determined by the class of the connected powered device. • Static Management—In the static PoE management mode, you specify the maximum power for each PoE interface. The PoE controller then allocates this amount of power to the interface from its total budget. c. For PoE Global, you can indicate Enable All, Disable All, or None. <p>NOTE: If you deselect Configure PoE, PoE is disabled and the global PoE settings supported by this profile (poe guard-band, poe fpc all guard-band, poe management, poe fpc all management, and poe interface all) are deleted from the switch when the profile is deployed on the switch.</p>

Syslog Settings

Optionally, expand the Syslog Settings and provide the following system logging settings.

Table 33: Device Profile Management Settings for Routing (continued)

Task	Action
Enable Device Logging for Switches	<p>To enable device logging for switches:</p> <ol style="list-style-type: none"> Under Enable Device Log, click Add. The Add Log window opens. Select the log type for switching, either Console, File, User, or Host. <ul style="list-style-type: none"> Console logging sends system log messages to the console. File logging sends system log messages to the file you specify in File Name. User logging sends system log messages to the terminal session of the user specified in User Name. You will also need to provide the name of the user. Host logging sends system log messages to the server specified in Host. Host can be either an IP address or host name. Under Services, click Add. The phrase <i>Click to enter value</i> appears in both the Service column and Severity Filter column. Click the phrase <i>Click to enter value</i> in the Service column. A list box replaces the phrase in the Service column. From the Service list, select a logging service: Any, Authorization, Change-log, Conflict-log, Daemon, DFC, External, Firewall, FTP, Interactive-commands, Kernel, NTP, PFE, Security or User. Click the phrase <i>Click to enter value</i> in the Severity Filter column. A list box replaces the phrase in the Severity Filter column. Select an available severity filter from the list, either Alert, Any, Critical, Emergency, Error, Info, None, Notice, or Warning. The filter is added to the list of Severity Filters. The filter is activated when the corresponding service is triggered. Click OK. The log is added to the Enable Device Log list.
Edit Logging Settings	Select a Log Type from the Enable Device Log list and click Edit to change the configuration.

Table 33: Device Profile Management Settings for Routing (continued)

Task	Action
Delete Logging Settings	Select a Log Type from the Enable Device Log list and click Delete to remove the server configuration.

To configure protocol settings, either click **Next** or click **Protocol Settings**. To use the default protocol settings, skip to final review by clicking **Review** at the top of the wizard window.

Specifying Protocol Settings for Routing Device Common Settings

To configure the protocol settings for an Routing Device profile, enter the settings described in [Table 34 on page 211](#). All settings are optional.

Table 34: Device Profile Protocol Settings for Routing

Field	Action
Enable Storm Control	
Select this option to enable storm control on a switch.	
Spanning Tree Settings	
Spanning Tree Protocol Settings for switches only	<p>Select one of spanning-tree protocol (STP) settings for switches: STP, RSTP (default), MSTP, or None of these.</p> <ul style="list-style-type: none"> Spanning Tree Protocol—With STP configured, the switches use the IEEE 802.1D 2004 specification, force version 0. This configuration runs a version of RSTP that is compatible with classic, basic STP as defined in the 802.1D 1998 specification. Rapid Spanning Tree Protocol—RSTP provides faster reconvergence time than the original STP both by identifying certain links as point-to-point and by using protocol handshake messages rather than fixed timeouts. VLAN Spanning Tree Protocol (VSTP) and RSTP can be configured concurrently. You can selectively configure up to 253 VLANs by using VSTP; the remaining VLANs will be configured by using RSTP. VSTP and RSTP are the only spanning-tree protocols that can be configured concurrently on a switch. Multiple Spanning Tree Protocol—MSTP enables multiple VLANs to be mapped to the same spanning-tree instance, reducing the number of spanning-tree instances needed to support a large number of VLANs. MSTP provides multiple forwarding paths for data traffic and enables load-balancing. It improves the fault tolerance of the network because a failure in one instance, or forwarding path, does not affect other instances. <p>You can also select the Enable VSTP check box to enable VSTP.</p>
Multicast Settings	
Enable IGMP	Selecting this option enables Internet Group Management Protocol (IGMP) on all the interfaces for the selected device. Default is disabled. IGMP is a communications protocol used by both hosts and adjacent routers on IP networks to establish multicast group memberships.
Enable IGMP Snooping	Enables IGMP snooping on all VLANs. Default is enabled.

Table 34: Device Profile Protocol Settings for Routing (continued)

Field	Action
Enable DHCP Relay Select this option to display the DHCP Relay settings.	
Add DHCP Relay to Device Profile	<p>To add DHCP Relay to this Device Profile:</p> <ol style="list-style-type: none">1. Select Legacy DHCP Relay (default).2. Add one or more DHCP servers to the Device Common Settings profile:<ol style="list-style-type: none">a. Click Add under DHCP Servers. The Add Server window opens.b. Type an IP Address.c. Click OK. The server is added to the list of DHCP Servers.

Table 34: Device Profile Protocol Settings for Routing (continued)

Field	Action
Add Extended DHCP Relay to a Device Profile	<p>To add Extended DHCP Relay to this Device Profile:</p> <ol style="list-style-type: none"> 1. Select Extended DHCP Relay instead of Legacy DHCP Relay. 2. Add one or more DHCP Server Groups to the Device Common Settings profile: <ol style="list-style-type: none"> a. Click Add under Add DHCP Servers Group. The Add Server Group window opens. b. Provide a name for the server group. c. Optionally, make this an active server group by checking Active Group. d. Add servers to the group by clicking Add under DHCP Servers. The phrase <i>Click to enter value</i> appears in the IP Address column. e. Select <i>Click to enter value</i> and then enter an IP Address. f. Click OK. The server is added to the DHCP server group list. g. Add a relay interface group by clicking Add under Add Relay Interface Group. The Add DHCP Relay Interface window opens. h. Type a DHCP interface group name. i. Select a server group from the Server Group list. j. Click OK. The group is added to the Relay Interface Group list.

Click either **Next** or **Review**, to see the Review page. For review directions, see [“Reviewing and Saving a Device Common Settings Configuration” on page 213](#).

Reviewing and Saving a Device Common Settings Configuration

From this page, you can save or make changes to Device Common Settings:

- To make changes to the settings, click the **Edit** associated with the configuration you want to change.

Alternatively, you can also click appropriate sections of the workflow at the top of the page that corresponds to the configuration you want to change.

When you have completed your modifications, click **Review** to return to this page.

- To save a new profile or to save modified settings to an existing profile, click **Finish**.

The Manage Device Common Settings page is displayed with the new or modified profile listed

What to Do Next

Once the Device Common Settings profile is created, you must assign the profile to the required device by using the Manage Device Profile page and then deploy the Device profile by using the **Deploy** mode. To assign a Device Common Settings profile to a device, see *Security Director Release Notes*.



NOTE: A device can have only one Device profile assigned to it. However, you can assign the same Device profile to multiple devices.

Assigning Device Common Settings to Devices

Once a Device Common Settings profile is created or discovered (system-created profile), you must assign it to devices using the steps described in this topic. You can assign a Device profile to a either single device, a series of single devices, or a Custom Group of devices (see [“Creating Custom Device Groups” on page 188](#)).



NOTE: A device can have only one Device Common Settings profile assigned to it.


You must have one or more device profiles created or discovered before you can assign a device profile to a device. When you deploy an assigned device profile, the configuration is pushed onto the device.

This topic describes:

- [Assigning Device Common Settings on page 214](#)
- [Editing the Assignments of the Device Common Setting on page 216](#)

Assigning Device Common Settings

To assign device common settings to either a single device, a series of single devices, or members of a Custom Group:

1. Click  in the Connectivity Services Director banner.
2. Select **Device Common Settings** from the Profile and Configuration Management menu in the Tasks pane.

The Manage Device Common Settings page is displayed. The page displays all the device profiles that you configured as well as the system-created profiles detected during device discovery.

3. Select an undeployed profile from the list of profiles and then click **Assign**.

The Assign Device Profile page for the selected device family appears with a wizard consisting of three parts, Device Selection, Profile Assignment, and Review. Device Selection is displayed.

4. Expand the Device Selection object tree and select one or more objects to receive the device profile. You must place a check next to a device to select it—simply highlighting the device does not select it.



NOTE: If Connectivity Services Director fails to read the configuration of one or more devices after device discovery, those devices are not displayed in the Device Selection list. You will not be able to assign profiles to those devices. The Manage Jobs page in System mode displays details of the device discovery jobs. Use the information displayed on this page to take appropriate corrective steps to enable Connectivity Services Director to reread the configuration of the failed device. For more information, see [“Discovering Devices in a Physical Network” on page 177](#).

5. Click either **Next** or click **Profile Assignment** from the wizard workflow.

The Profile Assignment page opens, displaying your selections, including their Device (name), Type, Assigned To, and Attributes. The Assigned To column now has the entry DEVICE and the Attributes column has the entry Undefined.

6. Click **Define** in the **Attributes** column in the Assignments table to configure the attributes.

The Configure Attributes window opens, listing all the Layer 3 interfaces available on the device.

- a. Select the Layer 3 interfaces that are required for DHCP relay from the Available list and using the right arrow, move them to the Selected list. You can reorder the interfaces using the UP and DOWN arrows.
 - b. Click **Save** to save the interface list and close the Configure Attributes window.
7. You can view the assignment details for the selected device and also remove any assignments:
 - To view the assignment details, select the device and click **View Assignments**.

The Profile Details page for selected device appears. Expand the **Device** name to view the details of the assignment. The assignment status displays the status whether the device is deployed or is pending device update, and so on.

- To delete a device common setting assignment for a device, select the device from the Assignments table and click **Remove**.
8. Click **Next** or click **Review** from the wizard workflow to review the assignments. On the Review page, click **Edit** to edit the profile assignment.
 9. Click **Finish** once you are done reviewing the profile assignment.

The Create Profile Assignments Job Details window appears with a status report for the profile assignment job—click **OK** to close this window. If you have assigned the profile to a large number of objects, the profile assignment job can take some time to complete. Instead of waiting for the Job Details dialog box to report job completion status, you can close it and check the details of the profile assignment job at a later time using the Manage Job task in System mode.



NOTE: If any assignment fails, the profile assignment job fails and none of the assignments are created. Check the details for the profile assignment job for information about why the assignment failed.

An assigned Device profile has the Assignment State *Pending Deployment* in the Manage Device Common Settings list. Deploy any device profile in this state.

To view the details of a profile, select the profile from the Manage Device Common Settings page and then click **Details**.

Editing the Assignments of the Device Common Setting

Use the Edit Assignments page to change device common setting assignments. To edit an existing assignment:

1. Select a profile from the **Manage Device Common Settings** page and click **Edit Assignment**.

The Edit Assignments page for the selected device appears.

2. Expand the **Devices** cabinet and make the desired change from the **Operation** column of the table.
3. Click **Define** from the **Attributes** column of the table to modify the attributes.

The Configure attributes page is displayed listing all the Layer 3 interfaces available on the device.

- Select the Layer 3 interfaces that are required for DHCP relay from the Available box and using the right arrow, move them to the Selected box.

You can rearrange the order of the interfaces using the up and down arrows.

- Click **Save** after you are done with selecting the interfaces.
4. Click **Apply** once you are done with the changes.

The Manage Device Common Settings page is displayed.

Configuring Class of Service (CoS)

- [Understanding Class of Service \(CoS\) Profiles on page 219](#)
- [Creating and Managing Wired CoS Profiles on page 224](#)

Understanding Class of Service (CoS) Profiles

When a network experiences congestion and delay, some packets must be prioritized to avoid random loss of data. Class of service (CoS) (also known as QoS) accomplishes this prioritization by dividing similar types of traffic, such as e-mail, streaming video, voice, large document file transfer, into classes. You then apply different levels of priority, such as those for throughput and packet loss, to each group, and thereby control traffic behavior. For example, when packets must be dropped, you can ensure that packet loss takes place according to your configured rules. CoS also enables you to rewrite the Differentiated Services code point (DSCP), IP precedence, or 802.1p CoS bits of packets exiting a specific interface, thus enabling you to tailor outgoing packets to meet the network requirements of remote peers.

On Data Center Switching devices, CoS can be used to configure Ethernet interfaces to support Fibre Channel over Ethernet (FCoE) traffic.

- [How Would I Use CoS \(also known as QoS\)? on page 219](#)
- [How Does CoS Work? on page 220](#)
- [What Wireless Network Traffic Aspects Can I Control Using CoS? on page 221](#)
- [What CoS Parameters Can I Control? on page 222](#)
- [What Are the Default CoS Traffic Types? on page 222](#)
- [Data Center Switching CoS Configuration on page 223](#)
- [How Do I Implement Class of Service? on page 223](#)
- [Editing Discovered CoS Profiles on page 223](#)

How Would I Use CoS (also known as QoS)?

On an Ethernet trunk, you can mark frames with a class-of-service (CoS) value. CoS is used to define trunk connections as full-duplex, incoming only, or outgoing only.

Network devices such as routers and switches can be configured to use existing CoS values on incoming packets from other devices (trust mode), or can rewrite the CoS values to something completely different. Layer 2 markings also can extend to the WAN;

for example, with a frame relay network. CoS is usually limited to use within an organization's intranet.

With legacy telephone systems, CoS can be used to define the permissions an extension will have on a private branch exchange (PBX) or Centrex. Some users might need extended voicemail message retention or the ability to forward calls to a cell phone, while others have no need to make calls outside the office. Permissions for a group of extensions can be changed by modifying a CoS variable applied to the entire group.



NOTE: CoS configurations can be complicated, so unless it is required, we recommend that you do not alter the default class names or queue number associations.

How Do I Create CoS Groups?

Use 802.1Q tagged VLANs to group users and enable CoS to set priorities supported by downstream devices.

How Is CoS Different From QoS?

CoS operates only on 802.1Q VLAN Ethernet at the data link layer (layer 2), while quality-of-service (QoS) mechanisms operate at the IP network layer (layer 3). 802.1p Layer 2 tagging can be used by QoS to differentiate and shape network traffic.

How Does CoS Work?

CoS is a 3-bit field in an Ethernet frame header when 802.1Q VLAN tagging has been applied. The 3-bit field specifies a priority value between 0 and 7 that can be used by QoS to differentiate and shape network traffic. Different devices use different priority values. When you choose to create a CoS profile, Connectivity Services Director displays the priority based on the device family that you chose. You can modify these or add more priority values

It is helpful to think of forwarding classes as output queues. In effect, the end result of classification is the identification of an output queue for a particular packet. For a classifier to assign an output queue to each packet, it must associate the packet with one of the forwarding classes listed in [Table 35 on page 220](#).

Table 35: 3-Bit CoS Field in Ethernet Header with VLAN Tagging

CoS Value	Priority Applied
0	Best-effort is a backward compatibility feature.
1	Assured-forwarding offers a high-level of assurance that the packets are delivered as long as the packet flow from the client stays within a certain Service profile that you define.

Table 35: 3-Bit CoS Field in Ethernet Header with VLAN Tagging (continued)

CoS Value	Priority Applied
2	<p>Multicast assured-forwarding offers a high level of assurance that the multicast packets are delivered as long as the packet flow from the customer stays within a certain Service profile that you define. The software accepts excess traffic, but it applies a tail drop profile to determine if the excess packets are dropped and not forwarded. Up to two drop probabilities (low and high) are defined for this service class.</p> <p>Multicast expedited-forwarding delivers assured bandwidth, low loss, low delay, and low delay variation (jitter) end-to-end for multicast packets in this service class. The software accepts excess traffic in this class, but in contrast to the multicast assured forwarding class, out-of-profile multicast expedited-forwarding class packets can be forwarded out of sequence or dropped.</p> <p>Multicast best-effort does not apply any special CoS handling to the multicast packets. These packets are usually dropped under congested network conditions.</p>
3	
4	
5	Expedited-forwarding delivers assured bandwidth, low loss, low delay, and low delay variation (jitter) end-to-end for packets in this service class.
6	
7	Network-connect

Note: The forwarding classes multicast expedited-forwarding, multicast assured-forwarding, and multicast best-effort are applicable to ACX, M, MX, PTX Series routers.

Differentiated Services indicate how a packet is forwarded. Because the three bits used in Layer 2 simple priority tagging provide minimal direction in managing traffic, the protocol Differentiated Services (DS or DiffServ) was developed to enhance traffic differentiation.

What Wireless Network Traffic Aspects Can I Control Using CoS?

In addition to separating traffic into classes, you can also optionally configure these settings with CoS:

- Apply a bandwidth limit to the data sessions and to aggregated categories such as trunk interfaces, Layer 3 interfaces, access interfaces, and routed VLAN interfaces.
- Assign the same CoS level to all traffic on the Service profile SSID. This is called static CoS and overrides settings indicated on the 802.1p, overrides DSCP markings in the packets themselves, and disregards any filters that mark CoS. You indicate the value assigned to all user traffic.
- Allow the controller to use the client DSCP for radio ingress traffic and ignore Wi-Fi Multimedia (WMM).
- Specify a traffic class for voice traffic and optionally apply a bandwidth limit to the voice sessions and to aggregated categories. You can also enable static CoS for voice traffic, which overrides settings indicated on the 802.1p, overrides DSCP markings in

the packets themselves, and disregards any filters that mark CoS. You indicate the value assigned to all voice traffic.

- Specify which of 11 forwarding queues are used. You can modify the action corresponding to each forwarding queue to suit your requirements. This is referred to as access categories.

What CoS Parameters Can I Control?

You can use CoS profiles to group a set of class of service (CoS) parameters and apply it to one or more interfaces. You can configure the following parameters within a CoS profile:

- Classifiers—Packet classification refers to the examination of an incoming packet. This function associates the packet with a particular CoS servicing level.
- Scheduler maps—Schedulers define the properties of output queues. These properties include the amount of interface bandwidth assigned to the queue, the size of the memory buffer allocated for storing packets, the priority of the queue, and the drop profiles associated with the queue. You associate the schedulers with forwarding classes by means of scheduler maps. You can then associate each scheduler map with an interface, thereby configuring the queues, packet schedulers, and tail drop processes that operate according to this mapping.
- Rewrite values—A rewrite rule modifies the appropriate CoS bits in an outgoing packet. Modification of CoS bits enables the next downstream device to classify the packet into the appropriate service group. Rewriting or marking outbound packets is useful when the device is at the border of a network and must alter the CoS values to meet the policies of the targeted peer.
- Traffic-control profile—Traffic-control profiles enable traffic limitation of a certain class to a specified bandwidth and burst size. Packets exceeding the limits can be discarded, or can be assigned to a different forwarding class, a different loss priority, or both.

What Are the Default CoS Traffic Types?

On EX Series switches, the system provides you with these four predefined traffic types—Data, Voice, Video, and Network Control—with these default traffic configuration and shaping details:

- Data—Forwarding queue 0 (nd_best-effort), Buffer size 50%, Bandwidth reserved 30%
- Voice—Forwarding queue 5 (nd_expedited-forwarding), Buffer size 20%, Bandwidth reserved 0%
- Video—Forwarding queue 4 (nd_video-forwarding), Buffer size 20%, Bandwidth reserved 70%
- Network Control—Forwarding queue 7 (nd_network-control), Buffer size 10%, Bandwidth reserved 0%

For Campus Switching ELS, the system provides you with these four predefined traffic types—Data, Voice, Video, and Network Control—with these default traffic configuration and shaping details:

- Data—Forwarding queue 0 (nd_best-effort), Buffer size 50%, Bandwidth reserved 30%
- Voice—Forwarding queue 1 (nd_expedited-forwarding), Buffer size 20%, Bandwidth reserved 0%
- Video—Forwarding queue 2 (nd_video-forwarding), Buffer size 20%, Bandwidth reserved 70%
- Network Control—Forwarding queue 3 (nd_network-control), Buffer size 10%, Bandwidth reserved 0%

For Campus Switching ELS with *Hierarchical Post Scheduling* (Juniper Networks EX4600 Ethernet switches), Connectivity Services Director provides you with predefined forwarding classes—nd_cs_best-effort, nd_cs_video-forwarding, nd_cs_expedited-forwarding, and nd_cs_network-control. These forwarding classes are grouped under two priority groups—data_video_pg and voice_control_pg.

On data center switches, the system provides you with forwarding classes—nd_dc_best-effort, nd_dc_network-control, nd_dc_fcoe, nd_dc_no-loss, and nd_dc_mcast. These forwarding classes are grouped under three priority groups—data_control_pg, fcoe_noloss_pg, and multicast_pg.

For both Campus Switching ELS with *Hierarchical Post Scheduling* and Data Center Switching, you can modify and customize each of these priority groups and forwarding classes. For more details, see [“Creating and Managing Wired CoS Profiles” on page 224](#).

Data Center Switching CoS Configuration

For data center switching devices, these additional CoS features are available:

- Hierarchical Port Scheduling (ETS)—Hierarchical port scheduling (Enhanced Transmission Selection, or ETS) is a two-tier process that provides better port bandwidth utilization and greater flexibility to allocate resources to queues and to groups of queues.
- Priority-based flow control (PFC)—A link-level flow control mechanism.

How Do I Implement Class of Service?

CoS can be implemented from the MSS CLI, from Connectivity Services Director. RingMaster configures unicast traffic but does not configure multicast traffic. For directions to implement CoS from Connectivity Services Director, see [“Creating and Managing Wired CoS Profiles” on page 224](#).

Editing Discovered CoS Profiles

Duplicate scheduler configuration is deployed to the device when you edit a CoS profile that are automatically created by Connectivity Services Director as part of device discovery or out-of-band changes. In CoS configuration, a single classifier can be associated to

multiple ports regardless of the other CoS configuration. When Connectivity Services Director discovers a device with such configuration it will create multiple profiles, based on the difference in other CoS configurations, and mapped to same classifier configuration. If you modify classifier settings in such a CoS profile that is created automatically by Connectivity Services Director, Connectivity Services Director cannot modify the configuration because it is mapped to multiple profiles. Whenever you modify such a CoS profile that is created automatically, Connectivity Services Director will create new classifier settings configuration on the device and map the same to it, without affecting the existing classifier settings. Newly created classifier settings will have a name generated based on the profile name. Even if only one profile is mapped to the classifier settings, Connectivity Services Director creates new classifier settings and the old settings are orphaned.



NOTE: This behavior is applicable to both hierarchical and non hierarchical profiles, and is applicable for congestion notification profile name, traffic control profile name, scheduler map name, classifier name and rewrite rule settings.

**Related
Documentation**

- [Creating and Managing Wired CoS Profiles on page 224](#)

Creating and Managing Wired CoS Profiles

CoS profiles enable the grouping of class-of-service (CoS) parameters and apply them to one or more interfaces. Connectivity Services Director provides you with predefined traffic types for each CoS profile that you create. These traffic types represent the most common types of traffic for the device type. Each of these templates has preconfigured values for all CoS parameters based on the typical application requirements. You can change the preconfigured values of these parameters to suit your requirements.

This topic describes:

- [Managing Wired CoS Profiles on page 225](#)
- [Using the Default CoS Profiles for Routers on page 226](#)
- [Using the Default CoS Profiles for Campus Switching ELS with Hierarchical Port Scheduling on page 226](#)
- [Using the Default CoS Profiles for Data Center Switching on page 226](#)
- [Creating a Wired CoS Profile on page 227](#)
- [Specifying Settings for a Routing, Switching, and Campus Switching ELS CoS Profile on page 228](#)
- [Specifying Settings for a Campus Switching ELS CoS Profile with Hierarchical Port Scheduling \(ETS\) on page 232](#)
- [Specifying Settings for a Data Center Switching CoS Profile on page 236](#)
- [What to Do Next on page 243](#)

Managing Wired CoS Profiles

From the Manage CoS Profiles page, you can:

- Create a new CoS profile by clicking **Add**. For details, see “[Creating a Wired CoS Profile](#)” on page 227.
- Modify an existing CoS profile by selecting it and clicking **Edit**.
- View information about a profile by selecting the profile and clicking **Details**.
- Delete a CoS profile by selecting a profile and clicking **Delete**.



TIP: You cannot delete profiles that are in use—that is, assigned to objects or used by other profiles. To see the current assignments for a profile, select the profile and click **Details**.

- Clone an existing CoS profile by selecting it and clicking **Clone**.

[Table 36 on page 225](#) describes the information provided about wired CoS profiles on the Manage CoS Profiles page. This page lists all CoS profiles defined for your network, regardless of the scope you selected in the network view.

Table 36: Managing Wired CoS Profile Fields

Field	Description
Profile Name	Name given to the profile when the profile was created.
Family Type	The device family on which the profile was created: ACX Series routers, M Series routers, MX Series routers, PTX Series routers.
Description	Description of the profile that was entered when the profile was created. If the profile was created by using the CLI and then discovered by Connectivity Services Director, the description is <i>Profile created as part of device discovery</i> . TIP: To display the entire description, you might need to resize the Description column by clicking the column border in the heading and dragging it.
Creation Time	Date and time when the profile was created.
Update Time	Date and time when the profile was last modified.
User Name	The username of the user who created or modified the profile.



TIP: All columns might not be displayed. To show or hide fields listed in the Manage Authorization Profiles table, click the down arrow on the field header,

select **Columns**, and select or clear the check box adjacent to the field that you want to show or hide.

.....

Using the Default CoS Profiles for Routers

When you install Connectivity Services Director, a default CoS profile (juniper_CoS_template) is added to the Manage CoS Profiles page for routers and EX Series switches, and another with the same name is added for Campus Switching ELS. Default CoS profiles have most basic settings preconfigured. For example, the forwarding classes in the default CoS profile have already been assigned with default scheduler values. However, you can use the Edit CoS Profile page to optimize your communication with the network by customizing the bandwidth and buffer size assigned to each of the forwarding classes in the default CoS profile.

Using the Default CoS Profiles for Campus Switching ELS with Hierarchical Port Scheduling

When you install Connectivity Services Director, juniper_CS_Hier_Ethernet_CoS is the default CoS profiles that is installed for Campus Switching ELS with Hierarchical Port Scheduling.

To see the settings configured for a default profile, select it on the Manage CoS Profiles page, then click **Details**.

Using the Default CoS Profiles for Data Center Switching

When you install Connectivity Services Director, the following default CoS profiles are installed for Data Center Switching:

- juniper_DC_NonHier_Ethernet_CoS
- juniper_DC_Hier_Ethernet_CoS
- juniper_DC_NonHier_CoS
- juniper_DC_Hier_CoS
- juniper_DC_Hier_FCoE_CoS


To see the settings configured for a default profile, select it on the Manage CoS Profiles page, then click **Details**.

Creating a Wired CoS Profile

In Connectivity Services Director, you can create a CoS profile to group a set of Class of Service parameters and apply it to one or more network sessions.

For a CoS profile, you must specify the profile name. You can use defaults for the other values.

To create a wired CoS profile:

1. Click  in the Connectivity Services Director banner.
2. Under Select View, select one of the following: **Device View** or **Custom Group View**.



TIP: Do not select **Dashboard View** or **Topology View**.

3. From the Tasks pane, expand **Wired**, expand **Profiles**, and then select **CoS**.
4. Click **Add** to add a new profile.
Connectivity Services Director opens the Device Family Chooser window.
5. From the Device Family Chooser, select the wired device family for which you want to create a profile. The available device families are **Switching (EX)**, **Campus Switching ELS > Non-Hierarchical Port Scheduling**, **Campus Switching ELS > Hierarchical Port Scheduling**, and **Data Center Switching**.
6. Click OK.
7. Complete the appropriate settings using the steps mentioned in [“Specifying Settings for a Routing, Switching, and Campus Switching ELS CoS Profile”](#) on page 228, [“Specifying Settings for a Campus Switching ELS CoS Profile with Hierarchical Port Scheduling \(ETS\)”](#) on page 232, or [“Specifying Settings for a Data Center Switching CoS Profile”](#) on page 236.

Specifying Settings for a Routing, Switching, and Campus Switching ELS CoS Profile

Create a CoS profile for switching by providing a profile name and, optionally, changing any default settings for Traffic Configuration and Shaping.

1. Enter the CoS switching settings described in [Table 37 on page 228](#). Required settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 37: CoS Profile Settings for Routers, EX and Campus Switching ELS

Field	Action
Profile Name	Type the name of the profile. You can use up to 64 characters for profiles created for wired devices. Profile name must not contain special characters or spaces. Note that profiles that are automatically created by Connectivity Services Director as part of device discovery or out-of-band changes may contain the underscore (_) character.
Description	Type a description of the profile.

2. Connectivity Services Director includes four predefined traffic types, Data, Voice, Video, and Network Control. You can either modify those traffic types or you can create your own traffic type. Modify and customize any listed traffic type by selecting the traffic type from the list and clicking **Edit**, then changing any of the settings described in [Table 38 on page 228](#).
3. To create your own traffic type, click **Add** and then configure the settings described in [Table 38 on page 228](#).

Table 38: Traffic Configuration and Shaping for EX Switching and Campus Switching ELS

Field	Description
Traffic Type	If you are editing a Connectivity Services Director default traffic type, this field cannot be changed. If you are adding a traffic type, indicate the type of traffic—this can be any value, such as a server name or something to do with your business.

Table 38: Traffic Configuration and Shaping for EX Switching and Campus Switching ELS (continued)

Field	Description
Forwarding Name	<p>If you are editing a Connectivity Services Director default traffic type, this field cannot be changed. If you are adding a traffic type, you can use one of the predefined forwarding classes for your switch or you can create your own forwarding class. These forwarding classes are always provided: nd_best-effort, nd_network-control, nd_video-forwarding, and nd_expedited-forwarding. To create your own forwarding class, type a name instead of selecting an option.</p> <p>Most switches support the four predefined forwarding classes listed above. The exception is the EX4300 switch, which has eight default forwarding classes, including the standard four classes, plus multicast-network-connect, multicast-assured-forwarding, multicast-expedited-forwarding, and multicast-network-connect.</p>
Forwarding Queue	<p>Existing forwarding classes already have associated queues that cannot be altered. If you defined a new forwarding class by specifying your own Forwarding Name, then select an internal queue number to which forwarding classes are assigned. Most switches support queues 0 - 10. The exception is the EX4300 switch, which supports queues 0 - 11.</p> <p>By default, if a packet is not classified, it is assigned to the class associated with queue 0. You can assign more than one forwarding class to a queue number.</p>

Scheduler Map

A note in the Scheduler Map section indicates how much buffer size and bandwidth you have available to configure. For example, the message "You have been left with 0 percent buffer size and 0 percent bandwidth." means that you have no available buffer or bandwidth, and you must reconfigure existing traffic types to free some bandwidth before configuring additional traffic types.

Low Priority	Enable Low Priority if you want the queue to receive low priority.
Strict High Priority	<p>Enable Strict High Priority if you want the queue to receive preferential treatment over a low-priority queue. Unlimited bandwidth is assigned to a strict-high priority queue.</p> <p>A strict-high priority queue receives preferential treatment over a low-priority queue. Unlimited bandwidth is assigned to a strict-high priority queue. Queues are scheduled according to the queue number, starting with the highest queue, 7, with decreasing priority down through queue 0. Traffic in higher-numbered queues is always scheduled prior to traffic in lower-numbered queues. In other words, in case of two high-priority queues, the queue with the higher queue number is processed first.</p> <p>NOTE: You can modify this field in the Traffic Configuration and Shaping table or from the Traffic Configuration and Shaping window.</p>

Table 38: Traffic Configuration and Shaping for EX Switching and Campus Switching ELS (continued)

Field	Description
Buffer Size (%)	<p>Buffer Size (%) is the size of the memory buffer allocated for storing packets. Use the slider to specify the scheduler Buffer Size percentage.</p> <p>NOTE: You can modify this value by double-clicking this field in the Traffic Configuration and Shaping table or by sliding the bar in the Traffic Configuration and Shaping window.</p>
Bandwidth Reserved (%)	<p>Bandwidth Reserved (%) is the amount of interface bandwidth assigned to the queue. Move the slider to specify the Bandwidth Reserved percentage. Defaults are:</p> <ul style="list-style-type: none"> • Data: 30% • Voice: Strict High • Video: 70% • Network control: 0% <p>If Strict-High is enabled for this traffic type, you cannot reserve bandwidth.</p> <p>NOTE: This field displays the value based on either your input or on the transmit-rate parameter from the switch, if that parameter is configured. While specifying transmit-rate on the EX Series switch, if you choose to specify the value as an exact rate, Connectivity Services Director converts this value and displays it as a percentage in the Bandwidth Reserved (%) field. You can modify this percentage value from the CoS Profile page.</p>
Shaping Rate	<p>Move the Shaping Rate slider to throttle the rate of packet transmission by setting a maximum bandwidth (rate in bits per second) or a maximum percentage of bandwidth for a queue or a forwarding class.</p>
Traffic Classification Behavior aggregate classification classifies packets. The DSCP or DSCP IPv6 precedence bits of the IP header convey the behavior aggregate class information. The information might also be found in the IEEE 802.1ad, or IEEE 802.1p CoS bits.	
Classifier Type	<p>Select a classifier type—DSCP, DSCP-IPv6, INET-precedence, or IEEE-802.1—and associate the corresponding code-point aliases to loss priorities.</p> <p>NOTE: You can specify code-point—loss priority associations for one or more classifier types.</p> <ul style="list-style-type: none"> • DSCP—Differentiated services code point, a field in IPv4 headers, is used to classify traffic. • DSCP-IPv6—Differentiated services code point, a field in IPv6 headers, is used to classify traffic. • INET precedence—Field that indicates class of service rewrite rules are used to classify traffic. • IEEE-802.1—IEEE 802.1ad, or IEEE 802.1p CoS bits are used to classify traffic.

Table 38: Traffic Configuration and Shaping for EX Switching and Campus Switching ELS (continued)

Field	Description
Classifier Code Points	
Code Points	<p>The code points list includes all available and unselected code points for the selected classifier type.</p> <p>Specify one or more code-point aliases or bit sets to associate with a forwarding class by moving the value to one of the two lists, Loss Priority Low or Loss Priority High.</p>
Loss Priority Low	Indicate that packets have low loss priority by selecting code-point aliases from the Code Points table and using the LEFT and RIGHT arrows to move them into the appropriate loss priority table.
Loss Priority Medium-Low	Indicate that packets have medium-low loss priority by selecting code-point aliases from the Code Points table and using the LEFT and RIGHT arrows to move them into the appropriate loss priority table.
Loss Priority Medium-High	Indicate that packets have medium-high loss priority by selecting code-point aliases from the Code Points table and using the LEFT and RIGHT arrows to move them into the appropriate loss priority table.
Loss Priority High	Indicate that packets have high loss priority by selecting code-point aliases from the Code Points table and using the LEFT and RIGHT arrows to move them into the appropriate loss priority table.

- Click **OK** to close the Add Traffic and Classification window and save your configuration.

Your changes are added to this CoS profile.



NOTE: If all bandwidth has already been reserved, your changes are not made. Reduce the bandwidth reserved from another Traffic Type, then repeat the configuration.

- To configure rewrite rules for a forwarding queue, click **Configure Rewrite Rules** at the bottom of the screen. The Configure Rewrite Rules window appears. Specify rewrite rule settings as described below to alter CoS values in outgoing packets on the outbound interfaces of an edge switch:
 - Select the forwarding class for which you want to create or modify rewrite rules. Connectivity Services Director lists all the forwarding classes that you have used for configuring traffic in the Traffic Configuration and Shaping section.

- b. For each classifier's loss priority, select a code-point alias for each loss-priority type—Low, Medium-Low, Medium-High, and High.
6. Click **OK** to save the rewrite rules and close the Configure Rewrite Rules window.
The system saves the rewrite rules and returns to the **Create CoS Profile** page.
7. Click **Done**.

After you create a CoS profile for switching devices, associate the CoS profile with a Port profile. For directions, see *Creating and Managing Port Profiles*.

Specifying Settings for a Campus Switching ELS CoS Profile with Hierarchical Port Scheduling (ETS)

You can create a CoS profile for Campus Switching ELS with Hierarchical Post Scheduling by specifying the profile settings and the traffic configuration and shaping details. Hierarchical port scheduling is a two-tier process that provides better port bandwidth utilization and greater flexibility to allocate resources to queues and to groups of queues. Hierarchical scheduling includes the Junos OS implementation of enhanced transmission selection (ETS, described in IEEE 802.1Qaz).

When you open the Create CoS Profile page, Connectivity Services Director displays two predefined priority groups—`data_video_pg` and `voice_control_pg`—with default forwarding classes grouped under each of them. You can modify these priority groups or forwarding classes according to your network requirements.

To specify the settings for the CoS profile:

1. Enter the settings described in [Table 39 on page 232](#). Required settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 39: CoS Profile Basic Settings for Campus Switching ELS CoS Profile with Hierarchical Port Scheduling (ETS)

Field	Action
Profile Name	Type the name of the profile. You can use up to 64 characters for profiles created for wired devices. Profile name must not contain special characters or spaces. Note that profiles that are automatically created by Connectivity Services Director as part of device discovery or out-of-band changes may contain the underscore (_) character.
Description	Type the description of the profile.

2. Specify settings in the Priority Group and Traffic Settings section.

The table lists priority groups and the forwarding classes they contain in an expandable list. Priority groups refer to forwarding class sets in the device. You can perform these tasks on priority groups and forwarding classes:

- To add a new priority group, click **Add Priority Group**. The Add Priority Group and Traffic Control Profile Window opens. Enter the settings as described in [Table 40 on page 233](#).

Table 40: Add Priority Group and Traffic Control Profile Window

Field	Description
Priority Group Name	Enter a name for the priority group.
Traffic Control Profile Settings	
Transmit Rate (%)	Select a transmit rate percentage for the priority group.
Shaping Rate (%)	Select a shaping rate percentage for the priority group.

- To edit a priority group or forwarding class's properties, click the field that you want to edit in the table. The properties that can be edited are described in [Table 41 on page 233](#).

Table 41: Priority Group and Traffic Settings Table Properties

Field	Description
No Loss	Select to make the forwarding class lossless. Not applicable to priority groups.
Strict High	Select to cause the forwarding class to receive preferential treatment over a low-priority queue. Unlimited bandwidth is assigned to a strict-high priority queue. Not applicable to priority groups.
Transmit Rate (%)	Select the percentage of interface bandwidth assigned to the forwarding class or priority group. If you have enabled Strict-High , you cannot reserve bandwidth for this traffic type.
Shaping Rate (%)	Select a shaping rate percentage for the forwarding class or priority group.
Buffer Size (%)	Select the percentage of the memory buffer allocated for storing packets for the forwarding class. Not applicable to priority groups.

- To edit a forwarding class's properties, click its name. The Edit Traffic Classification and Shaping for priority group window opens. Enter the settings as described in [Table 42 on page 233](#).

Table 42: Edit and Add Traffic Classification and Shaping for Priority Group Window

Field	Description
Forwarding Class Name	Select or specify a name for the forwarding class.
Forwarding Class Queue	Specify the internal queue numbers to which forwarding classes are assigned.

Table 42: Edit and Add Traffic Classification and Shaping for Priority Group Window (continued)

Field	Description
No Loss	Select to make the forwarding class lossless.
Scheduler Map	
Strict High	Select if you want the queue to receive preferential treatment over a low-priority queue. Unlimited bandwidth is assigned to a strict-high priority queue.
Transmit Rate	Select the percentage of interface bandwidth assigned to the forwarding class. If you have enabled Strict-High , you cannot reserve bandwidth for this traffic type.
Shaping Rate	Select a shaping rate percentage for the forwarding class.
Buffer Size (%)	Select the percentage of the memory buffer allocated for storing packets for the forwarding class.
Traffic Classification	
Classifier Type	Select the classifier type that maps packets to a forwarding class and a loss priority.
Code Points	Specify one or more code-points for associating with a forwarding class.
Loss Priority Low	Indicates that packets have low loss priority. Select code points from the Code Points table and use the LEFT and RIGHT arrows to move them into the appropriate loss priority table.
Loss Priority Medium High	Indicates that packets have medium high loss priority. Select code points from the Code Points table and use the LEFT and RIGHT arrows to move them into the appropriate loss priority table.
Loss Priority High	Indicates that packets have high loss priority. Select code points from the Code Points table and use the LEFT and RIGHT arrows to move them into the appropriate loss priority table.

- To add a forwarding class to a priority group, click the **Add Forwarding Class** link at the end of the priority group's list of forwarding classes. The Add Traffic Classification and Shaping for priority group window opens. Enter the settings as described in [Table 42 on page 233](#).
 - To remove a priority group or forwarding class, click the X at the end of its table row.
3. Specify priority-based flow control (PFC) settings in the PFC Settings section. Enter the settings as described in [Table 43 on page 234](#).

Table 43: PFC Settings for Campus Switching ELS CoS Profile with Hierarchical Port Scheduling (ETS)

Field	Description
Input Cable Length (meter)	Enter the length of the cable attached to the input interface, in meters.
Input	

Table 43: PFC Settings for Campus Switching ELS CoS Profile with Hierarchical Port Scheduling (ETS) (continued)

Field	Description
Add	Click to add an input congestion notification profile (CNP). A new entry appears in the table.
Remove	Click to remove the selected input CNP.
IEEE Code Point	Select the IEEE code point for the input CNP.
Maximum Receive Size (bytes)	Enter the maximum receive unit (MRU) on an interface for traffic that matches the PFC priority, in bytes.
Output	
Add	Click to add an output CNP. A new entry appears in the table.
Remove	Click to remove the selected output CNP.
IEEE Code Point	Select the IEEE code point for the output CNP.
Queue List	Select output queues on which to enable flow control (PFC pause).

- Specify rewrite rule settings in the Rewrite Rule Settings section. Enter the settings as described in [Table 44 on page 235](#).

Table 44: Rewrite Rule Settings for Campus Switching ELS CoS Profile with Hierarchical Port Scheduling (ETS)

Field	Description
Forwarding Name	The name of the forwarding class.
Queue	The number corresponding to the forwarding queue. You cannot modify this field.
Rewrite Type	Select a rewrite-rules mapping for the traffic that passes through the various queues on the interface.
Egress Code Point - Loss Priority Low	Specify a code-point for association with a forwarding class for loss priority low.
Egress Code Point - Loss Priority Medium High	Specify a code-point for association with a forwarding class for loss priority medium high.
Egress Code Point - Loss Priority High	Specify a code-point for association with a forwarding class for loss priority high.

- Click **Done** to save the changes to the profile.

Specifying Settings for a Data Center Switching CoS Profile

You can create a CoS profile by specifying the profile settings and the traffic configuration and shaping details.

To specify the settings for the CoS profile:

1. Enter the settings described in [Table 45 on page 236](#). Required settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 45: CoS Profile Basic Settings for Data Center Switching

Field	Action
Profile Name	Type the name of the profile. You can use up to 64 characters for profiles created for wired devices. Profile name must not contain special characters or spaces. Note that profiles that are automatically created by Connectivity Services Director as part of device discovery or out-of-band changes may contain the underscore (_) character.
Description	Type the description of the profile.

2. In the Traffic Classification and Shaping Settings section, select one of these options:
 - **Hierarchical Port Scheduling (ETS)**—Hierarchical port scheduling (Enhanced Transmission Selection, or ETS) is a two-tier process that provides better port bandwidth utilization and greater flexibility to allocate resources to queues and to groups of queues (for QFX and QFabric devices).
 - **Non Hierarchical Port Scheduling**—Non-hierarchical scheduling is a one-tier process that provides port bandwidth utilization and allocates resources to queues (for EX4500 and EX4550 transit switches).
3. If you selected Hierarchical Port Scheduling (ETS), specify settings in the Priority Group and Traffic Settings section.

The table lists priority groups and the forwarding classes they contain in an expandable list. Priority groups refer to forwarding class sets in the device. You can perform these tasks on priority groups and forwarding classes:

- To add a new priority group, click **Add Priority Group**. The Add Priority Group and Traffic Control Profile Window opens. Enter the settings as described in [Table 46 on page 237](#).

Table 46: Add Priority Group and Traffic Control Profile Window

Field	Description
Priority Group Name	Enter a name for the priority group.
Traffic Control Profile Settings	
Transmit Rate (%)	Select a transmit rate percentage for the priority group.
Shaping Rate (%)	Select a shaping rate percentage for the priority group.

- To edit a priority group or forwarding class's properties, click the field that you want to edit in the table. The properties that can be edited are described in [Table 47 on page 237](#).

Table 47: Priority Group and Traffic Settings Table Properties

Field	Description
No Loss	Select to make the forwarding class lossless. Not applicable to priority groups.
Strict High	Select to cause the forwarding class to receive preferential treatment over a low-priority queue. Unlimited bandwidth is assigned to a strict-high priority queue. Not applicable to priority groups.
Transmit Rate (%)	Select the percentage of interface bandwidth assigned to the forwarding class or priority group. If you have enabled Strict-High , you cannot reserve bandwidth for this traffic type.
Shaping Rate (%)	Select a shaping rate percentage for the forwarding class or priority group.
Buffer Size (%)	Select the percentage of the memory buffer allocated for storing packets for the forwarding class. Not applicable to priority groups.

- To edit a forwarding class's properties, click its name. The Edit Traffic Classification and Shaping for priority group window opens. Enter the settings as described in [Table 48 on page 237](#).

Table 48: Edit and Add Traffic Classification and Shaping for Priority Group Window

Field	Description
Forwarding Class Name	Select or specify a name for the forwarding class.
Forwarding Class Queue	Specify the internal queue numbers to which forwarding classes are assigned.
No Loss	Select to make the forwarding class lossless.
Scheduler Map	

Table 48: Edit and Add Traffic Classification and Shaping for Priority Group Window (continued)

Field	Description
Strict High	Select if you want the queue to receive preferential treatment over a low-priority queue. Unlimited bandwidth is assigned to a strict-high priority queue.
Transmit Rate	Select the percentage of interface bandwidth assigned to the forwarding class. If you have enabled Strict-High , you cannot reserve bandwidth for this traffic type.
Shaping Rate	Select a shaping rate percentage for the forwarding class.
Buffer Size (%)	Select the percentage of the memory buffer allocated for storing packets for the forwarding class.
Traffic Classification	
Classifier Type	Select the classifier type that maps packets to a forwarding class and a loss priority.
Code Points	Specify one or more code-points for associating with a forwarding class.
Loss Priority Low	Indicates that packets have low loss priority. Select code points from the Code Points table and use the LEFT and RIGHT arrows to move them into the appropriate loss priority table.
Loss Priority Medium High	Indicates that packets have medium high loss priority. Select code points from the Code Points table and use the LEFT and RIGHT arrows to move them into the appropriate loss priority table.
Loss Priority High	Indicates that packets have high loss priority. Select code points from the Code Points table and use the LEFT and RIGHT arrows to move them into the appropriate loss priority table.

- To add a forwarding class to a priority group, click the **Add Forwarding Class** link at the end of the priority group's list of forwarding classes. The Add Traffic Classification and Shaping for priority group window opens. Enter the settings as described in [Table 48 on page 237](#).
 - To remove a priority group or forwarding class, click the **X** at the end of its table row.
4. If you selected Non Hierarchical Port Scheduling, specify settings in the Traffic Configuration and Shaping table.

The table lists forwarding classes. You can perform these tasks on forwarding classes:

- To add traffic configuration and shaping details for different types of traffic, click **Add** in the Traffic Configuration and Shaping box. The Add Traffic Classification and Shaping window opens.
- To modify the details of an existing traffic configuration, select the traffic configuration from the list and click **Edit**. The Edit Traffic Classification and Shaping window opens.



NOTE: You can modify some of the details in the Traffic Configuration and Shaping table without having to open the Edit Traffic Classification and Shaping window—by clicking on the field that you want to modify.

- To delete a traffic configuration entry, select the traffic configuration from the list and click **Remove**.

The system deletes the selected traffic configuration entry.

To create your own traffic type, click **Add** and then configure the settings described in [Table 49 on page 239](#).

Table 49: Traffic Configuration and Shaping for EX Switching and Campus Switching ELS

Field	Description
Traffic Type	If you are editing a Connectivity Services Director default traffic type, this field cannot be changed. If you are adding a traffic type, indicate the type of traffic—this can be any value, such as a server name or something to do with your business.
Forwarding Name	<p>If you are editing a Connectivity Services Director default traffic type, this field cannot be changed. If you are adding a traffic type, you can use one of the predefined forwarding classes for your switch or you can create your own forwarding class. These forwarding classes are always provided: nd_best-effort, nd_network-control, nd_video-forwarding, and nd_expedited-forwarding. To create your own forwarding class, type a name instead of selecting an option.</p> <p>Most switches support the four predefined forwarding classes listed above. The exception is the EX4300 switch, which has eight default forwarding classes, including the standard four classes, plus multicast-network-connect, multicast-assured-forwarding, multicast-expedited-forwarding, and multicast-network-connect.</p>
Forwarding Queue	<p>Existing forwarding classes already have associated queues that cannot be altered. If you defined a new forwarding class by specifying your own Forwarding Name, then select an internal queue number to which forwarding classes are assigned. Most switches support queues 0 - 10. The exception is the EX4300 switch, which supports queues 0 - 11.</p> <p>By default, if a packet is not classified, it is assigned to the class associated with queue 0. You can assign more than one forwarding class to a queue number.</p>
Scheduler Map <p>A note in the Scheduler Map section indicates how much buffer size and bandwidth you have available to configure. For example, the message “You have been left with 0 percent buffer size and 0 percent bandwidth.” means that you have no available buffer or bandwidth, and you must reconfigure existing traffic types to free some bandwidth before configuring additional traffic types.</p>	
Low Priority	Enable Low Priority if you want the queue to receive low priority.

Table 49: Traffic Configuration and Shaping for EX Switching and Campus Switching ELS (continued)

Field	Description
Strict High Priority	<p>Enable Strict High Priority if you want the queue to receive preferential treatment over a low-priority queue. Unlimited bandwidth is assigned to a strict-high priority queue.</p> <p>A strict-high priority queue receives preferential treatment over a low-priority queue. Unlimited bandwidth is assigned to a strict-high priority queue. Queues are scheduled according to the queue number, starting with the highest queue, 7, with decreasing priority down through queue 0. Traffic in higher-numbered queues is always scheduled prior to traffic in lower-numbered queues. In other words, in case of two high-priority queues, the queue with the higher queue number is processed first.</p> <p>NOTE: You can modify this field in the Traffic Configuration and Shaping table or from the Traffic Configuration and Shaping window.</p>
Buffer Size (%)	<p>Buffer Size (%) is the size of the memory buffer allocated for storing packets. Use the slider to specify the scheduler Buffer Size percentage.</p> <p>NOTE: You can modify this value by double-clicking this field in the Traffic Configuration and Shaping table or by sliding the bar in the Traffic Configuration and Shaping window.</p>
Bandwidth Reserved (%)	<p>Bandwidth Reserved (%) is the amount of interface bandwidth assigned to the queue. Move the slider to specify the Bandwidth Reserved percentage. Defaults are:</p> <ul style="list-style-type: none"> • Data: 30% • Voice: Strict High • Video: 70% • Network control: 0% <p>If Strict-High is enabled for this traffic type, you cannot reserve bandwidth.</p> <p>NOTE: This field displays the value based on either your input or on the transmit-rate parameter from the switch, if that parameter is configured. While specifying transmit-rate on the EX Series switch, if you choose to specify the value as an exact rate, Connectivity Services Director converts this value and displays it as a percentage in the Bandwidth Reserved (%) field. You can modify this percentage value from the CoS Profile page.</p>
Shaping Rate	<p>Move the Shaping Rate slider to throttle the rate of packet transmission by setting a maximum bandwidth (rate in bits per second) or a maximum percentage of bandwidth for a queue or a forwarding class.</p>
<p>Traffic Classification</p> <p>Behavior aggregate classification classifies packets. The DSCP or DSCP IPv6 precedence bits of the IP header convey the behavior aggregate class information. The information might also be found in the IEEE 802.1ad, or IEEE 802.1p CoS bits.</p>	

Table 49: Traffic Configuration and Shaping for EX Switching and Campus Switching ELS (continued)

Field	Description
Classifier Type	<p>Select a classifier type—DSCP, DSCP-IPv6, INET-precedence, or IEEE-802.1—and associate the corresponding code-point aliases to loss priorities.</p> <p>NOTE: You can specify code-point—loss priority associations for one or more classifier types.</p> <ul style="list-style-type: none"> DSCP—Differentiated services code point, a field in IPv4 headers, is used to classify traffic. DSCP-IPv6—Differentiated services code point, a field in IPv6 headers, is used to classify traffic. INET precedence—Field that indicates class of service rewrite rules are used to classify traffic. IEEE-802.1—IEEE 802.1ad, or IEEE 802.1p CoS bits are used to classify traffic.
Classifier Code Points	
Code Points	<p>The code points list includes all available and unselected code points for the selected classifier type.</p> <p>Specify one or more code-point aliases or bit sets to associate with a forwarding class by moving the value to one of the two lists, Loss Priority Low or Loss Priority High.</p>
Loss Priority Low	Indicate that packets have low loss priority by selecting code-point aliases from the Code Points table and using the LEFT and RIGHT arrows to move them into the appropriate loss priority table.
Loss Priority Medium-Low	Indicate that packets have medium-low loss priority by selecting code-point aliases from the Code Points table and using the LEFT and RIGHT arrows to move them into the appropriate loss priority table.
Loss Priority Medium-High	Indicate that packets have medium-high loss priority by selecting code-point aliases from the Code Points table and using the LEFT and RIGHT arrows to move them into the appropriate loss priority table.
Loss Priority High	Indicate that packets have high loss priority by selecting code-point aliases from the Code Points table and using the LEFT and RIGHT arrows to move them into the appropriate loss priority table.

- If you selected Hierarchical Port Scheduling (ETS), specify priority-based flow control (PFC) settings in the PFC Settings section. Enter the settings as described in [Table 50 on page 242](#).

Table 50: PFC Settings for Data Center Switching Hierarchical Port Scheduling (ETS) CoS Profile

Field	Description
Input Cable Length (meter)	Enter the length of the cable attached to the input interface, in meters.
Input	
Add	Click to add an input congestion notification profile (CNP). A new entry appears in the table.
Remove	Click to remove the selected input CNP.
IEEE Code Point	Select the IEEE code point for the input CNP.
Maximum Receive Size (bytes)	Enter the maximum receive unit (MRU) on an interface for traffic that matches the PFC priority, in bytes.
Output	
Add	Click to add an output CNP. A new entry appears in the table.
Remove	Click to remove the selected output CNP.
IEEE Code Point	Select the IEEE code point for the output CNP.
Queue List	Select output queues on which to enable flow control (PFC pause).

6. If you selected Non-Hierarchical Port Scheduling, specify priority-based flow control (PFC) settings in the PFC Settings section. Enter the settings as described in [Table 51 on page 242](#).

Table 51: PFC Settings for Data Center Switching Non-Hierarchical Port Scheduling CoS Profile

Field	Description
Input	
Add	Click to add an input congestion notification profile (CNP). A new entry appears in the table.
Remove	Click to remove the selected input CNP.

7. If you selected Hierarchical Port Scheduling (ETS), specify rewrite rule settings in the Rewrite Rule Settings section as described in [Table 52 on page 242](#).

Table 52: Rewrite Rule Settings for Data Center Switching CoS Profile

Field	Description
Forwarding Name	The name of the forwarding class.

Table 52: Rewrite Rule Settings for Data Center Switching CoS Profile (continued)

Field	Description
Queue	The number corresponding to the forwarding queue. You cannot modify this field.
Rewrite Type	Select a rewrite-rules mapping for the traffic that passes through the various queues on the interface.
Egress Code Point - Loss Priority Low	Specify a code-point for association with a forwarding class for loss priority low.
Egress Code Point - Loss Priority Medium High	Specify a code-point for association with a forwarding class for loss priority medium high.
Egress Code Point - Loss Priority High	Specify a code-point for association with a forwarding class for loss priority high.

8. If you selected Non-Hierarchical Port Scheduling, click **Configure Rewrite Rules** at the bottom of the screen to configure rewrite rules for a forwarding queue. The Configure Rewrite Rules window appears. Specify rewrite rule settings as described below to alter CoS values in outgoing packets on the outbound interfaces of an edge switch:
 - a. Select the forwarding class for which you want to create or modify rewrite rules. Connectivity Services Director lists all the forwarding classes that you have used for configuring traffic in the Traffic Configuration and Shaping section.
 - b. For each classifier's loss priority, select a code-point alias for each loss-priority type—Low, Medium-Low, Medium-High, and High.
9. Click **Done** to save the changes to the profile.

What to Do Next

After you have created a CoS profile for switching devices, you can associate the CoS profile to a Port profile.

Related Documentation

- [Understanding Class of Service \(CoS\) Profiles on page 219](#)

Configuring Link Aggregation Groups (LAGs)

- [Understanding Link Aggregation on page 245](#)
- [Managing and Creating a Link Aggregation Group on page 245](#)

Understanding Link Aggregation

You can combine multiple physical Ethernet ports to form a logical point-to-point link, known as a link aggregation group (LAG) or bundle. A LAG provides more bandwidth than a single Ethernet link can provide. Additionally, link aggregation provides network redundancy by load-balancing traffic across all available links. If one of the links fails, the system automatically load-balances traffic across all remaining links. In a Virtual Chassis, LAGs can be used to load-balance network traffic between member routers.

The maximum number of interfaces that can be grouped into a LAG and the maximum number of LAGs supported on a router varies according to the router model and the version of and the version of Juniper Networks Junos operating system (Junos OS) that is running on that router.

Managing and Creating a Link Aggregation Group

IEEE 802.3ad link aggregation enables you to group Ethernet interfaces to form a single link layer interface, also known as a link aggregation group (LAG) or bundle.

Aggregating multiple links between physical interfaces creates a single logical point-to-point trunk link or a LAG. Link Aggregation Control Protocol (LACP), a component of IEEE 802.3ad, provides additional functionality for LAGs.

LACP ensures that both ends of the Ethernet link are functional and are members of the aggregation group before the link is added to the LAG. If you use LACP, make sure that LACP is enabled at both the local and remote ends of the link. When LACP is configured, it detects misconfigurations on the local end or the remote end of the link. Thus, LACP can help to prevent communication failure. When LACP is not enabled, a local LAG might attempt to transmit packets to a remote single interface, which causes the communication to fail. However, when LACP is enabled, a local LAG cannot transmit packets unless a LAG with LACP is also configured on the remote end of the link.

The maximum number of interfaces that can be grouped into a LAG and the maximum number of LAGs supported on a router varies according to the router model and the version of Juniper Networks Junos operating system (Junos OS) that is running on that router. Be aware of the maximum number of interfaces per LAG and the maximum number of LAGs that are supported on your routers by referring to your device specific documentation before implementing LAG in your network.



NOTE: You only see the Manage Lag option under Device Management when a qualified router is selected in the View Pane.

When creating LAGs, follow these guidelines:

- You must configure the LAG on both sides of the link.
- You must set the interfaces on either side of the link to the same speed.
- You can configure and apply firewall filters on a LAG.

This topic includes:

- [Link Aggregation Group Options on page 246](#)
- [Creating a Link Aggregation Group on page 247](#)
- [What To Do Next on page 249](#)

Link Aggregation Group Options

From the Manage LAG page, you can:

- Create a new Link Aggregation by clicking **Create**. The Create Link Aggregation window opens—for directions, see [“Creating a Link Aggregation Group” on page 247](#).
- Modify an existing Link Aggregation by selecting it and clicking **Edit**. The Modify Link Aggregation window opens. You can modify all the fields in the Modify Link Aggregation window, except the Interface Name field.
- Delete a Link Aggregation Group by selecting it and clicking **Delete**.

[Table 53 on page 246](#) describes the information provided about the link aggregation configurations on the LACP (Link Aggregation Control Protocol) Configuration page. This page lists all link aggregation groups defined on the selected device.

Table 53: LACP (Link Aggregation Control Protocol) Configuration Fields

Field	Description
Logical Interface Name	Name given to the aggregated interface when the LAG was created.
Member Interfaces	Names of individual member interfaces.

Table 53: LACP (Link Aggregation Control Protocol) Configuration Fields (continued)

Field	Description
LACP Mode	<p>Mode in which LACP packets are exchanged between the interfaces.</p> <p>The possible modes are:</p> <ul style="list-style-type: none"> Active—Indicates that the interface initiates transmission of LACP packets Passive—Indicates that the interface responds only to LACP packets.
Description	<p>The description for the LAG.</p> <p>TIP: If you cannot view the entire description, you can resize the Description column by clicking the column border in the heading and dragging it.</p>
Deployment State	<p>The deployment state of the link aggregation. Deployment state can be:</p> <ul style="list-style-type: none"> Pending Deployment—Indicates that the LAG is not yet deployed on the device. Deployed—Indicates that the LAG is deployed on the device. Pending Removal—Indicates that the LAG is deleted.
Creation Time	Date and time when this profile was created.
Update Time	Date and time when this profile was last modified.
User Name	The username of the user who created or modified the profile.



TIP: All columns might not be displayed. To show or hide fields in the LACP (Link Aggregation Control Protocol) Configuration table, click the DOWN arrow on the field header, select **Columns**, and select or clear the check box adjacent to the field that you want to show or hide.

Creating a Link Aggregation Group

You can create one or more LAGs for your device in Device View. The number of interfaces that can be grouped into a LAG and the total number of LAGs supported on a router varies according to router model.

To create a link aggregation group:

1. In the View pane, select a router for link aggregation.



NOTE: The Manage LAG task is only available when a qualified router is selected in the View pane.

2. Click on the  **Build** tab.

3. Select **Wired > Manage LAG** in the Tasks pane.

The Manage LAG page opens.

4. Click **Create**.

The Create Link Aggregation window opens.

5. Use the up and down arrows to select an AE Name for the aggregation interface. The interface name begins with **ae** followed by an interface number.

6. Select the mode in which LACP packets are to be exchanged between interfaces, either **Active** or **Passive**.

- **Active**—Indicates that the interface initiates transmission of LACP packets
- **Passive**—Indicates that the interface responds only to LACP packets.

7. Enter a description for the link aggregation.

8. Configure up to eight available interfaces on the LAG. Select one or more interfaces from the Available list and then click the **RIGHT** arrow to move them to the Selected list.



NOTE: The Available interfaces list displays only those interfaces that are not part of any link aggregation.

9. Click **OK** to save the link aggregation configuration.

A message confirms that the link aggregation is created successfully and ready to be deployed to a device. If the configuration contains an error, the message instead indicates the error.

10. Click **OK** to close the information message.

The LAG appears in the Manage LAG list.

What To Do Next

The configuration changes that you make in the Build mode are not deployed to devices automatically. After you create a link aggregation group, you must manually deploy the changes to the routers in Deploy mode. For details, see *Deploying Configuration to Devices*.



TIP: Even though link aggregation configuration is not contained within a profile, you can view the link aggregation groups assigned to a router by using the View Assigned Profiles task in Build mode.

- Related Documentation**
- *Understanding Link Aggregation*
 - *Viewing Profiles Assigned to a Device*

CHAPTER 15

Managing Network Devices

- [Viewing the Device Inventory Page in Device View of Connectivity Services Director on page 252](#)
- [Viewing the Physical Inventory of Devices on page 253](#)
- [Viewing Licenses With Connectivity Services Director on page 254](#)
- [Viewing a Device's Current Configuration from Connectivity Services Director on page 255](#)
- [Accessing a Device's CLI from Connectivity Services Director on page 256](#)
- [Accessing a Device's Web-Based Interface from Connectivity Services Director on page 257](#)
- [Deleting Devices on page 258](#)
- [Rebooting Devices on page 258](#)

Viewing the Device Inventory Page in Device View of Connectivity Services Director

The Device Inventory page lists devices managed by Connectivity Services Director and provides basic information about the devices, such as IP address and current operating status. The Device Inventory page is available in Build and Deploy mode and is the default landing page for Build mode.

The scope you have selected in the View pane and the network view that you have selected from the View selector determines which devices are listed in the Device Inventory page. For example:

- If you are in the Device View and select My Network, all devices managed by Connectivity Services Director are listed.

The Device Inventory page provides three pie charts that summarize the status of the devices in your selected scope:

- Devices by Family—Indicates the proportion of devices in each device family.
- Connection State—Shows the proportion of devices that are up or down. In this chart, Virtual Chassis count as one device.
- Configuration State—Shows the proportion of devices in each configuration state. See the Config State entry in [Table 54 on page 252](#) for definitions of the configuration states.

Mouse over a pie segment to view the actual number of devices and the percentage represented by that pie segment.

[Table 54 on page 252](#) describes the fields in the Device Inventory table.

Table 54: Fields in the Device Inventory Table

Field	Description
Hostname	Configured name of the device or IP address if no hostname is configured.
IP Address	IP Address of the device.
Serial Number	Serial number of device chassis.
Platform	Model number of the device.
OS Version	Operating system version running on the device.
Device Family	Device family of the device, such as JUNOS for MX Series routers.
Device Type	Type of the device: <ul style="list-style-type: none"> • ROUTER—ACX Series routers, M Series routers, MX Series routers, and PTX Series routers

Table 54: Fields in the Device Inventory Table (continued)

Field	Description
Connection State	<p>Connection status of the device in Connectivity Services Director:</p> <ul style="list-style-type: none"> • UP—Device is connected to Connectivity Services Director. • DOWN—Device is not connected to Connectivity Services Director. • N/A—Access point state is unavailable to Connectivity Services Director.
Config State	<p>Displays the configuration status of the device:</p> <ul style="list-style-type: none"> • In Sync—The configuration on the device is in sync with the Connectivity Services Director configuration for the device. • Out Of Sync—The configuration on the device does not match the Connectivity Services Director configuration for the device. This state is usually the result of the device configuration being altered outside of Connectivity Services Director. You cannot deploy configuration on a device from Connectivity Services Director when the device is Out Of Sync. To resolve this state, use the Resynchronize Device Configuration task in Deploy mode. • Sync failed—An attempt to resynchronize an Out Of Sync device failed. • Synchronizing—The device configuration is in the process of being resynchronized. • N/A—The device is down or is an access point.
Manageability State	<p>Displays if the device is directly manageable or not.</p> <p>This is a hidden field. To display the Manageability State field, click any column, click the down arrow to expand the list, select Columns from the list, and then enable Manageability State.</p>

Viewing the Physical Inventory of Devices

You can view the physical inventory of all the devices in your network in the Device Physical Inventory page. The Device Physical Inventory page displays information about the slots that are available for a device and provides information about power supplies, chassis cards, fans, part numbers, and so on. Connectivity Services Director displays hardware inventory by device name, based on data retrieved both from the device during discovery and resynchronizing operations, and from the data stored in the hardware catalog. For each managed device, the physical inventory page provides descriptions for field replaceable units (FRUs), part numbers, model numbers, and the pluggable locations from which empty slots are determined.

To view the Device Physical Inventory page, while in the Build mode, select a router from the View pane and select **Device Management > Physical Inventory** from the Tasks pane.

The physical inventory page displays the model number, part number, serial number, and description for the following, depending on the device that you selected:

- For standalone routers, the page displays details of the switch, the chassis, the Flexible PIC Concentrator (FPC), the PIC slot, the PIC installed in the PIC slot, the power supply, the fan tray, and the routing engine.

You can view the following details from the Device Physical Inventory page as described in [Table 55 on page 254](#).

Table 55: Fields in the Device Physical Inventory Table

Field	Description
Item	Name of the device and the components that are part of the device. By default, Connectivity Services Director displays the device and components in an expanded tree structure. You can click a device or component to collapse or expand the sub-components.
Model Number	Model number of the FRU hardware component.
Part Number	Part number of the router chassis component.
Serial Number	The hardware serial number of the device.
Description	The description about the component.

Viewing Licenses With Connectivity Services Director

Juniper Networks devices require a license to operate some features. You can view the licenses for devices connected to Connectivity Services Director.

To view the license for a Juniper Networks device on your network:

1. Select the **Build** icon in the Connectivity Services Director banner.
2. In the View pane, select a device.
3. In the Tasks pane, select **View License Information**.

The Licenses page for that object is displayed with the fields listed in [Table 56 on page 254](#).

Table 56: Viewing Licenses with Connectivity Services Director

Field	Description
Feature Name	Name of the licensed SKU or feature. It can be used to look up the license with Juniper Networks. Not all devices support this.
License Count	Number of times an item has been licensed. This value can have contributions from more than one licensed SKU or feature. Alternatively, it can be 1, no matter how many times it has been licensed.

Table 56: Viewing Licenses with Connectivity Services Director (continued)

Field	Description
Used Count	Number of times the feature is used. For some types of licenses, the license count will be 1, no matter how many times it is used. For capacity-based licensable items, if infringement is supported, the license count can exceed the given count, which has a corresponding effect on the need count.
Need Count	Number of times the feature is used without a license. Not all devices can provide this information.
Given Count	Number of instances of the feature that are provided by default.



NOTE: If a device does not have a license, a blank page is displayed with the message, *No license is installed on this device*. If you are sure the device has a license, try resynchronizing the device before displaying the license again.



NOTE: If you apply a new license to an existing device, you must resynchronize the device before the new license is seen in Connectivity Services Director. For directions, see [“Resynchronizing Device Configuration” on page 778](#).

Viewing a Device's Current Configuration from Connectivity Services Director

You can view a device's current configuration from Connectivity Services Director. This is a convenient way to view device configurations without leaving Connectivity Services Director.

To view a device's current configuration:

1. Click **Build** or **Deploy** in the Connectivity Services Director banner.
2. Select the device in the View pane.
3. Select **Device Management > Show Current Configuration** in the Tasks pane.
4. The device's current configuration displays in the main window.

Accessing a Device's CLI from Connectivity Services Director

Connectivity Services Director enables you to connect to the CLI for devices in your network, using SSH.

This topic describes the steps to connect to a router by using SSH (Secure Shell). SSH is a cryptographic network protocol used for remote shell services or command execution. SSH is one of the many access services that are supported on the Juniper Networks devices. All Juniper Network devices have SSH enabled by default.

To connect to a device by using SSH:

1. Do one of the following:
 - In the View pane, select the device to which you want to connect.
 - In the Topology View, locate the device to which you want to connect.
2. Do one of the following:
 - With the device selected in the View pane, select **Build** mode and select **Tasks > Device Management > SSH to Device**.
 - While in the Topology View, select the device to which you want to launch the SSH connection and click **Device Management > SSH To Device**.

The SSH to Device dialog box appears.

3. Enter the username and password to connect to the selected device and click **Connect**.



NOTE: Ensure that you have removed Pop-Up blockers, if any, before you click **Connect**.

The SSH console to the router or controller opens in a separate browser tab or window depending on your browser settings. Refer to the [MX Series documentation](#) for more information about using the CLI for MX Series routers.



NOTE: Any configuration changes you make to a device, using the CLI qualify as out-of-band changes in Connectivity Services Director. Out-of-band configuration changes can cause the configuration state of a managed device to become out of sync, which indicates that the device configuration no longer matches the Build mode configuration for the device. Use the Resynchronize Device Configuration task in Deploy mode to resynchronize the device configuration.

Accessing a Device's Web-Based Interface from Connectivity Services Director

Connectivity Services Director enables you to connect to the routers in your network, using the device Web-based interface.

This topic describes the steps to connect to a router by using the J-Web interface or to a controller by using Web View. The J-Web interface is a graphical user interface, using which you can monitor, configure, troubleshoot, and manage routers. Web View is a web-based management application that enables you to perform common configuration and management tasks on devices.

You can connect and configure a device by using the J-Web interface or Web View only if the device is configured to accept HTTP or HTTPS as a management service. You can configure HTTP or HTTPS as a management service using the Device Common Settings profile.

To connect to a device using the J-Web interface or Web View:

1. Do one of the following:
 - In the View pane, select the device to which you want to connect.
 - In the Topology view, locate the device to which you want to connect.
2. Do one of the following:
 - While selecting the device in the View pane, select Build mode and select **Tasks** pane > **Device Management** > **Launch Web View**.
 - While in the Topology View, select the device for which you want to launch the Web connection and click **Device Management** > **Launch Web View**.

The Web View or J-Web Login page appears.

3. Enter the username and password to connect to the selected router and click **Login**.

If the credentials that you entered are valid, the system displays the J-Web or Web View home page for the selected device.



NOTE: Any configuration changes you make to a device using the Web interface qualify as out-of-band changes in Connectivity Services Director. Out-of-band configuration changes can cause the configuration state of a managed device to become out of sync, which indicates that the device configuration no longer matches the Build mode configuration for the device. Use the Resynchronize Device Configuration task in Deploy mode to resynchronize the device configuration.

Deleting Devices

You can delete devices that are no longer used from Connectivity Services Director. Deleting a device removes all device configuration and device inventory information from the Junos Space database. Once a device is deleted from the database, all the profiles associations, device configurations, and inventory information of the deleted device are also deleted. However, the system maintains the audit logs and monitoring data for the device even after the device is deleted.

Use the Delete Devices page to delete devices from Connectivity Services Director. While in Build mode, click **Delete Devices** from the **Tasks > Device Management** menu. The Delete Devices page appears.

The Delete Devices page displays the devices contextually depending on your selection in the View pane. For example, if you select a particular switch family in Device View and click Delete Devices, only switches that belong to that switch family are displayed.

To delete devices, complete the following tasks:

1. Select the check box adjacent to the devices that you want to delete.
2. Click **Done**.

Connectivity Services Director prompts you to confirm the deletion. Click **Yes** to confirm the deletion or **No** to go back and make changes to the selection.

Rebooting Devices

Use the Reboot Devices task to immediately reboot the selected device. This task is available in all scopes when in Build mode. To reboot one or more devices immediately:

1. Select the scope in the View pane that contains the devices you want to reboot.
2. Select Reboot Devices from the Tasks pane.
3. Expand the tree on the page as needed to locate the available devices.
4. Select the check box for one or more devices.
5. Click **Done** to start the reboot or click **Cancel** to return to the Device Inventory page.

The rebooting process triggers a Cold Start Alarm that can be seen in Fault mode.

PART 5

Building a Topology View of the Network

- [Downloading and Installing CSD-Topology on page 261](#)
- [Configuring Topology Acquisition and Connectivity Between the CSD-Topology and Path Computation Clients on page 289](#)
- [Accessing the Topology View of CSD-Topology on page 299](#)

CHAPTER 16

Downloading and Installing CSD-Topology

- [CSD-Topology Installation and Configuration Overview on page 261](#)
- [Installation Prerequisites on page 262](#)
- [Installing the CSD-Topology Software Using the RPM Bundle on page 262](#)
- [Minimum Hardware and Software Requirements for Junos VM on VMWare on page 263](#)
- [Installing the JunosVM for CSD-Topology on page 264](#)
- [Connecting an x86 Server to the Network on page 281](#)
- [Interactive Method of Installing the RPM Image and CSD-Topology Software from a USB or DVD Drive on page 286](#)

CSD-Topology Installation and Configuration Overview

Install Juniper Networks CSD-Topology by downloading and installing the CSD-Topology RPM bundle.

For the RPM bundle installation, we recommend that you install CentOS 6.6 or 6.7 with the minimal ISO. If you are using a different version of Linux, contact JTAC to determine whether your Linux version is supported.

After you successfully install the CSD-Topology software on an x86 server, you must establish a connection between the CSD-Topology and the network by configuring Path Computation Element Protocol (PCEP) on each PE router to configure the router as a Path Computation Client (PCC). A PCC supports the configurations related to the Path Computation Element (PCE) and communicates with the CSD-Topology (PCE), which by default is configured to accept a PCEP connection from any source address. After you have established communication between the CSD-Topology and the PCCs, you can configure topology acquisition using BGP-LS. For BGP-LS topology acquisition, you must configure both the CSD-Topology and the PCC routers.

**NOTE:**

We recommend that you use BGP-LS instead of IGP adjacency for topology acquisition for the following reasons:

- The OSPF and IS-IS databases have lifetime timers, which means that if the OSPF or IS-IS neighbor is down, the corresponding database is not removed immediately. CSD-Topology is, therefore, not able to determine whether the topology is valid.
- Using BGP-LS minimizes the risk of making the JunosVM a transit router between AS areas if the GRE metric is not properly configured.
- Typically, CSD-Topology is located in a Network Operations Center (NOC) Data Center, multihops away from the backbone and MPLS TE routers. This is easily accommodated by BGP-LS, but more difficult for IGP protocols because they would have to employ a tunneling mechanism such as GRE to establish adjacency.

Related Documentation

- [Connecting an x86 Server to the Network on page 281](#)

Installation Prerequisites

Before you install CSD-Topology, ensure your system meets the following requirements:

- Recommended minimum hardware requirements:
 - 32 GB RAM
 - 500 GB HDD
- CSD-Topology supports the CentOS 6.x versions only. CentOS 7 is not supported.

Related Documentation

- [Connecting an x86 Server to the Network on page 281](#)

Installing the CSD-Topology Software Using the RPM Bundle

We recommend that you install CentOS 6.6 or 6.7 with the minimal ISO. CentOS can be downloaded from http://mirror.centos.org/centos/6/isos/x86_64. If you are using a different version of Linux, contact JTAC to determine whether your Linux version is supported.

For the hardware requirements that must be met for installing the CSD-Topology software or virtual machine (VM), see [“Installation Prerequisites” on page 262](#).

1. Access the Junos Space Connectivity Services Director software download page:

```
https://www.juniper.net/support/downloads/?p=spacecsd
```

2. Select the Software tab.
3. From the Version drop-down menu, select **2.0**.
4. From under the Application Package heading, download CSD-Topology.
5. Install the RPM bundle.

```
[root@hostname~]# yum localinstall
CSD-Topology-Bundle-2.1.0-20160703_202104_67972_345.x86_64.rpm
[root@hostname~]# cd /opt/csd/csd_topology_bundle/
[root@hostname csd_topology_bundle]# ./install.sh
```

During the installation, you may need to respond to prompts about configuring bridge interfaces. The existing eth0 bridge will need to be migrated to external0 bridge, and the existing eth1 bridge to mgmt0 bridge. If the system Ethernet interface name is not already **eth0**, you must manually create the bridge interface.

The installation process prompts you to enter different credentials to use such as credentials for the Cassandra server. Specifically, the user credentials that are used to access the GUI are also used to validate API users.

You must ensure that the security settings (such as iptables and SELinux) allow the required services and that the underlying networking settings (such as IP addresses and interfaces) are correctly configured. In the context of Connectivity Services Director, access to the following ports is necessary:

- Access to port 8443
- Outbound SSH connections to perform the CLI data collection
- Inbound PCEP connections (TCP port 4189) for networks using PCEP

Related Documentation • [Installation Prerequisites on page 262](#)

Minimum Hardware and Software Requirements for Junos VM on VMWare

Table 57 on page 263 lists the hardware requirements.

Table 57: Minimum Hardware Requirements for VMware

Description	Value
Number of cores	Minimum of 2
Memory	2 GB
Storage	Local or NAS

Table 58 on page 264 lists the software requirements.

Table 58: Software Requirements for VMware

Description	Value
Hypervisor	ESXi 5.5 Update 2
Management Client	vSphere 5.5 or vCenter Server

Installing the JunosVM for CSD-Topology

The CSD-Topology runs Junos in a virtual machine (JunosVM) that uses routing protocols to communicate with the network and dynamically learn the network topology. To provide real-time updates of the network topology, the JunosVM, which is based on a virtual route reflector (VRR), establishes a BGP-link state (LS) peering session with one or more routers from the existing MPLS TE backbone network.

The VRR feature allows you to implement route reflector capability using a general purpose virtual machine that can be run on a 64-bit Intel-based blade server or appliance. Because a route reflector works in the control plane, it can run in a virtualized environment. A virtual route reflector on an Intel-based blade server or appliance works the same as a route reflector on a router, providing a scalable alternative to full mesh internal BGP peering. For more information regarding VRR, see [Understanding Virtual Route Reflector](#)

VRR supports different physical PCI devices such as E1000 and VRRNET3. The procedure in this section is specific to E1000 and VRRNET3 devices.

The JunosVM (VRR) software image is located at <https://www.juniper.net/support/downloads/?p=vrr#sw>.

The IP address of the JunosVM is configurable in the northstar.cfg file. The name of the property is ntad_host and it defaults to 172.16.16.2. In the sample configuration scenario described in this topic, an IP address is assigned to the Ethernet interface, eth1, of the CSD-Topology VM, and an IP address is assigned to the management Ethernet interface, em0, of the JunosVM.



NOTE: The configuration discussed in this section assumes that the JunosVM can be reached at the 172.16.16.2 address. If a different address is used for the connection between the JunosVM and CSD-Topology VM, you must update the /opt/csd-topology/data/northstar.cfg file (the property name is ntad_host=172.16.16.2) to point to the correct address where the JunosVM can be reached.

The interfaces, eth0 and eth2, of the CSD-Topology VM must be connected to the management Ethernet interfaces, em1 and em2, respectively, of the JunosVM or the Hypervisor. The connection between eth0 and em1 is the router-facing link, whereas the connection between eth2 and em2 is the management link.



NOTE: The procedure for installing the JunosVM for CSD-Topology has been validated only for Junos OS Release 14.2R6.

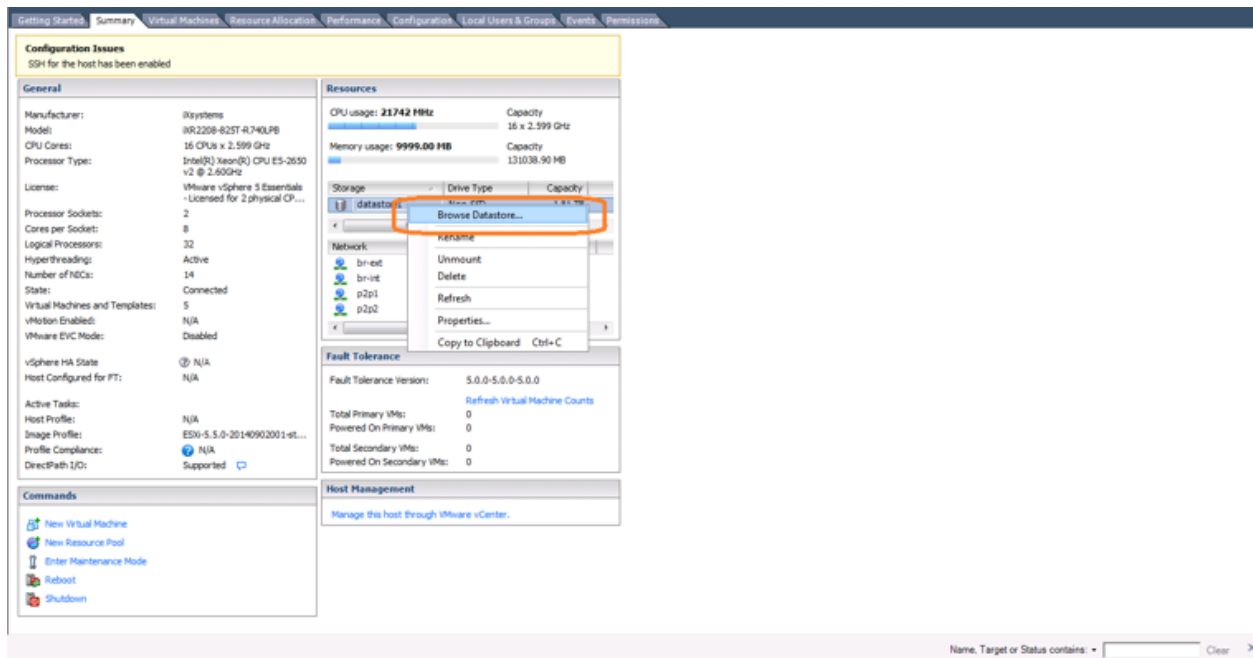
To install VRR with vSphere for E1000 and VRRNET3 adapters and configure the JunosVM (VRR VM) for CSD-Topology, perform these tasks:

- [Setting Up the Datastore on page 265](#)
- [Creating VRR VMs on page 267](#)
- [Configuring the JunosVM on page 275](#)
- [Configuring the CSD-Topology Server with the JunosVM IP Address on page 276](#)
- [Verifying the Connectivity Between the CSD-Topology Server and JunosVM on page 277](#)
- [Verifying That the CSD-Topology Services Are Running on page 277](#)
- [Stopping Firewall on the CSD-Topology Server on page 278](#)
- [Configuring Peer Routers and Topology Acquisition on the JunosVM on page 278](#)
- [Specifying the Topology Details in the Connectivity Services Director GUI on page 280](#)

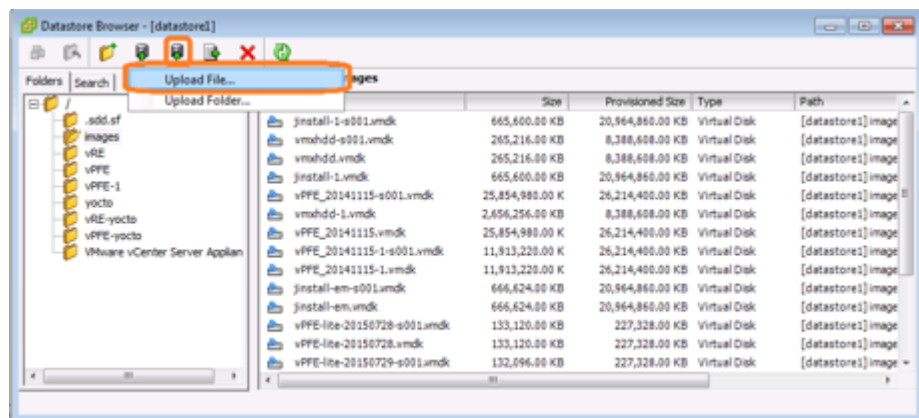
Setting Up the Datastore

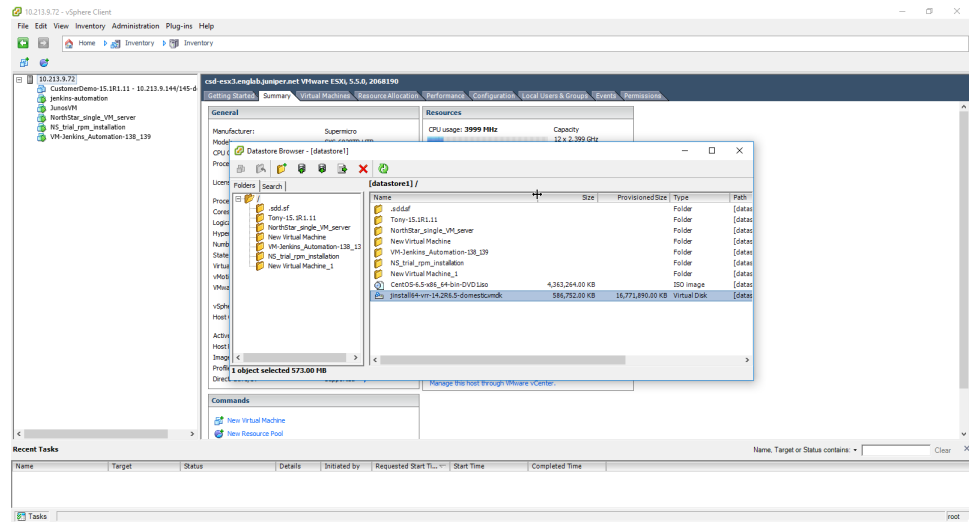
To upload VRR to the ESXi datastore:

1. Download the VRR software package for VMware from the [VRR page](#).
2. Launch the vSphere Web Client for your ESXi server and log in to the server.
3. Click the **Summary** tab, select the datastore under Storage, right-click, and select **Browse Datastore**.



4. In the Datastore Browser, click the **Upload** button, select **Upload File**, and upload the **jinstall64-vrr*.vmdk** files for the package contents



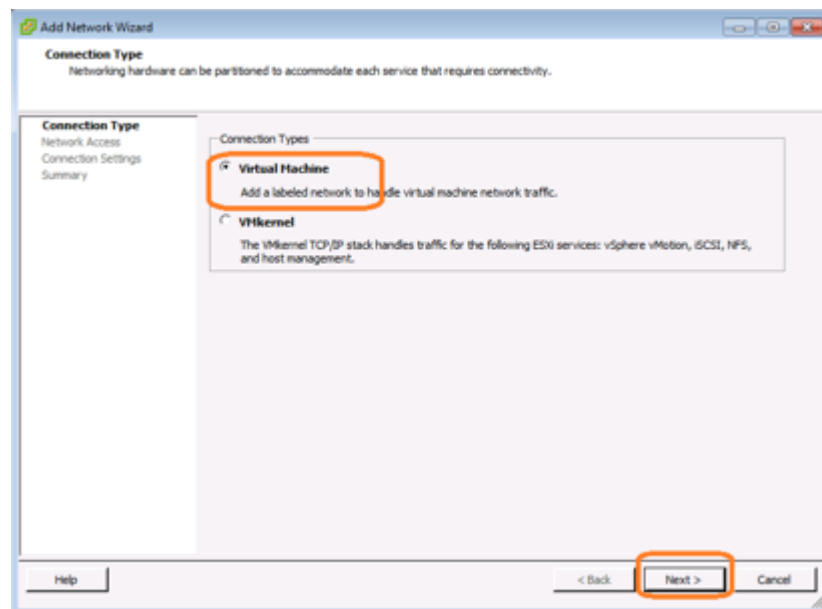


Creating VRR VMs

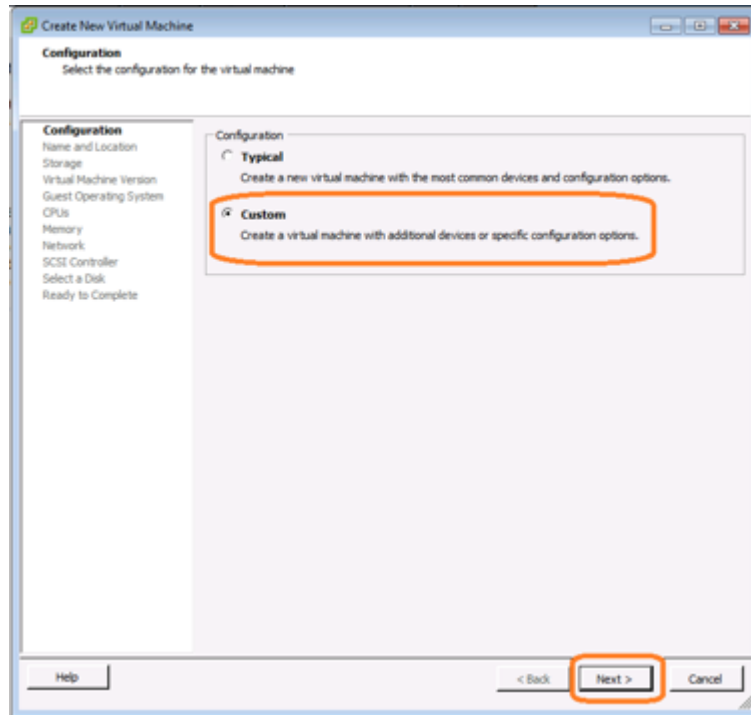
To create a JunosVM or VRR VM:

1. In the left navigation pane, select the ESXi server. In the Getting Started tab, click **Create a new virtual machine**.

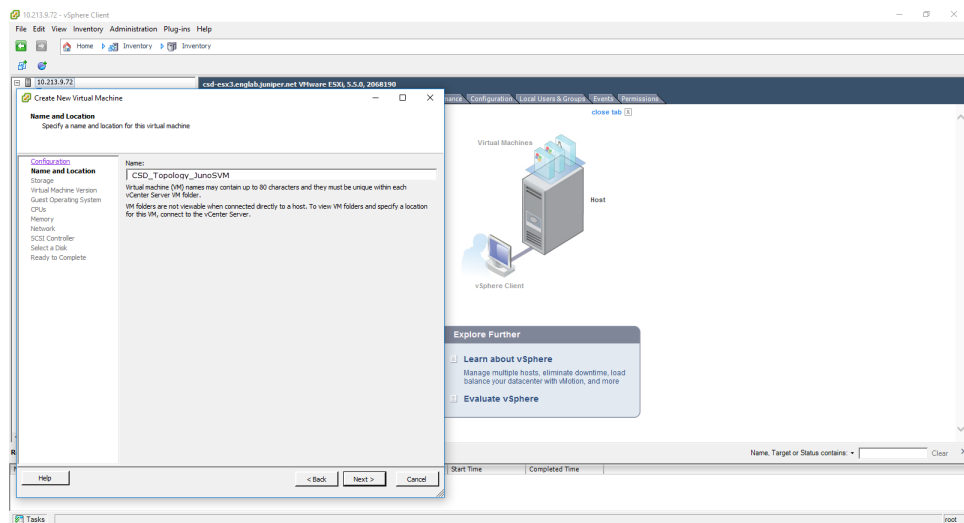
The Create New Virtual Machine wizard appears.



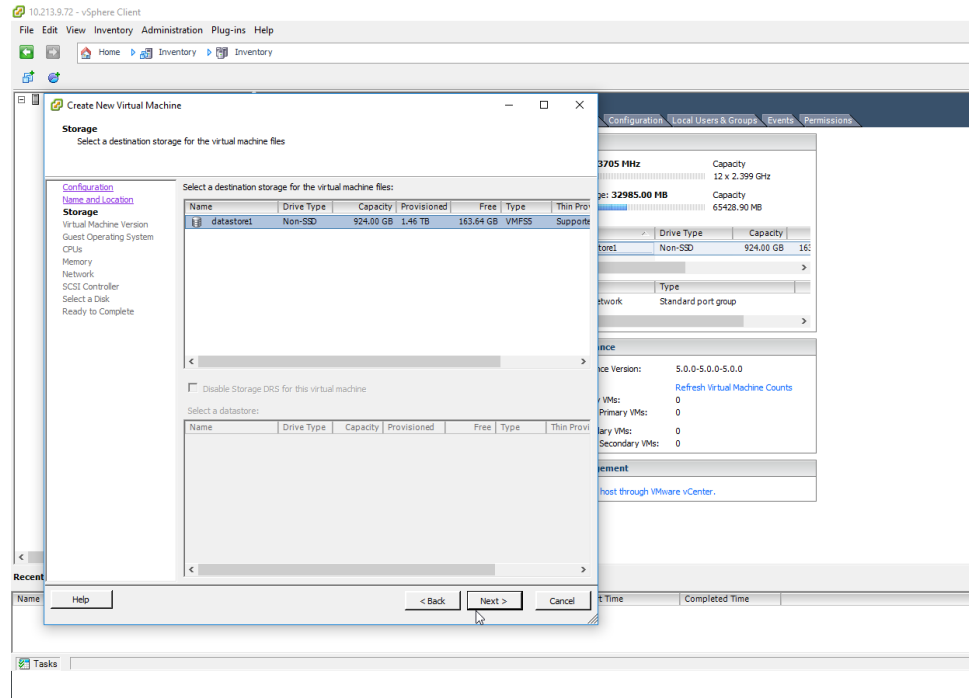
2. In the Configuration pane, select the **Custom** button and click **Next**.



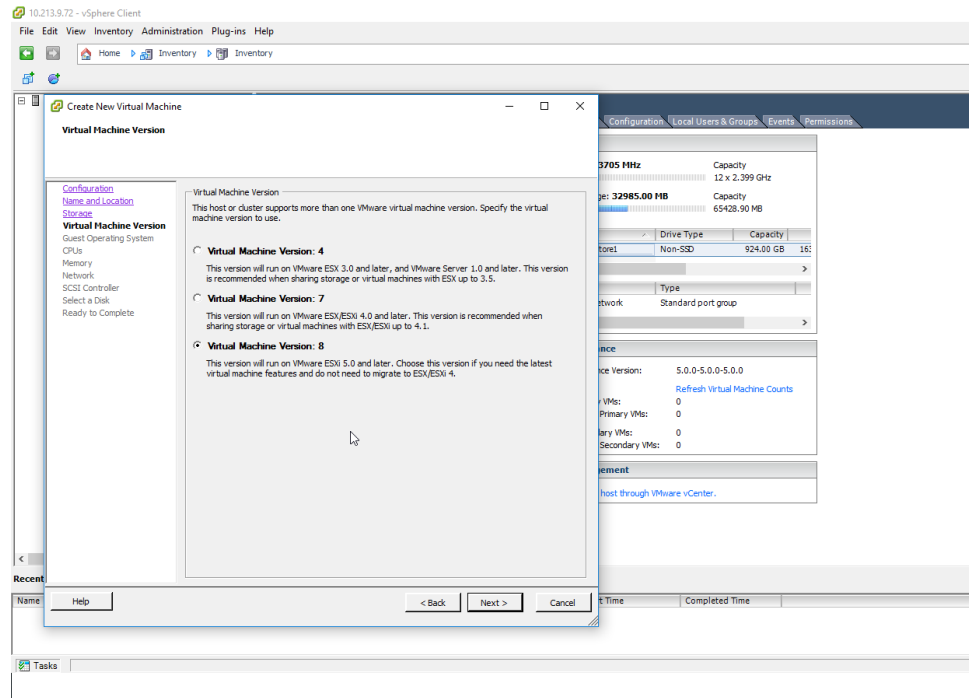
3. In the Name and Location pane, specify the name of the VM and click **Next**. For example, **CSD-Topology_JunosVM** for the JunosVM.



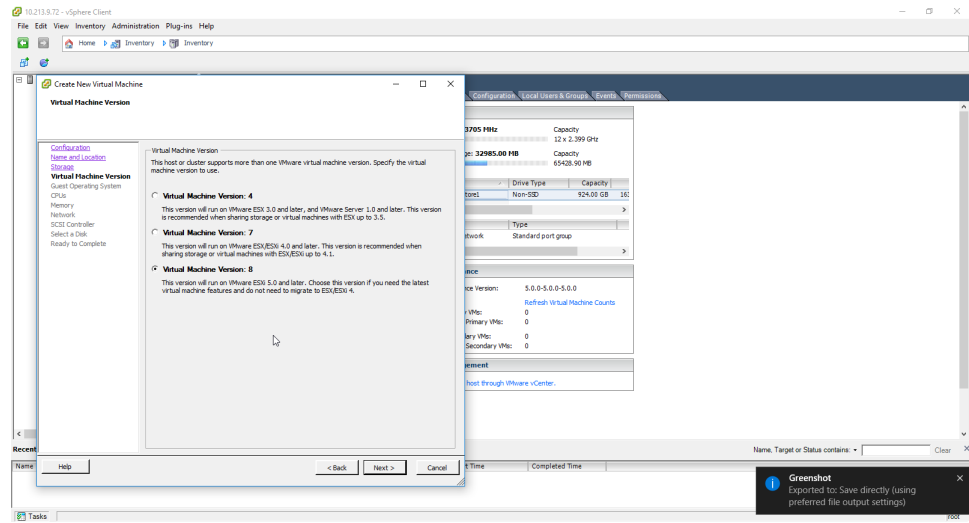
4. In the Storage pane, select appropriate datastore (for example, **datastore1**) for the destination storage of the VM and click **Next**.



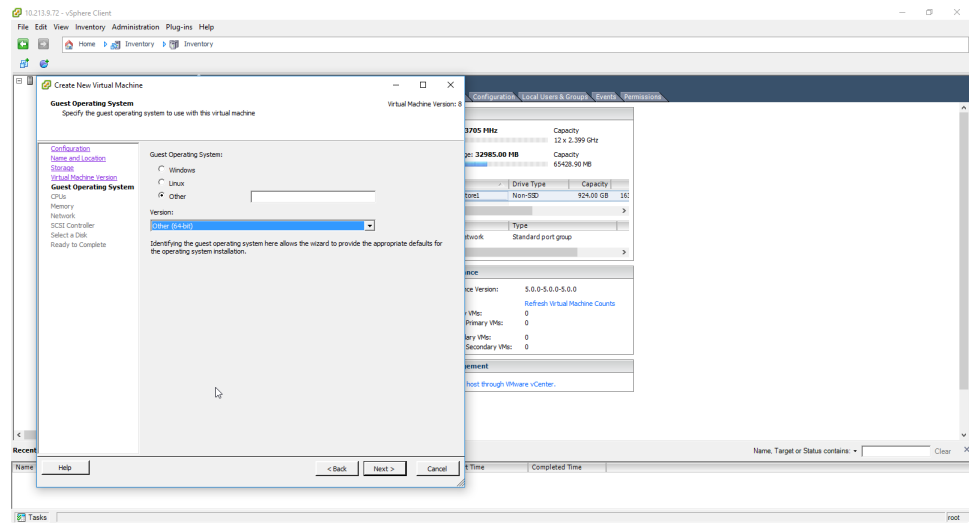
- In the Virtual Machine Version pane, select the **Virtual Machine Version: 8** button and click **Next**.



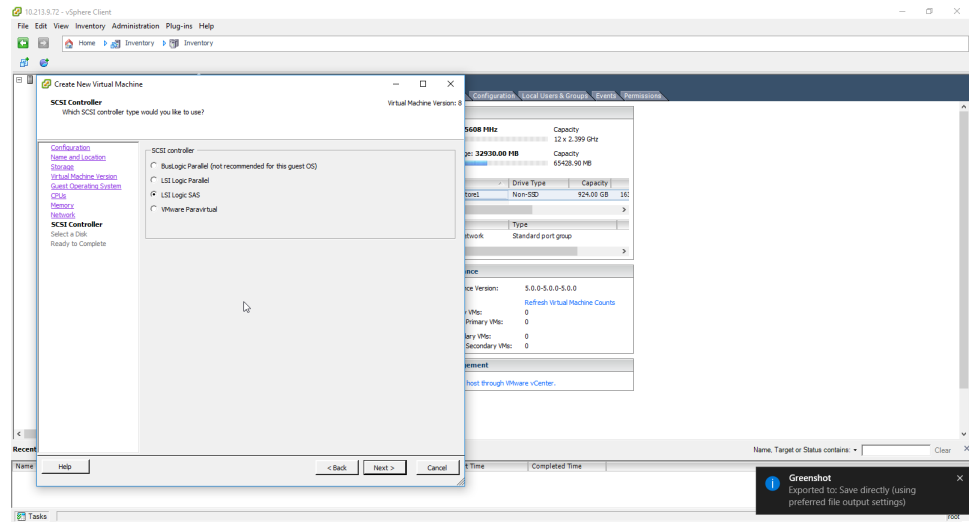
- In the Guest Operating System pane, select the **Other** button, select **Other (64-bit)** from the list, and click **Next**.



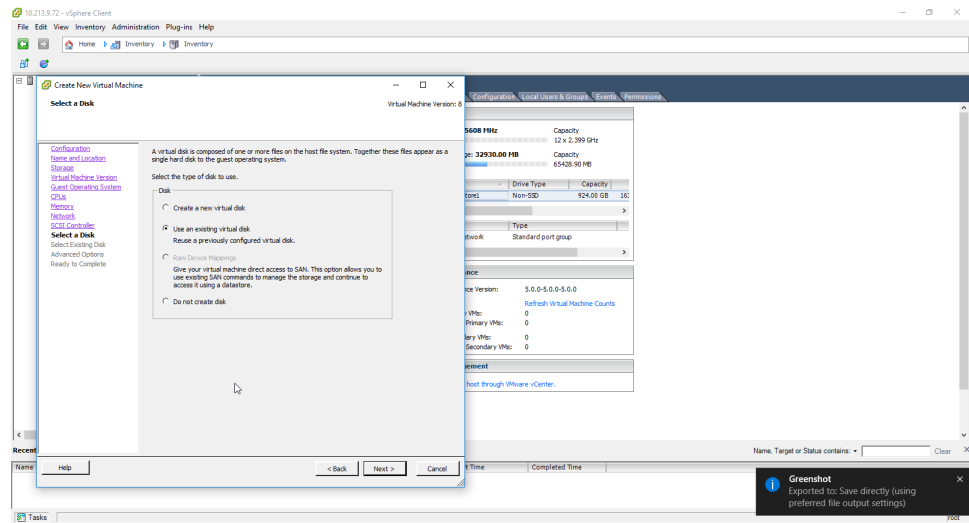
7. In the CPUs pane, select 2 for the number of cores per virtual socket and click **Next**.



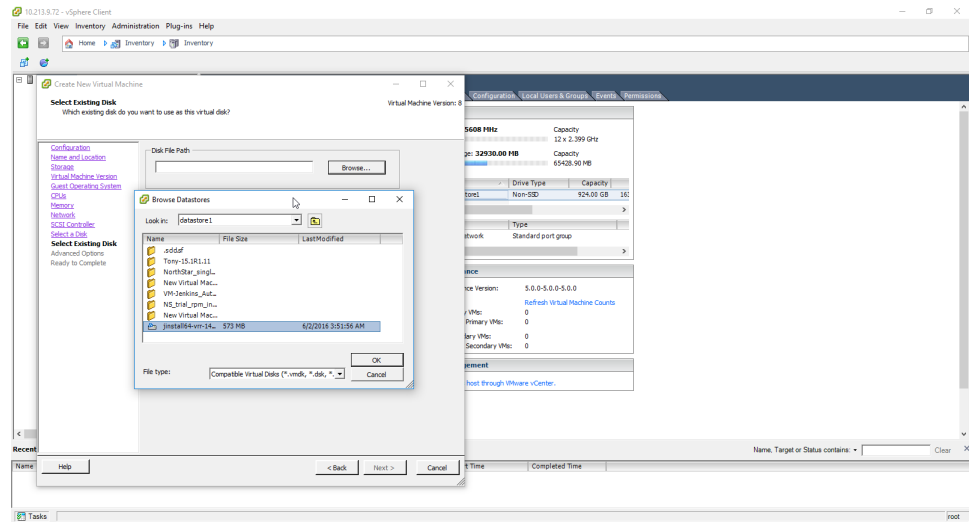
8. In the Memory pane, select 2 GB from the Memory Size list for the VM and click **Next**.



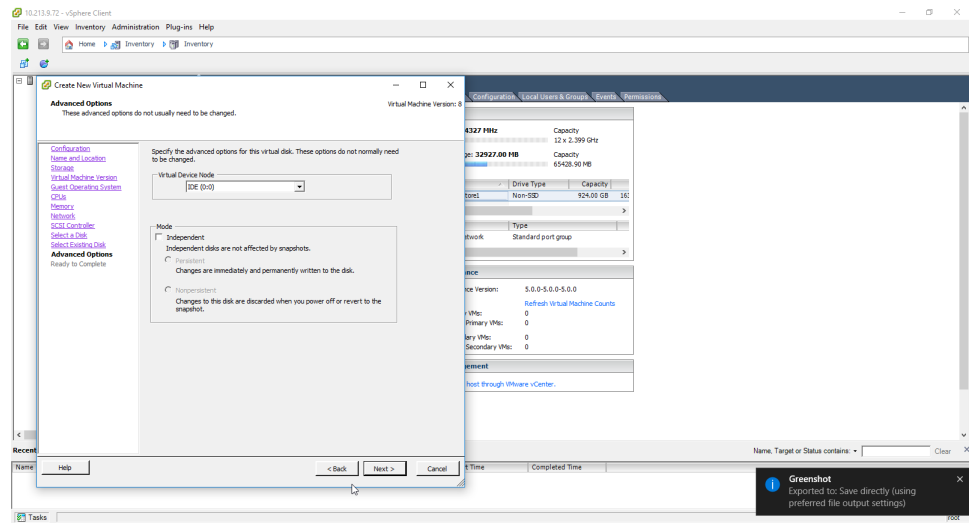
11. In the Select a Disk pane, select the **Use an existing virtual disk** button and click **Next**.



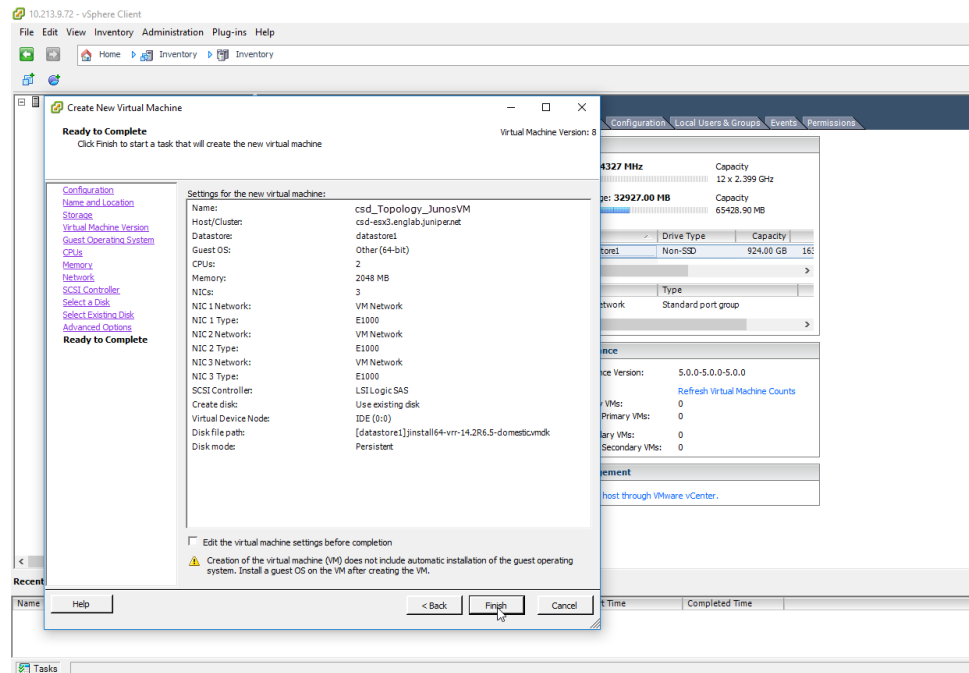
12. In the Select Existing Disk pane, click **Browse** to select the appropriate **install64-vmx*** file from the datastore and click **Next**.



13. In the Advanced Options pane, click **Next** to accept the default options.



14. In the Ready to Complete pane, click **Finish**.



Configuring the JunosVM

To configure the JunosVM:

1. Enter the following commands from the Junos OS CLI interface. Replace the variables with actual values to suit your network needs

```

set system host-name csd_topology_junosvm
set system root-authentication encrypted-password xxxx
set system login announcement "This JunOS VM is running in non-persistent
mode.\nIf you make any change on this JunOS VM,\nPlease make sure you save to
the Host using net_setup.py utility, otherwise the config will be lost if
this VM is restarted.\n\n"

set system processes routing force-32-bit
set interfaces em0 unit 0 family inet address Management IP address on JunosVM
set interfaces em2 unit 0 family inet address Management IP address on JunosVM
set interfaces lo0 unit 0 family inet filter input protect-re
set interfaces lo0 unit 0 family mpls
set routing-options static route 0.0.0.0/0 next-hop next-hop-address
set routing-options autonomous-system 36000
set protocols topology-export
set protocols mpls traffic-engineering database import igp-topology
set protocols mpls traffic-engineering database import policy TE
set protocols bgp group csdtopology type internal
set protocols bgp group csdtopology description "csdtopology BGP-TE Pering"
set protocols bgp group csdtopology local-address JunosVM management IP address
set protocols bgp group csdtopology family traffic-engineering unicast
set protocols bgp group csdtopology allow 0.0.0.0/0
set protocols isis traffic-engineering igp-topology
set policy-options prefix-list internal-net csdtopology server IP address
set policy-options policy-statement TE term 1 from family traffic-engineering
set policy-options policy-statement TE term 1 then accept
set policy-options policy-statement TE from family traffic-engineering
set policy-options policy-statement TE then accept
set firewall interface-set mgmt-intf em0.0
set firewall filter protect-re term mgmt-intf from interface-set mgmt-intf
set firewall filter protect-re term mgmt-intf then accept
set firewall filter protect-re term internal-net from prefix-list internal-net
set firewall filter protect-re term internal-net then accept
set firewall filter protect-re term ssh from protocol tcp
set firewall filter protect-re term ssh from port ssh
set firewall filter protect-re term ssh then accept
set firewall filter protect-re term bgp from protocol tcp
set firewall filter protect-re term bgp from port bgp
set firewall filter protect-re term bgp then accept
set firewall filter protect-re term ntp from protocol udp
set firewall filter protect-re term ntp from port ntp
set firewall filter protect-re term ntp then accept
set firewall filter protect-re term ospf from protocol ospf
set firewall filter protect-re term ospf then accept
set firewall filter protect-re term icmp from protocol icmp
set firewall filter protect-re term icmp then accept
set firewall filter protect-re term traceroute from protocol udp
set firewall filter protect-re term traceroute from port 33200-33600
set firewall filter protect-re term traceroute then accept
set firewall filter protect-re term default-discard then syslog
set firewall filter protect-re term default-discard then discard

```

Configuring the CSD-Topology Server with the JunosVM IP Address

To associate the CSD-Topology VM with JunosVM:

1. Establish an SSH session with the server running the CSD-Topology software.
2. Edit **northstar.cfg** file as follows:

```
modify /opt/csd-topology/data/northstar.cfg ntad_host=Management IP address of
the JunosVM
```

where **ntad_host** is the name of the topology discovery process running on the JunosVM. In this example, the management IP address of the JunosVM is 172.16.16.2.

3. Restart the JunosVM services.

```
sservice csd_topology restart all
```

Verifying the Connectivity Between the CSD-Topology Server and JunosVM

To verify the connectivity between the CSD-Topology server and JunosVM:

1. Establish a session with the server running the CSD-Topology software.
2. Run the **netstat** command to verify that connectivity is established between the CSD-Topology server and JunosVM.

```
[root@csd-topo ~]# netstat -an | grep 450
tcp        0      0 172.16.16.1:35178    172.16.16.2:450
ESTABLISHED
```

Verifying That the CSD-Topology Services Are Running

To verify that the CSD-Topology services are running correctly:

1. Access CSD-Topology server VM.
2. Run the **csd_topology status** command.

```
[root@csd-topo ~]# csd_topology status
infra:cassandra          RUNNING pid 1881, uptime 4 days, 21:12:20
infra:ha_agent           RUNNING pid 1880, uptime 4 days, 21:12:20
infra:haproxy            RUNNING pid 1877, uptime 4 days, 21:12:20
infra:nodejs             RUNNING pid 2558, uptime 4 days, 21:10:47
infra:rabbitmq           RUNNING pid 1879, uptime 4 days, 21:12:20
infra:zookeeper          RUNNING pid 1878, uptime 4 days, 21:12:20
listener1:listener1_00   RUNNING pid 1876, uptime 4 days, 21:12:20
northstar:mladapter       RUNNING pid 2707, uptime 4 days, 21:10:04
northstar:npat           RUNNING pid 2661, uptime 4 days, 21:10:15
northstar:npat_ro        RUNNING pid 2658, uptime 4 days, 21:10:15
northstar:pceserver      RUNNING pid 2586, uptime 4 days, 21:10:36
```

northstar:pcserver	RUNNING	pid 2620, uptime 4 days, 21:10:25
northstar:toposerver	RUNNING	pid 2659, uptime 4 days, 21:10:15

Stopping Firewall on theCSD-Topology Server

You can optionally stop firewall services. To stop firewall services on the CSD-Topology server:

1. Access CSD-Topology server VM.
2. Stop firewall services on the CSD-Topology server.

```
[root@csd_topo csd_topology_bundle]# service iptables stop
```

Configuring Peer Routers and Topology Acquisition on the JunosVM

To configure the peer route settings on the JunosVM for BGP peering:

1. Configure a policy.

```
[edit policy-options]
user@PE1# set policy-statement TE term 1 from family traffic-engineering
user@PE1# set policy-statement TE term 1 then accept
```

2. Configure BGP-link state (LS) distribution on the CSD-Topology for topology acquisition

- a. Specify the autonomous system (AS) number for the node (BGP peer).

```
[edit routing-options]
user@csd_topology_junosvm# set autonomous-system AS_number
```

- b. Specify the BGP group name and type for the node.

```
[edit protocols bgp]
user@csd_topology_junosvm# set group group_1 type internal
```

- c. Specify a description for the BGP group for the node.

```
[edit protocols bgp group group_1]
user@csd_topology_junosvm# set description "CSD-Topology BGP-TE Peering"
```

- d. Specify the address of the local end of a BGP session.

This is the IP address for the JunosVM external IP address which is used to accept incoming connections to the JunosVM peer and to establish connections to the remote peer.

```
[edit protocols bgp group group_1]
user@csd_topology_junosvm# set local-address <junosVM IP address>
```

- e. Enable the traffic engineering features for the BGP routing protocol.

```
[edit protocols bgp group group_1]
user@csd_topology_junosvm# set family traffic-engineering unicast
```

- f. Specify the IP address for the neighbor router that connects with the CSD-Topology.

```
[edit protocols bgp group group_1]
user@csd_topology_junosvm# set neighbor <router loopback IP address>
```



NOTE: You can specify the router loopback address if it is reachable by the BGP peer on the other end. But for loopback to be reachable, usually some IGP has to be enabled between the CSD-Topology JunosVM and the peer on the other end.

3. Import the routes into the traffic-engineering database.

```
[edit protocols mpls traffic-engineering database]
user@PE1# set import policy TE
```

4. Configure a BGP group by specifying the IP address of the router that peers with the CSD-Topology as the local address (typically the loopback address) and the JunosVM external IP address as the neighbor.

```
[edit routing-options]
user@PE1# set autonomous-system AS Number

[edit protocols bgp group csd-topology]
user@PE1# set type internal
user@PE1# set description "CSD-Topology BGP-TE Peering"
user@PE1# set local-address <router-IP-address>
user@PE1# set family traffic-engineering unicast
user@PE1# set export TE
user@PE1# set neighbor <JunosVM IP-address>
```

Specifying the Topology Details in the Connectivity Services Director GUI

To specify the topology preferences on the Connectivity Services Director server:

1. From the Junos Space user interface, click the **System** icon on the Connectivity Services Director banner.

The options that you can configure in System mode are displayed in a drop-down menu.

2. Select **Preferences** from the drop-down menu to open the Preferences page.

The Preferences page opens with User Preferences as the default tab.

3. Click the **Topology** tab to configure the CSD-Topology preference settings.

The settings that you can configure on the Topology tab are displayed.

4. In the L3 Topology Settings section, do the following:

- a. Select the **Use PCEP** check box to use the Path Computation Element Protocol (PCEP) for discovery of LSPs. PCEP enables communication between a PCC and the CSD-Topology to learn about the network and LSP path state and communicate with the Path Computation Clients (PCCs). If you select the **Use PCEP** check box, the LSP data is collected by using PCEP.

By default, this check box is not selected. If you do not enable this option to use PCEP for discovery of LSPs, Connectivity Services Director discovers the LSPs by parsing the configuration statements and operational command outputs of the devices that it manages.

- b. In the Topology Server field, specify the topology server IP address, which is the IP address of the system on which the CSD-Topology application is running.
- c. In the UserName and Password fields, specify the username and password of the user to allow the Connectivity Services Director to connect to the topology server.

- d. Click **Validate** beside the Password field, which triggers a task to examine and verify the entered credentials for connecting to the CSD-Topology server. A dialog box is displayed to indicate whether the specified credentials are valid or not.
 - e. Click **OK** to close the dialog box. If the login credentials for communicating with the CSD-Topology are invalid, correct the username and password values and revalidate them.
5. Click **OK** to save the settings.
You are prompted to confirm the changes you made to topology preferences.
 6. Click **Yes** to confirm.

The Preferences page is closed. A dialog box is displayed to confirm the successful saving of topology preferences. Click **OK** to close the dialog box.

**Related
Documentation**

- [Connecting an x86 Server to the Network](#)

Connecting an x86 Server to the Network

For minimum hardware requirements, see [“Installation Prerequisites” on page 262](#).

To establish basic TCP connectivity to the network, you must connect your x86 64-bit network appliance (running the CSD-Topology software) directly to a switch or router.

Before configuring the x86 server to connect to the network, download and install the RPM bundle as described in [“Installing the CSD-Topology Software Using the RPM Bundle” on page 262](#).

After installing the RPM bundle, the following default settings apply:

- Host machine:
 - User=**root**
 - Password=**csdtopology**
 - IP addresses:
 - external0=**dhcp**
 - host mgmt0=**172.16.17.1/24**
 - host management:internal network=**172.16.16.1/24**



NOTE: The Path Computation Server (PCS) runs native on the host machine, and the host address is the PCS.

- JunosVM:

- User=**csdtopology**
- Password=**csdtopology**
- Root Password=**csdtopology**
- IP addresses:
 - em0=**172.16.16.2/24**
 - em1=**none**
 - em2=**172.16.17.2/24**



NOTE:

The following default values are also configured for the JunosVM configuration:

- JunosVM internal IP address: 172.16.16.2
- JunosVM internal netmask: 255.255.255.0



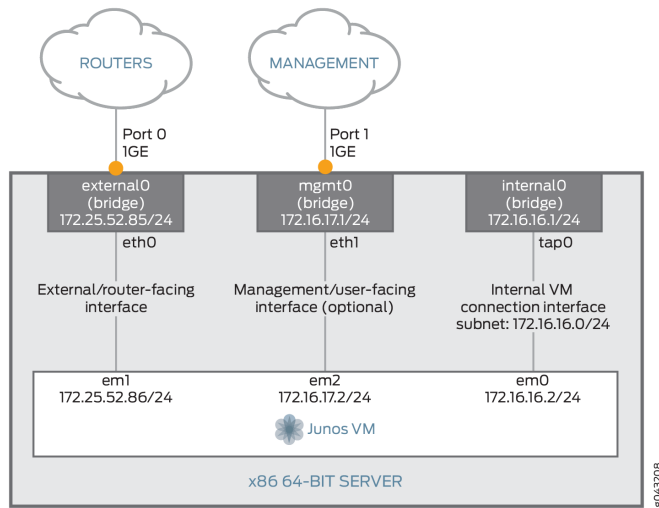
NOTE: The JunosVM internal IP and netmask should not be changed.



NOTE: For network security, by default, JunosVM SSH and telnet access is restricted and available only from the host server (PCS server) using the 172.16.16.2 IP address. To remove this restriction, you can manually remove the firewall filter on the JunosVM lo0 (loopback) configuration.

Figure 20 on page 283 shows the default interfaces and preconfigured addresses on the x86 appliance.

Figure 20: Interfaces and Addresses Preconfigured on the x86 Appliance



To establish basic connectivity between the x86 network appliance and a switch or router:

1. Power on the x86 network appliance.
2. Use one of the following options to access the x86 console:

- Use a serial cable to connect to the serial console.

You can use an SSH client (hypertem, minicom, or securecr) to connect to the serial console.



NOTE: To set up the serial port connection, refer to your hardware manual.



NOTE: The serial port setting should be 9600-8-N-1 with hardware control enabled.

- If your network appliance has two or more Ethernet ports, use an Ethernet cable to connect to the x86 appliance management interface.
 - a. Connect an Ethernet cable from a laptop computer to 1-Gigabit Ethernet port 1 on the x86 appliance.
 - b. Configure the IP address on your laptop to 172.16.17.10/24.
 - c. Using an SSH client, connect to the x86 appliance at IP address 172.16.17.1.
- 3. On the network appliance, connect a 1-Gigabit Ethernet or 10-Gigabit Ethernet port to the LAN switch or router that you will use to access the network.



NOTE: The Ethernet interface on the switch or router must be configured in access/untagged mode.

4. From prompt, log in to the x86 system with the username **root** and password **password**.
5. To configure the required network settings, access the Main Menu:

```
[root@csd-topo ~]# /opt/csd-topology/utis/net_setup.py
```

The Main Menu, shown in [Figure 21 on page 284](#), displays the options that you can select to configure the host and JunosVM settings, verify network settings, perform maintenance and troubleshooting, and collect trace and log files.

Figure 21: CSD-Topology Main Menu

```
Main Menu:
.....
A.) Host configuration
B.) JunosVM configuration
.....
C.) Check Network Setting
.....
D.) Maintenance & Troubleshooting
.....
E.) HA Setting
.....
F.) Collect Trace/Log
.....
X.) Exit
.....

Please select a letter to execute.
```



NOTE: To establish connectivity between the x86 network appliance and a switch or router, the host IP and JunosVM IP addresses (including netmask and default gateway) must be from the same subnet.

- a. To create the host configuration:



NOTE: You must provide settings for the host external IP address, host external netmask, and host default gateway. All other host settings are optional.

1. Type **A** at the prompt and press Enter to update the host configuration.
The current CSD-Topology host configuration settings are displayed.
 2. For each host setting you want to configure, enter the number that corresponds to the specific host parameter (host external IP address, host external netmask, host management IP address, host default gateway, and so forth), and enter the appropriate value.
 3. After you configure the required host settings, type **B** to apply the host settings.
- b. To create the JunosVM configuration:



NOTE: You must provide settings for the JunosVM external IP address, JunosVM external netmask, JunosVM default gateway, and BGP AS number. All other JunosVM settings are optional.

1. Type **B** at the prompt and press Enter to update the CSD-Topology JunosVM configuration.
The current JunosVM configuration settings are displayed.
 2. For each JunosVM setting you want to configure, enter the number that corresponds to the specific JunosVM parameter (JunosVM external IP address, JunosVM external netmask, JunosVM management IP address, JunosVM default gateway, and BGP AS number), and enter the appropriate value.
 3. After configuring the required JunosVM settings, type **C** to apply the JunosVM settings.
6. Verify the host and JunosVM configurations and deploy.
- a. Type **C** at the prompt and press Enter to view all current host configuration and JunosVM configuration settings.
 - b. To apply all updated host and JunosVM configuration settings to the CSD-Topology, type **Y** and press Enter.

Related Documentation

- [Configuring Connectivity for BGP-LS Topology Acquisition on page 291](#)
- [Configuring Connectivity for OSPF Topology Acquisition on page 294](#)
- [Configuring Connectivity for IS-IS Topology Acquisition on page 296](#)

Interactive Method of Installing the RPM Image and CSD-Topology Software from a USB or DVD Drive

You can install the CSD-Topology RPM image on any x86 64-bit network appliance.

Before configuring the x86 server to connect to the network, download and install the RPM bundle as described in [“Installing the CSD-Topology Software Using the RPM Bundle” on page 262](#).

If you have a keyboard and monitor as part of your system, the interactive installation method is preferred. To install the ISO image on the x86 network appliance from a USB drive using the interactive method:

1. Power on the x86 network appliance.

The CSD-Topology login prompt is displayed after you power on the appliance.

2. Enter the following command to launch the interactive user interface:

```
[root@csd-topo ~]# /csd-topology/csd_topology_2.0.0_interactive_install.md
```

3. Plug in the USB or DVD drive with the RPM image of the CSD-Topology package to the x86 appliance.
4. When the “Welcome to CSD-Topology(SCL 6.6R2.0)” screen is displayed, select the appropriate Boot option (the default is **Boot from Local HDD**), and press Enter to start the CSD-Topology installation.

The CentOS 6 logo screen is displayed.

5. Click **Next**.
6. Select your preferred language for the installation process, and click **Next**.
7. Choose your preferred storage type, and click **Next**.
8. Indicate your time zone, and click **Next**.
9. Enter and confirm the root password, and click **Next**.
10. Select a partitioning option, and click **Next**.



NOTE: Because CSD-Topology is installed in /opt/, be sure to allocate sufficient space for /opt.

11. Indicate your preferences regarding boot loader (two screens), and click **Next** after completing each screen.
12. Select **Core** installation, and click **Next**.
13. The CentOS 6 logo screen is displayed, showing installation progress. When the installation completes, the screen shows that all packages are completed.
14. Two errors are displayed because the password has not yet been initialized and the license key has not yet been added:
 - The state of all CSD-Topology processes shows as STOPPED.
 - The state of the PCServer process shows as FATAL.
15. To resolve the license error, copy the npatpw license file to /opt/pcs/db/sys.



NOTE: Be sure the owner of the file is pcs.

16. To resolve the password error, access the Main Menu:

```
[root@csd-topo ~]# /opt/csd-topology/utls/net_setup.py
```

From the Main Menu shown in [Figure 22 on page 287](#), select **D** for Maintenance & Troubleshooting.

Figure 22: CSD-Topology Controller Main Menu

```
Main Menu:
.....
A.) Host configuration
B.) JunosVM configuration
.....
C.) Check Network Setting
.....
D.) Maintenance & Troubleshooting
.....
E.) HA Setting
.....
F.) Collect Trace/Log
.....
X.) Exit
.....

Please select a letter to execute.
```

Select **9** to Initialize all credentials.

The state of all processes should now show as RUNNING.

Disconnect the USB flash drive or DVD drive that is connected to the x86 network appliance.

17. Power on the x86 network appliance.

The system requires a few minutes to power on. Then the CSD-Topology login prompt is displayed.

18. From the CSD-Topology login prompt, enter user **root** and the root password you selected during the installation to log in to the CSD-Topology CLI.

19. Run each of the following commands to verify that the JunosVM and Path Computation Server (PCS) processes are running and that key directories were successfully installed:

- a. As root user, run the **service csdtopology status** command to verify that JunosVM is running. This command tells you the status of all processes, the disk space being used, network configuration check results, and JunosVM check results.
- b. After your license is set, run the **ps-ef | grep PCS** command to verify that the PCS is running on specific ports.

- Related Documentation**
- [Installation Prerequisites on page 262](#)
 - [Installing the CSD-Topology Software Using the RPM Bundle on page 262](#)

Configuring Topology Acquisition and Connectivity Between the CSD-Topology and Path Computation Clients

- [Configuring PCEP on a PE Router \(from CLI\) on page 289](#)
- [Configuring Connectivity for BGP-LS Topology Acquisition on page 291](#)
- [Configuring Connectivity for OSPF Topology Acquisition on page 294](#)
- [Configuring Connectivity for IS-IS Topology Acquisition on page 296](#)

Configuring PCEP on a PE Router (from CLI)

A Path Computation Client (PCC) supports the configurations related to the Path Computation Element (PCE) and communicates with the CSD-Topology, which by default is configured to accept a Path Computation Element Protocol (PCEP) connection from any source address. However, you must configure PCEP on each PE router to configure the router as a PCC and establish a connection between the PCC and the CSD-Topology. A PCC initiates path computation requests, which are then executed by the CSD-Topology.

The following requirements apply for each PCC in the network that the CSD-Topology can access:

- The corresponding JSDN package (with PCEP support) is installed on the router.



NOTE: You must boot the PCC router with the Junos OS 14.2X1.1 image, and then boot the router a second time with the JSDN image. After the router boots up a second time, the router (functioning as a PCC) is able to support the configurations related to the PCE and communicate with the CSD-Topology.



NOTE: For a PCEP connection, the PCC can connect to the CSD-Topology using an in-band or out-of-band management network, provided that IP connectivity is established between the Path Computation Server (PCS) and the specified PCEP local address. In some cases, an additional static route might be required from the CSD-Topology to reach the PCC, if the IP address is unreachable from the CSD-Topology default gateway.

To configure a PE router as a PCC:

1. Enable external control of LSPs from the PCC router to the CSD-Topology.

```
[edit protocols]
user@PE1# set mpls lsp-external-controller pccd
```

2. Specify the loopback address of the PCC router as the local address, for example:

```
[edit protocols]
user@PE1# set pcep pce csdtopology local-address 10.0.0.101
```



NOTE: As a best practice, the router ID is usually the loopback address, but is not necessarily configured this way.

3. Specify the CSD-Topology (**csdtopology**) as the PCE that the PCC connects to, and specify the CSD-Topology host external IP address as the destination address.

```
[edit protocols]
user@PE1# set pcep pce csdtopology destination-ipv4-address 10.99.99.1
```

4. Configure the destination port for the PCC router that connects to the CSD-Topology (PCE server) using the TCP-based PCEP.

```
[edit protocols]
user@PE1# set pcep pce csdtopology destination-port 4189
```

5. Configure the PCE type.

```
[edit protocols]
user@PE1# set pcep pce csdtopology pce-type active
user@PE1# set pcep pce csdtopology pce-type stateful
```

6. Enable LSP provisioning.

```
[edit protocols]
user@PE1# set pcep pce csdtopology lsp-provisioning
```

7. To verify that PCEP has been configured on the router, open a telnet session to access the router, and run the following commands:

```
user@PE1> show configuration protocols mpls
```

Sample output:

```
lsp-external-controller pccd;
```

```
user@PE1> show configuration protocols pcep
```

Sample output:

```
pce csdtopology {  
  local-address 10.0.0.101;  
  destination-ipv4-address 10.99.99.1;  
  destination-port 4189;  
  pce-type active-stateful;  
  lsp-provisioning;  
}
```

**Related
Documentation**

- [Mapping a Management IP Address for Path Computation Clients](#)
- [Configuring Connectivity for BGP-LS Topology Acquisition on page 291](#)
- [Configuring Connectivity for OSPF Topology Acquisition on page 294](#)
- [Configuring Connectivity for IS-IS Topology Acquisition on page 296](#)

Configuring Connectivity for BGP-LS Topology Acquisition

After you have successfully established a connection between the CSD-Topology and the network, you can configure topology acquisition using Border Gateway Protocol Link State (BGP-LS). For BGP-LS topology acquisition, you must configure both the CSD-Topology and the PCC routers.

**NOTE:**

We recommend that you use BGP-LS instead of IGP adjacency for the following reasons:

- The OSPF and IS-IS databases have a lifetime timer, and if the OSPF or IS-IS neighbor is down, the OSPF or IS-IS database is not removed immediately, and the CSD-Topology will not be able to determine whether the topology is valid or not.
- Using BGP-LS minimizes the risk of making the JunosVM a transit router between AS areas if the GRE metric is not properly configured.
- Typically, the CSD-Topology is located in a NOC Data Center and multihops away from the backbone routers and MPLS TE routers.



NOTE: If BGP-LS is used, JunosVM is configured to automatically accept any I-BGP session from, in this example, 0.0.0.0/0. However, you must verify that JunosVM is correctly configured and that it has IP reachability to the peering router.

Before you begin, complete the following tasks:

- Verify IP connectivity between a switch (or router) and the x86 appliance on which CSD-Topology software is installed.
- Make sure that PCEP is configured on each PE router in the network topology.

To configure BGP-LS topology acquisition, see:

- [Configuring BGP-LS Topology Acquisition on the CSD-Topology on page 292](#)
- [Configuring Topology Acquisition on the PCC Routers on page 293](#)

Configuring BGP-LS Topology Acquisition on the CSD-Topology

To configure BGP-LS on the CSD-Topology for topology acquisition, perform the following configuration steps from the CSD-Topology JunosVM:

1. Initiate an SSH or telnet session to the JunosVM external IP or management IP address.
2. Specify the autonomous system (AS) number for the node (BGP peer).

```
[edit routing-options]
user@csd_topology_junosvm# set autonomous-system AS_number
```

3. Specify the BGP group name and type for the node.

```
[edit protocols bgp]
user@csd_topology_junosvm# set group group_1 type internal
```

- Specify a description for the BGP group for the node.

```
[edit protocols bgp group group_1]
user@csd_topology_junosvm# set description "csd-topology BGP-TE Peering"
```

- Specify the address of the local end of a BGP session.

This is the IP address for the JunosVM external IP address which is used to accept incoming connections to the JunosVM peer and to establish connections to the remote peer.

```
[edit protocols bgp group group_1]
user@csd_topology_junosvm# set local-address <junosVM IP address>
```

- Enable the traffic engineering features for the BGP routing protocol.

```
[edit protocols bgp group group_1]
user@csd_topology_junosvm# set family traffic-engineering unicast
```

- Specify the IP address for the neighbor router that connects with the CSD-Topology.

```
[edit protocols bgp group group_1]
user@csd_topology_junosvm# set neighbor <router loopback IP address>
```



NOTE: You can specify the router loopback address if it is reachable by the BGP peer on the other end. But for loopback to be reachable, usually some IGP has to be enabled between the CSD-Topology JunosVM and the peer on the other end.

Configuring Topology Acquisition on the PCC Routers

To enable the CSD-Topology to discover the network, you must add the following configuration on each router that peers with the CSD-Topology. The CSD-Topology JunosVM must peer with at least one router from each area (autonomous system).

To configure topology acquisition, initiate a telnet session to each PCC router and add the following configuration:

- Configure a policy.

```
[edit policy-options]
user@PE1# set policy-statement TE term 1 from family traffic-engineering
user@PE1# set policy-statement TE term 1 then accept
```



NOTE: This configuration is appropriate for both OSPF and IS-IS.

2. Import the routes into the traffic-engineering database.

```
[edit protocols mpls traffic-engineering database]
user@PE1# set import policy TE
```

3. Configure a BGP group by specifying the IP address of the router that peers with the CSD-Topology as the local address (typically the loopback address) and the JunosVM external IP address as the neighbor.

```
[edit routing-options]
user@PE1# set autonomous-system AS Number

[edit protocols bgp group bgp group1]
user@PE1# set type internal
user@PE1# set description "CSD-Topology BGP-TE Peering"
user@PE1# set local-address <router-IP-address>
user@PE1# set family traffic-engineering unicast
user@PE1# set export TE
user@PE1# set neighbor <JunosVM IP-address>
```

- See Also**
- [Configuring PCEP on a PE Router \(from CLI\) on page 289](#)
 - [Mapping a Management IP Address for Path Computation Clients](#)
 - [Configuring Connectivity for OSPF Topology Acquisition on page 294](#)
 - [Configuring Connectivity for IS-IS Topology Acquisition on page 296](#)

Configuring Connectivity for OSPF Topology Acquisition

If BGP-LS is not being used, one of the IGP protocols must be configured on the CSD-Topology. To enable OSPF on CSD-Topology, before you begin, verify IP connectivity between a switch (or router) and the x86 appliance on which CSD-Topology software is installed.

To configure OSPF topology acquisition, see:

- [Configuring OSPF on the CSD-Topology on page 294](#)
- [Configuring OSPF Over GRE on the CSD-Topology on page 295](#)

Configuring OSPF on the CSD-Topology

To configure OSPF on the CSD-Topology:

1. Configure the policy.

```
[edit policy-options]
user@csd_topology_junosvm# set policy-statement TE term 1 from family
traffic-engineering
user@csd_topology_junosvm# set policy-statement TE term 1 then accept
```

2. Populate the traffic engineering database.

```
[edit]
user@csd_topology_junosvm# set protocols mpls traffic-engineering database import
policy TE
```

3. Configure OSPF.

```
[edit]
user@csd_topology_junosvm# set protocols ospf area area interface interface
interface-type p2p
```

Configuring OSPF Over GRE on the CSD-Topology

Once you have configured OSPF on the CSD-Topology, you can take the following additional steps to configure OSPF over GRE:

1. Initiate an SSH or telnet session using the IP address for the CSD-Topology JunosVM external IP address.
2. Configure the tunnel.

```
[edit interfaces]
user@csd_topology_junosvm# set gre unit 0 tunnel source local-physical-ip
user@csd_topology_junosvm# set gre unit 0 tunnel destination destination
user@csd_topology_junosvm# set gre unit 0 family inet address tunnel-ip-addr
user@csd_topology_junosvm# set gre unit 0 family iso
user@csd_topology_junosvm# set gre unit 0 family mpls
```

3. Enable OSPF traffic engineering on the JunosVM and add the GRE interface to the OSPF configuration.

```
[edit protocols ospf]
user@csd_topology_junosvm# set traffic-engineering
user@csd_topology_junosvm# set area area interface gre.0 interface-type p2p
user@csd_topology_junosvm# set area area interface gre.0 metric 65530
```

- See Also**
- [Configuring PCEP on a PE Router \(from CLI\) on page 289](#)
 - [Mapping a Management IP Address for Path Computation Clients](#)
 - [Configuring Connectivity for BGP-LS Topology Acquisition on page 291](#)
 - [Configuring Connectivity for IS-IS Topology Acquisition on page 296](#)

Configuring Connectivity for IS-IS Topology Acquisition

If BGP-LS is not being used, you must configure one of the IGP protocols on the CSD-Topology. To enable IS-IS on the CSD-Topology, before you begin, complete the following tasks:

1. Verify IP connectivity between a switch (or router) and the x86 appliance on which CSD-Topology software is installed.
2. Configure interfaces on the JunosVM for IS-IS routing, for example:

```
[edit]
user@csd_topology_junosvm# set interfaces em0 unit 0 family inet address
172.16.16.2/24
user@csd_topology_junosvm# set interfaces em1 unit 0 family inet address
192.168.179.117/25
user@csd_topology_junosvm# set interfaces em0 unit 0 family inet address
172.16.16.2/24
user@csd_topology_junosvm# set interfaces em2 unit 0 family mpls
user@csd_topology_junosvm# set interfaces lo0 unit 0 family inet address
88.88.88.88/32 primary
user@csd_topology_junosvm# set routing-options static route 0.0.0.0/0 next-hop
192.168.179.126
user@csd_topology_junosvm# set routing-options autonomous-system 1001
```

To configure IS-IS topology acquisition, see:

- [Configuring IS-IS on the CSD-Topology on page 296](#)
- [Configuring IS-IS Over GRE on the CSD-Topology on page 297](#)

Configuring IS-IS on the CSD-Topology

To configure IS-IS topology acquisition and enable IS-IS routing, perform the following steps on the CSD-Topology JunosVM:

1. Configure the policy.

```
[edit policy-options]
user@csd_topology_junosvm# set policy-statement TE term 1 from family
traffic-engineering
user@csd_topology_junosvm# set policy-statement TE term 1 then accept
```

2. Populate the traffic engineering database.

```
[edit protocols]
user@csd_topology_junosvm# set mpls traffic-engineering database import policy TE
```

3. Configure IS-IS.

```
[edit protocols]
```



```
user@csd_topology_junosvm# set isis interface interface level level metric metric
user@csd_topology_junosvm# set isis interface interface point-to-point
```

Configuring IS-IS Over GRE on the CSD-Topology

Once you have configured IS-IS on the CSD-Topology, you can take the following additional steps to configure IS-IS over GRE:

1. Initiate an SSH or telnet session using the IP address for the CSD-Topology JunosVM external IP address.
2. Configure the tunnel.

```
[edit interfaces]
user@csd_topology_junosvm# set gre unit 0 tunnel source local-physical-ip
user@csd_topology_junosvm# set gre unit 0 tunnel destination destination
user@csd_topology_junosvm# set gre unit 0 family inet address tunnel-ip-addr
user@csd_topology_junosvm# set gre unit 0 family iso
user@csd_topology_junosvm# set gre unit 0 family mpls
```

3. Add the GRE interface to the IS-IS configuration.

```
[edit protocols isis]
user@csd_topology_junosvm# set interface gre.0 level level metric 65530
user@csd_topology_junosvm# set interface gre.0 point-to-point
```

- See Also**
- [Configuring PCEP on a PE Router \(from CLI\) on page 289](#)
 - [Mapping a Management IP Address for Path Computation Clients](#)
 - [Configuring Connectivity for BGP-LS Topology Acquisition on page 291](#)
 - [Configuring Connectivity for OSPF Topology Acquisition on page 294](#)

CHAPTER 18

Accessing the Topology View of CSD-Topology

- [Understanding the Network Topology in Connectivity Services Director on page 300](#)
- [Monitoring the Topology of Network Elements Managed by CSD-Topology Overview on page 301](#)
- [Specifying Topology Preferences on page 302](#)
- [CSD-Topology Topology Map Window Overview on page 304](#)
- [Working with the Graphical Image in the Topology View Window on page 306](#)
- [Expanding and Collapsing Groups by Using the Topology Map Grouping Shortcut Menu on page 309](#)
- [Filtering Links, LSPs, and Services by Using the Topology Map Node Shortcut Menu on page 310](#)
- [Removing the Highlighted LSPs by Using the Topology Map LSPs Shortcut Menu on page 311](#)
- [Viewing the Service Path by Using the Topology Map Service Shortcut Menu on page 312](#)
- [Filtering Devices, LSPs, and Services for Sorting and Segregating the Topology View on page 313](#)
- [Segregating the Displayed Devices by Searching the Entire Topology View on page 314](#)
- [Resynchronizing the Topology View on page 315](#)
- [Viewing Device Details of a CSD-Topology for Examining Traffic Transmission on page 316](#)
- [Viewing LSP Details of a CSD-Topology for Analyzing Network Changes on page 318](#)
- [Viewing Link Details of a CSD-Topology for Determining the Operational Status on page 321](#)
- [Viewing Service Details of a CSD-Topology for Monitoring and Troubleshooting Service Parameters on page 323](#)
- [Viewing Topology Map Group Details in a Pop-Up Dialog Box on page 326](#)
- [Viewing Topology Map Device Details in a Pop-Up Dialog Box on page 328](#)
- [Viewing Topology Map Link Details in a Pop-Up Dialog Box on page 330](#)
- [Viewing Topology Map LSP Details in a Pop-Up Dialog Box on page 332](#)

- [Viewing Topology Map Service Details in a Pop-Up Dialog Box on page 334](#)
- [Enabling the Collection of LSP and Service Association Details on page 336](#)
- [Using Custom Grouping for Devices in a CSD Topology on page 336](#)
- [Viewing Generated Alarms for Services in the Topology View on page 337](#)
- [Viewing the Optical Link Details for Examining the Performance of Optical Links on page 338](#)

Understanding the Network Topology in Connectivity Services Director

Junos Space Connectivity Services Director provides features for monitoring and managing Juniper Networks ACX Series routers, M Series routers, MX Series routers, and PTX Series routers. Connectivity between devices and their association with their location provide the foundation for rendering topology in a complete manner.

As a network administrator, you must have a clear understanding of the various networking devices in your network, their physical locations, and how these devices are interconnected in your network. The network topology represents the interconnection between various devices in your network, which are managed by Connectivity Services Director, based on their connectivity and association to their physical surroundings. The network topology provides a visual insight into the network, which is useful for debugging, troubleshooting, planning, and executing administrative actions.

Before you access the topological view of your network, you must:

- Discover the devices managed by Connectivity Services Director in your network. For details about discovering devices, see [“Discovering Devices in a Physical Network” on page 177](#).



NOTE: You must specify the SNMP parameters during device discovery to have all the devices discovered and managed by Connectivity Services Director available in Topology View.



NOTE: Ensure that you have enabled the LLDP, STP, or RSTP protocols on the devices as Connectivity Services Director uses these protocols to determine the connectivity of devices with their neighbors in the network. LLDP and RSTP protocols are enabled by default on all MX Series routers.

Network topology enables you to view all the discovered devices in your network, where the devices are located along with their physical interconnection with other devices in your network. Topology also provides visualization around physical connectivity between various discovered interconnected devices. Multiple links displayed between nodes use line bending to avoid hidden trunks in the topology.

You can use the Topology View to zoom in or zoom out of a site to a group of devices and a group of devices to a site. In the Topology View, you can also double-click a site

or a zone to view the devices in a site. You can also see the connectivity between a device and its immediate neighbors, alarms details, and so on.

Network topology also provides visualization around physical connectivity between various discovered interconnected devices. You can move the topology map by holding down the left mouse button, dragging the mouse to another point, and letting go of the mouse.

**Related
Documentation**

- [Monitoring the Topology of Network Elements Managed by CSD-Topology Overview on page 301](#)
- [Specifying Topology Preferences on page 128](#)
- [CSD-Topology Topology Map Window Overview on page 304](#)
- [Working with the Graphical Image in the Topology View Window on page 306](#)

Monitoring the Topology of Network Elements Managed by CSD-Topology Overview

Connectivity Services Director enables you to monitor the network elements, such as devices and links, that are configured, administered, and maintained using CSD-Topology. The CSD-Topology enables granular configuration and control of IP and MPLS flows in large service provider and enterprise networks. By establishing a connection between the CSD-Topology, which is a topology server from the perspective of Connectivity Services Director, and the server on which Connectivity Services Director is running, a topological network view or map is presented that enables you to visualize label-switched paths (LSPs), links, and services for monitoring and debugging network faults and traffic outages in IP and MPLS networks. Fault, configuration, accounting, performance, and security (FCAPS) is an explicit model that is used to achieve the operational objectives of network management. Connectivity Services Director offers an effective management system for a complete FCAPS functionality.

To compute optimal paths through the network, the CSD-Topology requires a consolidated view of the network topology. The Topology View of the network includes the nodes, links, and their attributes (metric, link utilization bandwidth, and so forth) that form the network topology. Therefore, any router CLI configuration changes to interior gateway protocol (IGP) metric, Resource Reservation Protocol (RSVP) bandwidth, Priority/Hold values, and so forth are instantly available from the Topology View of Connectivity Services Director.

Without the need to traverse to the CSD-Topology GUI, you can use the Topology View from within the Connectivity Services Director GUI to obtain a global and expansive view of the network state for monitoring, management, and proactive planning. In the CSD-Topology, a Path Computation Client (PCC) is a client application that requests the Path Computation Element (PCE) to perform path computations for the PCC's external label-switched paths (LSPs). The Path Computation Element Protocol (PCEP) enables communication between a PCC and the CSD-Topology to learn about the network and LSP path state and communicate with the PCCs. By providing a view of the global network state and bandwidth demand in the network, the CSD-Topology is able

to compute optimal paths and provide the attributes that the PCC uses to resignal the LSPs.

You can also sort and classify the devices, LSPs, or services of interest and applicability for your network environment to diagnose the traffic-handling capacity, performance, and operating efficiency of the paths through which packets traverse through the circuit managed by the CSD-Topology.

You can also view the optical links configured on the optical interfaces of devices, such as PTX Series routers, on the topology map. You can sort and filter the optical links to be displayed on the topology map for easier and optimal monitoring. Only PTX3000 routers are currently supported for display on the topology map, which can contain integrated photonic line cards (IPLCs) that work in conjunction with optical inline amplifiers (optical ILAs).

Related Documentation

- [Specifying Topology Preferences on page 128](#)
- [CSD-Topology Topology Map Window Overview on page 304](#)
- [Working with the Graphical Image in the Topology View Window on page 306](#)

Specifying Topology Preferences

You must first configure the communication and authentication settings between the CSD-Topology system and the Connectivity Services Director server by using the Preferences page before you can view the topology, which is a pictorial representation of the baseline network that shows the sites, nodes, interconnecting links, label-switched paths (LSPs) configured over pseudowire links, and services. The settings that you specify on the Preferences page establish the connection between the system on which the Connectivity Services Director application is running and the CSD-Topology server. The CSD-Topology server runs on a virtual machine (CSD-Topology VM), which works in conjunction with Junos OS running on another virtual machine (JunosVM), to use routing protocols to communicate with the network and dynamically learn the network topology. You must configure the Connectivity Services Director application with the IP address of the CSD-Topology server and the login credentials to access the CSD-Topology system. If you do not configure the connection between the CSD-Topology and Connectivity Services Director servers when you navigate to the Topology View, a message is displayed stating that you must first set up the connection before you can view the topology map that shows the interconnections among devices.

To specify topology preferences on the Connectivity Services Director server:

1. From the Junos Space user interface, click the **System** icon on the Connectivity Services Director banner.

The options that you can configure in System mode are displayed on a drop-down menu.

2. Select **Preferences** from the drop-down menu to open the Preferences page.

The Preferences page opens with User Preferences as the default tab.

3. Click the **Topology** tab to configure topology preference settings.

The settings that you can configure on the Topology tab are displayed.

4. In the L2 Topology Settings section, do the following:

- a. In the Deleted Link Retention Period (Days) field, drag the slider to the right or left to specify a retention period for the deleted links in the Topology View.

By default, the deleted links are retained for one day. Drag the slider to the leftmost end of the line to specify the period for which deleted links must be preserved as one day. Drag the slider to the rightmost end of the line to specify the period for which deleted links must be preserved as 365 days or a year, which is the longest duration for which deleted links are preserved.

- b. Select the **Disable Autoupdate of Topology** check box to disable the automatic updates to the topology and, instead, enable the topology updates to be manually triggered by the user.

By default, automatic updates to the topology are disabled.

5. In the L3 Topology Settings section, do the following:

- a. Select the **Use PCEP** check box to use the Path Computation Element Protocol (PCEP) for discovery of LSPs. PCEP enables communication between a PCC and the CSD-Topology to learn about the network and LSP path state and communicate with the Path Computation Clients (PCCs). By default, this check box is not selected.

If you do not enable this option to use PCEP for discovery of LSPs, Connectivity Services Director discovers the LSPs by parsing the configuration statements and operational command outputs of the devices that it manages.

- b. In the Topology Server field, specify the topology server IP address, which is the IP address of the system on which the CSD-Topology application is running.

- c. In the UserName and Password fields, specify the username and password of the user to allow the Connectivity Services Director to connect to the topology server.

- d. Click **Validate** beside the Password field, which triggers a task to examine and verify the entered credentials for connecting to the CSD-Topology server.

A dialog box is displayed to indicate whether the specified credentials are valid or not.

- e. Click **OK** to close the dialog box. If the login credentials for communicating with the CSD-Topology are invalid, correct the username and password values and revalidate them.
- f. In the Refresh Topology Interval (Days) field, drag the slider right or left to specify the frequency in number of days at which the Layer 3 topology must be refreshed and displayed in the Topology View.

By default, the topology is refreshed once every day. Drag the slider to the leftmost end of the line to disable the refresh of the topology. Drag the slider to the rightmost end of the line to enable the refresh of topology once every 365 days or a year, which is the largest frequency you can specify for the refresh setting.

6. Click **OK** to save the settings.

You are prompted to confirm the changes you made to topology preferences.

7. Click **Yes** to confirm.

The Preferences page is closed. A dialog box is displayed to confirm the successful saving of topology preferences. Click **OK** to close the dialog box.

Related Documentation

- [Monitoring the Topology of Network Elements Managed by CSD-Topology Overview on page 301](#)
- [CSD-Topology Topology Map Window Overview on page 304](#)
- [Working with the Graphical Image in the Topology View Window on page 306](#)

CSD-Topology Topology Map Window Overview

As a network administrator, you must have a clear understanding of the various networking devices in your network, their physical locations, and how these devices are interconnected in your network. Connectivity between devices and their association with their locations provide the foundation for rendering topology in a complete manner. Connectivity Services Director enables you to monitor the devices that are managed by the CSD-Topology, besides offering a centralized view of the connectivity. The CSD-Topology topology map represents the interconnection between various devices in your network, which are managed by Junos Space Connectivity Services Director, based on their connectivity to and association with their physical surroundings. This information is useful for debugging, troubleshooting, planning, and executing administrative actions.

Before you can view the topology map, which is a pictorial representation of the baseline network that shows the sites, nodes, interconnecting links, label-switched paths (LSPs) configured over pseudowire links, and services, you must establish the connection between the system on which the Connectivity Services Director application is running and the CSD-Topology server. After you select **Topology View** from the View selector in Build mode, the topology (map) window is the main work area for any live network or network model you load into the system. The topology window is shown in [Figure 23 on page 305](#).

Multiple links displayed between nodes use *line bending* to avoid hidden trunks in the topology. The topology map enables expandable and collapsible views, which is useful when several nodes or devices are present in groups. Line bending refers to multiple parallel connector lines among devices displayed as curves to avoid overlapping between the lines.

On the topology map, devices or nodes are present in an ungrouped manner or are grouped based on the configured custom groups or sites. Sites represent a geographical region, such as a zone or a general area, within which devices are located. Different devices in a site are interconnected by links and LSPs. Services are configured on the different devices in a site. You can view the interconnection among sites, devices, links, LSPs, and services on the topology map.



NOTE: LSP names that are not unique in the network are not displayed on the topology map.



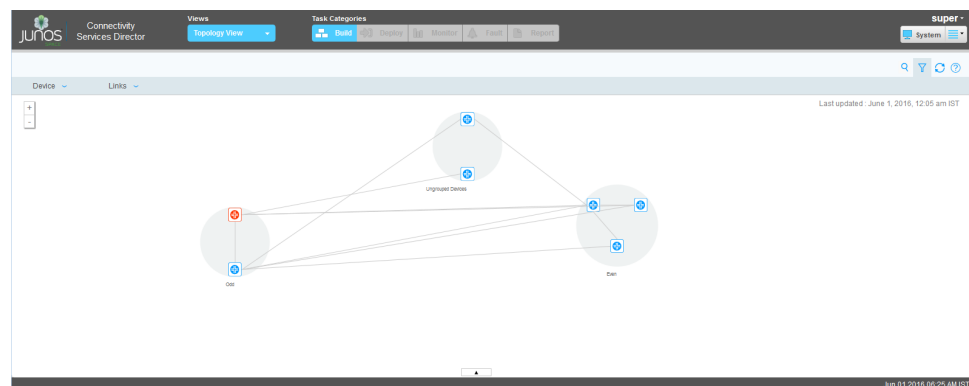
NOTE: You cannot view node locations by their geographic coordinates on the world map using latitude and longitude or automatic layouts on the Connectivity Services Director GUI.

The topology window displays important link and node properties. Links are color coded according to utilization. Alternatively, you can view links by other properties such as trunk type, protocols, coloring, status, and area. Nodes are color coded by symbols, icons, or vendor types.

Path information can be displayed in the topology window. The path function displays detailed path information between any two nodes found in the network based on factors such as the routing method used, reserved and actual bandwidth allocation, link distance, or oversubscription.

Figure 23 on page 305 displays the topology map window.

Figure 23: Topology Map Window



The topology window contains the following main components:

Filter dialog box (a funnel symbol)—For sorting and changing the settings of the Topology View

Search (magnifying glass icon)—For specifying the search criteria for filtering and viewing relevant data

Plus sign—For zooming in to the topology map for a detailed view of the elements on the map

Minus sign—For zooming out of the topology map for a high-level view of the entire map

Pictorial representation of the network on the upper portion of the page—For displaying the network

The upper portion of the right pane, which shows the topology map, is the middle portion of the topology window. In this area, you can double-click the zones that are displayed to expand and display the devices contained in that zone. The pop-up menu is accessed by right-clicking in the center pane that shows the topology map. Right-click a node, link, or group on the map to display a pop-up menu for that element.

Tables on the lower portion of the page—For viewing detailed information about devices, links, LSPs, and services configured for the network topology

Downward arrow at the bottom of the page—For hiding the table that displays information about devices, links, and LSPs, and for displaying the topology map in the entire canvas

Zoom in and zoom out—For zooming in and out by using the mouse scroll wheel for a detailed or high-level representation of the topology map

Moving the map—For dragging the map around by holding down the left mouse button

**Related
Documentation**

- [Monitoring the Topology of Network Elements Managed by CSD-Topology Overview on page 301](#)
- [Specifying Topology Preferences on page 128](#)
- [Working with the Graphical Image in the Topology View Window on page 306](#)

Working with the Graphical Image in the Topology View Window

In the Topology View of Build mode, the topology (map) window shown is the main work area for any live network or network model you load into the system. Multiple links displayed between nodes use line bending to avoid hidden trunks in the topology. The topology incorporates node aggregation collapsible views. You can also view node locations by their geographic coordinates on the world map using latitude and longitude or automatic layouts in the Topology View of Build mode.

The Topology View window displays important link and node properties, and also the devices contained in sites. Links interconnecting the devices are color coded according to utilization. Alternatively, you can view links by other properties such as trunk type, protocols, coloring, status, and area. Nodes are color-coded by symbols, icons, or vendor types.

Path information can be displayed in the Topology View window. The path function displays detailed path information between any two nodes found in the network based on factors such as routing method used, reserved and actual bandwidth allocation, link distance, or oversubscription.

The Topology View is a graphical representation of the baseline network.

- When the cursor is positioned over a network element in the Topology View, a description of the network element is displayed above each device.
- Double-click an element icon to collapse the devices or network elements and view the entire site or zone as an icon.
- Right-click an element to view more options for that element.
- Hold the left mouse button to drag the map around.
- Use the mouse scroll wheel to zoom in and out of the map.

Right-clicking on the map area displays a pop-up menu for more functions. You can move the map by holding down the left mouse button and dragging. You can zoom in and out by using the mouse scroll wheel.

In the Topology View, zones or sites are displayed as circular discs with devices when they are expanded or as small group symbols when they are collapsed. Devices or nodes are displayed within the appropriate zones as squares with the device icons. Links are displayed as gray solid connector lines. LSPs are displayed as color-coded solid connector lines. Services that are configured on nodes are displayed as dotted connector lines.



NOTE: LSP names that are not unique in the network are not displayed in the Topology View.

There are several ways to select nodes and links in the Topology View.

- Press Ctrl-click or Shift-click nodes and links.
- Right-click a node and use the Select options.
- Right-click a link and use the Select options.
- Click the plus sign to zoom in and the minus sign to zoom out of the Topology View.

When moving nodes on the map area, you are changing the graphical coordinates rather than the geographical coordinates. Graphical coordinates are the positions of the nodes in the Topology View window. Geographical coordinates are positions of the nodes according to actual physical locations (for example, latitude and longitude).

You can perform the following tasks with the View Topology page:

- [Filtering Devices, LSPs, and Services for Sorting and Segregating the Topology View on page 313](#)
- [Viewing Device Details of a CSD-Topology for Examining Traffic Transmission on page 316](#)
- [Viewing LSP Details of a CSD-Topology for Analyzing Network Changes on page 318](#)
- [Viewing Link Details of a CSD-Topology for Determining the Operational Status on page 321](#)
- [Viewing Service Details of a CSD-Topology for Monitoring and Troubleshooting Service Parameters on page 323](#)

The Map Preferences settings are saved to each client.



NOTE:

In the CSD-Topology database, the topology information that gets saved for each network includes the following:



NOTE: By default, the graphcoordaux file is automatically saved when closing a network to avoid losing auxiliary changes made to the map, such as map legend settings. Clear this check box to disable this feature.

group file—Groupings of network devices are saved in the group file

graphcoord file—Graphical coordinates of network devices are saved in the graphcoord file

graphcoordaux file—Stores the following map settings data:

Legends—Node and link color settings, link utilization color bar settings, and line styles.

Labels—Which node or link labels are turned on and labeling preferences for the bottom bar

Background Image—Background images to use

Country Maps—Country maps to use

Groups—Which groups are collapsed and which groups are expanded

- Related Documentation**
- [Monitoring the Topology of Network Elements Managed by CSD-Topology Overview on page 301](#)
 - [Specifying Topology Preferences on page 128](#)
 - [CSD-Topology Topology Map Window Overview on page 304](#)

Expanding and Collapsing Groups by Using the Topology Map Grouping Shortcut Menu

In the Topology View displayed in Build mode on the Connectivity Services Director GUI, you can collapse any groups, thereby displaying them as small group symbols, which enables you to obtain a high-level view of large network deployments with several devices and links. You can also expand any collapsed group in the topology to display and view details of the network elements.

To expand or collapse groups displayed in the Topology View:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Topology View**.

The topology map of the sites or zones and the devices configured in each zone using the CSD-Topology is displayed on the upper portion of the page. A table with details of devices, services, links, and LSPs is displayed on the lower portion of the page.

3. Right-click a zone or a group on the upper portion of the topology window and select either of the following options from the shortcut menu:

Collapse Groups—Collapses any groups, displaying them as small group symbols with their contents hidden

Expand Groups—Expands any collapsed group in the topology. The groups are displayed as discs and the contents are visible.

- Related Documentation**
- [Filtering Links, LSPs, and Services by Using the Topology Map Node Shortcut Menu on page 310](#)
 - [Removing the Highlighted LSPs by Using the Topology Map LSPs Shortcut Menu on page 311](#)
 - [Viewing the Service Path by Using the Topology Map Service Shortcut Menu on page 312](#)

Filtering Links, LSPs, and Services by Using the Topology Map Node Shortcut Menu

In a network topology that contains a large number of links configured among devices or nodes, it might be necessary to hide some of the links to avoid a cluttered view of multiple connector lines and display only the links that are of relevance for your network administration tasks. Also, you might need to filter LSPs and services for a particular device or node to selectively display only the LSPs and services configured for that device or node. You can obtain such a restricted set of necessary links, LSPs, and services by using the shortcut menu for each device or node.

To obtain a filtered display of LSPs, links, and services for a particular node in the Topology View:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Topology View**.

The topology map of the sites or zones and the devices configured in each zone using the CSD-Topology is displayed on the upper portion of the page. A table with details of devices, services, links, and LSPs is displayed on the lower portion of the page.

3. Select the **Devices** tab on the lower portion of the page.

The configured device details are displayed in a table.

4. Select the check boxes beside the devices that you want to view on the topology map.

The selected devices in the corresponding zones or custom groups are displayed on the topology map.

5. Mouse over a node icon or set of nodes and right-click to display a menu.

When you mouse over a device or a node, the name of the device or node is displayed as a tooltip.

The following options are available on the shortcut menu when you right-click each device or node:

Select Device—Highlights the device to indicate that it has been selected among other nodes displayed in the Topology View

Show Links—Displays the current route and the defined routes (for example, primary and backup) of the given tunnel in the Topology View. If multiple tunnels are selected, their primary paths are highlighted in the Topology View, and the tunnel currently selected in the path window is highlighted with a different color.

Hide Links—Removes the connector lines that are displayed to signify the links from the selected or source device to destination pairs of all tunnels on the topology map

Filters > Filter LSPs—Displays the LSPs that match the filter criteria that you specified for LSPs, such as whether LSPs that are up or down must be displayed, and whether delegated LSPs, CSD-Topology-initiated or PCEP-initiated LSPs, or router-initiated or PCC-initiated LSPs must be displayed.

Filters > Filter Services—Displays the services that match the filter criteria that you specified for services, such as whether point-to-point, Layer 3 VPN, or VPLS services must be displayed

Related Documentation

- [Expanding and Collapsing Groups by Using the Topology Map Grouping Shortcut Menu on page 309](#)
- [Removing the Highlighted LSPs by Using the Topology Map LSPs Shortcut Menu on page 311](#)
- [Viewing the Service Path by Using the Topology Map Service Shortcut Menu on page 312](#)

Removing the Highlighted LSPs by Using the Topology Map LSPs Shortcut Menu

You can remove the highlighted LSPs from being displayed in the Topology View in network scenarios in which several LSPs are configured for a service to prevent the topology map from being cluttered with a large set of connector lines. You might require to specifically focus on some of the LSPs that you want to troubleshoot and diagnose for faults and traffic disruptions.



NOTE: In the Topology View displayed in Build mode on the Connectivity Services Director GUI, mouse over an LSP and right-click to display a menu. When you mouse over an LSP, the name of the link is displayed as a tooltip.

To remove the highlighted LSPs from display in the Topology View:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Topology View**.

The topology map of the sites or zones and the devices configured in each zone using the CSD-Topology is displayed on the upper portion of the page. A table with details of devices, services, links, and LSPs is displayed on the lower portion of the page.

3. Select the **LSPs** tab on the lower portion of the page.

The configured LSP details are displayed in a table.

4. Select the check boxes beside the LSPs that you want to view on the topology map.

The selected LSPs are displayed as different color-coded lines on the map.

5. Mouse over an LSP and right-click to display a menu.

When you mouse over an LSP, the name of the link is displayed as a tooltip. The following option is available on the shortcut menu when you right-click each LSP:

Remove LSP Highlight > LSPName—Removes the selected LSPs displayed on the shortcut menu from being highlighted in the Topology View. This option is useful when a service is configured with multiple LSPs and you do not want the LSPs to be highlighted and shown.

**Related
Documentation**

- [Expanding and Collapsing Groups by Using the Topology Map Grouping Shortcut Menu on page 309](#)
- [Filtering Links, LSPs, and Services by Using the Topology Map Node Shortcut Menu on page 310](#)
- [Viewing the Service Path by Using the Topology Map Service Shortcut Menu on page 312](#)

Viewing the Service Path by Using the Topology Map Service Shortcut Menu

A service path is a connector that displays the LSP configured for a particular service on a device in the Topology View. Because of a large number of services that might be configured among devices in a topology, it is required to distinguish only the LSPs or service paths that connect from one device to another device. In such a case, you can select a service displayed in the Topology View and choose to hide or show the service path for analysis purposes.



NOTE: In the Topology View displayed in Build mode on the Connectivity Services Director GUI, mouse over a service and right-click to display a menu. When you mouse over a service, the name of the service is displayed as a tooltip.

To hide or display a service path associated with a device in the Topology View:

1. Select **Topology View** from the Views list in the Connectivity Services Director application.

The topology map of the sites or zones and the devices configured in each zone using the CSD-Topology is displayed.

2. Select the **Service** tab on the lower portion of the page.

The service details are displayed in a table.

3. Select the check box beside a service configured for devices in the topology.

The service paths that traverse the different devices on which the selected service is configured are displayed as highlighted lines in the Topology View.

4. Right-click a service path and select one of the following options available on the shortcut menu:

Hide Service Path—Removes the LSPs highlighted in the Topology View.

Retrieve Service Path—Retrieves an LSP associated with the service path.

Show Service Path—Displays the LSPs associated with the service.

**Related
Documentation**

- [Expanding and Collapsing Groups by Using the Topology Map Grouping Shortcut Menu on page 309](#)
- [Filtering Links, LSPs, and Services by Using the Topology Map Node Shortcut Menu on page 310](#)
- [Removing the Highlighted LSPs by Using the Topology Map LSPs Shortcut Menu on page 311](#)

Filtering Devices, LSPs, and Services for Sorting and Segregating the Topology View

In network environments that contain several thousands of devices, it might be helpful to sort and segregate the devices and their associated LSPs and links, based on certain filter conditions. You can specify the criteria that must be matched for the network elements shown in the Topology View. For example, you can specify that only devices that are up or only LSPs for devices on which Layer 3 VPN services are defined must be displayed.

To specify the filter criteria for segregating the displayed elements in the Topology View:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Topology View**.

The topology map of the sites or zones and the devices configured in each zone using the CSD-Topology is displayed on the upper portion of the page. A table with details of devices, services, links, and LSPs is displayed on the lower portion of the page.

3. Click the **Filter** icon (the funnel symbol) at the top-left corner of the Topology View window.

The Filter dialog box is displayed.

4. On the Devices tab, mouse over the tab to view the drop-down menu and do the following:
 - Select **Show All**, **Up**, or **Down** from the Device Status list to display the devices that are in any state, in the up state, or in the down state respectively.
 - Select the **Show Unmanaged Devices** check box to display the unmanaged devices that are present in the links in the topology. Alternatively, clear this check box to view only the managed devices in the topology.
 - Select **Custom Group**, **OSPF Area**, or **AS Number** from the Group by list to group the devices in the topology based on the configured custom groups, OSPF area, or autonomous system (AS) number respectively.
5. On the Links tab, mouse over the tab to view the drop-down menu and do the following:
 - Select the **Show All Links** check box to display all the links originating from each node in the topology.
 - Select the **Show Optical Links** check box to display only the optical links originating from each node in the topology.
 - Select **Up** or **Down** from the Operational Status list to display links that are either active or disabled.
6. Click **Filter** to save the filter criteria.

The dialog box is closed and you are returned to the Topology View.

Related Documentation

- [Viewing Device Details of a CSD-Topology for Examining Traffic Transmission on page 316](#)
- [Viewing LSP Details of a CSD-Topology for Analyzing Network Changes on page 318](#)
- [Viewing Link Details of a CSD-Topology for Determining the Operational Status on page 321](#)
- [Viewing Service Details of a CSD-Topology for Monitoring and Troubleshooting Service Parameters on page 323](#)

Segregating the Displayed Devices by Searching the Entire Topology View

In the Topology View displayed in Build mode on the Connectivity Services Director GUI, you can enter the strings or terms that you want to use as search labels to search for any node, link, or group and filter the display. The Search box is displayed on the top-right corner of the Topology View. You can search based on only one term or criterion at a time. You can search for nodes or devices on the topology map based on router ID, hostname, management IP address, and serial number of the device. In certain network deployments, you might require a certain set of devices that match a particular subnet to be viewed for obtaining a subset of the entire topology that is of interest and relevance to you. In such cases, you can specify the IP address of the device as the search term to view only the appropriate device that matches the search term.

To specify a search criterion for classifying the displayed devices in the Topology View:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Topology View**.

The topology map of the sites or zones and the devices configured in each zone using the CSD-Topology is displayed.

3. Click the **Search** icon (magnifying glass symbol) and enter the search term in the text field that is displayed.

The Search box is displayed on the top-right corner of the Topology View. A drop-down list prompts you to select a term that matches the characters you enter in the search field. The node that matches the search term is highlighted in the Topology View.

You can search based on only one criterion at a time. You can search for nodes or devices in the Topology View based on the router ID, hostname, management IP address, and serial number of the device. Delete the search term that you entered to remove the term from the search criterion.

Resynchronizing the Topology View

You can resynchronize the topology map displayed on the Connectivity Services Director GUI, which enables the latest links information, label-switched path (LSP) details, and device states to be retrieved from the CSD-Topology application and shown in the Topology View. This resynchronization capability enables you to view the most recent synchronization of paths signaled across routed network elements. It is essential to view the latest topology information in a network that has changing traffic conditions and transmission states to be able to modify the link and LSP settings according to the deployment needs. The resynchronization functionality enables you to obtain the up-to-date topology states.

To create a job to resynchronize the topology map:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Topology View**.

The topology map of the sites or zones and the devices configured in each zone using the CSD-Topology is displayed.

3. Click the **Resynch the Topology** icon (5 o'clock symbol) to create a job to resynchronize the topology map.

A job is triggered and a pop-up dialog box displays the job ID.

4. Click **OK** to close the pop-up dialog box.

You can navigate to the Job Management page to view the status of the resynchronization job (which you can launch by clicking the **System** button on the Connectivity Services Director banner and selecting **Manage Jobs** from the Tasks pane).

**Related
Documentation**

- [Configuring PCEP on a PE Router \(from CLI\) on page 289](#)

Viewing Device Details of a CSD-Topology for Examining Traffic Transmission

You can view the details of all of the devices or nodes in a Topology View that are managed by the CSD-Topology. Node addresses for the Node A and Node Z elements define the endpoint nodes for the tunnel. Devices that are discovered as part of the topology acquisition by the CSD-Topology and are not managed devices in the Connectivity Services Director database are displayed in gray. Devices that are discovered by the CSD-Topology using BGP and MPLS and are managed devices in the Connectivity Services Director database are displayed in blue.



NOTE: Because of the way in which the link-state database (LSDB) interior gateway protocols (IGPs) represent LAN connections (in order to improve scaling), multiple entries for the same hostname might be displayed on the Devices tab of the Topology View. Similarly, multiple entries for the same hostname might be displayed on the Devices tab because of the manner in which OSPF and ISIS associate with broadcast interfaces. The pseudonodes are represented in a distinct way on the GUI. When the IGP (OSPF or ISIS) builds neighboring relationships on broadcast media (such as Ethernet), the IGP represents this deployment as a hub-and-spoke topology with all nodes in the same broadcast domain having a point-to-point connection with a pseudonode. In such instances, the traffic engineering database includes a pseudonode on each interface that is configured with the interface-type LAN (the default). If such pseudonodes are not added, the topology displays a full-mesh of point-to-point connections between all nodes in the same LAN segment (this case occurs if you manually configure the interface type as point-to-multipoint [P2MP], and manually add each neighbor). The GUI represents these pseudonodes in a way that enables you to easily see that these are not real nodes (it can represent the pseudonode as a different entity, such as a special node or a LAN segment).

To view details of devices or nodes in the Topology View:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

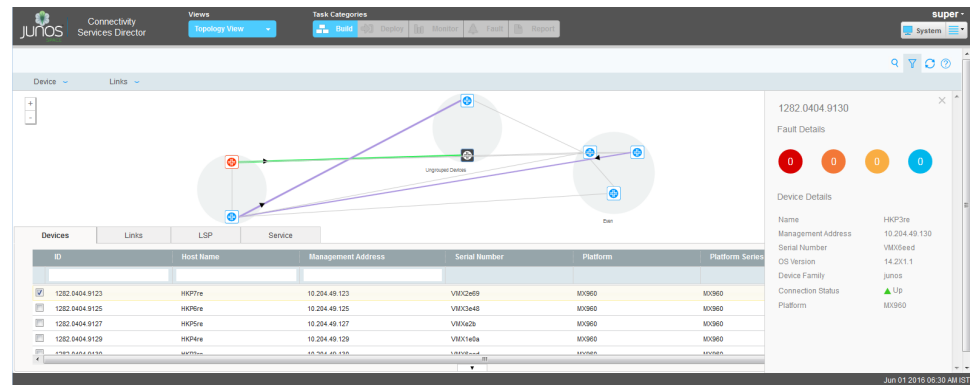
- From the View selector, select **Topology View**.

The topology map of the sites or zones and the devices configured in each zone using the CSD-Topology is displayed on the upper portion of the page. A table with details of devices, services, links, and LSPs is displayed on the lower portion of the page.

- Select the **Devices** tab on the lower portion of the page.

The device details are displayed in a table as follows (see [Figure 24 on page 317](#)):

Figure 24: Device Details in the Topology Map Window



For columns in the table that contain an empty text field displayed at the top of the table on each tab, you can enter the search criterion that you want to use for that particular column or parameter to sort and classify the display of values in the table. For parameters that you can enable or disable, you can select or clear the check boxes respectively. The page is refreshed to display the devices that match the specified criterion. The search criteria that you have entered are displayed above the first row of the table. You can click Clear All displayed beside each of the search terms to remove the previously defined search terms.

- Name—Hostname of the device. Click in the first cell in this column to enter the hostname as the criterion for filtering and displaying the devices in the table.
- Management Address—Management IP address of the node. Click in the first cell in this column to enter the management IP address as the criterion for filtering and displaying the devices in the table.
- Serial Number—Hardware serial number of the device
- Software Version—Junos OS software version and release number running on the device
- Platform—Platform type of the device, such as MX240 or MX480
- Platform Series—Device family to which the device belongs, such as MX Series for an MX240 router

Related Documentation

- [Filtering Devices, LSPs, and Services for Sorting and Segregating the Topology View on page 313](#)

- [Viewing LSP Details of a CSD-Topology for Analyzing Network Changes on page 318](#)
- [Viewing Link Details of a CSD-Topology for Determining the Operational Status on page 321](#)
- [Viewing Service Details of a CSD-Topology for Monitoring and Troubleshooting Service Parameters on page 323](#)

Viewing LSP Details of a CSD-Topology for Analyzing Network Changes

You can view the details of all the label-switched paths (LSPs) configured for devices in the Topology View that are managed by the CSD-Topology. For MPLS-enabled networks, after you configure an LSP, you should also configure a standby or secondary LSP to provide an alternate route in the event the primary route fails. The tunnel ID, from node, to node, and IP address of a secondary or standby tunnel must be identical to those of the primary tunnel.

When you expand a zone or a group in the Topology View, and select an LSP on the map, the LSP is highlighted. Different highlighting colors are used to distinguish the LSPs on the map.

To view details of LSPs in the Topology View:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

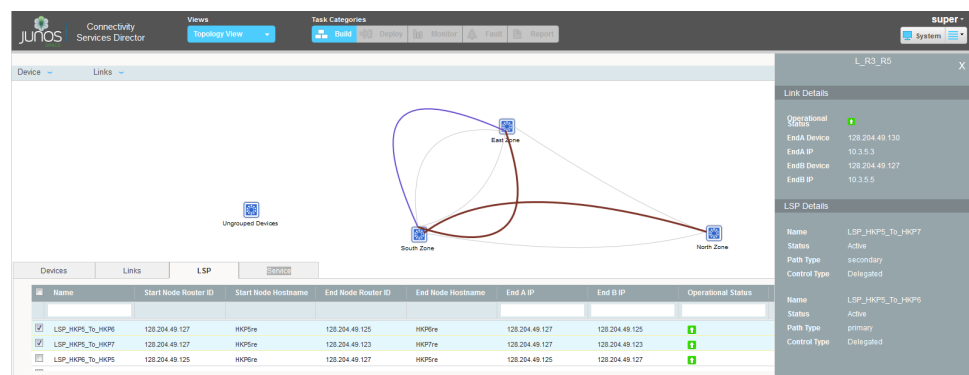
2. From the View selector, select **Topology View**.

The topology map of the sites or zones and the devices configured in each zone using the CSD-Topology is displayed.

3. Select the **LSPs** tab on the lower portion of the page.

The LSP details are displayed in a table as follows (see [Figure 25 on page 318](#)):

Figure 25: LSP Details in the Topology Map Window





NOTE: LSP names that are not unique in the network are not displayed in the Topology View.

For columns in the table that contain an empty text field displayed at the top of the table on each tab, you can enter the search criterion that you want to use for that particular column or parameter to sort and classify the display of values in the table. For parameters that you can enable or disable, you can select or clear the check boxes respectively. The page is refreshed to display the devices that match the specified criterion. The search criteria that you have entered are displayed above the first row of the table. You can click Clear All displayed beside each of the search terms to remove the previously defined search terms.

- **Name**—Name of the LSP. Click in the first cell in the Name column to enter the name of the LSP that you want to use as the filter for viewing the LSPs.
- **Start Node Router ID**—Node ID of the LSP head end. A router ID is used to uniquely identify the router within a BGP autonomous system (AS). The router ID is the IP address of the loopback interface.
- **Start Node Hostname**—Hostname of the router at the LSP head end
- **End Node Router ID**—Node ID of the LSP tail end
- **End Node Hostname**—Hostname of the router at the LSP tail end
- **End A IP**—IP address of the LSP head end. Click in the first cell in the End A IP column to enter the IP address of the head end that you want to use as the filter for viewing the LSPs.
- **End B IP**—IP address of the LSP tail end. Click in the first cell in the End B IP column to enter the IP address of the tail end that you want to use as the filter for viewing the LSPs.
- **Operational Status**—Whether the LSP is active (up) or inactive (down). Click in the first cell in the Operational Status column to select the status from the drop-down menu that you want to use as the filter for viewing the LSPs.
- **Path Type**—Whether the path is a primary path (explicit or dynamic) or a secondary path (explicit or dynamic)
- **Control Type**—Whether the LSP is router controlled or PCC initiated, CSD-Topology initiated or PCEP initiated, or CSD-Topology managed or delegated LSP. Click in the first cell in the Control Type column to specify the type of LSP from the drop-down menu that you want to use as the filter for viewing the LSPs.
- **Metric**—LSP tunnel metric
- **Setup Priority**—Setup priority supported by RSVP for the tunnel traffic



NOTE: You must assign priorities according to network policies to prevent resource poaching and LSP thrashing. The hold priority values should be lower than or equal to the setup priority value.

- Holding Priority—Hold priority supported by RSVP for the tunnel traffic



NOTE: The default is priority 07 and hold 07, which is the standard MPLS LSP definition in Junos OS. Setup priority determines whether a new LSP that preempts an existing LSP can be established. For preemption to occur, the setup priority of the new LSP must be higher than the setup priority of the existing LSP. In addition, the act of preempting the existing LSP must provide sufficient bandwidth to support the new LSP. Therefore, preemption occurs only if the new LSP can be set up successfully. You can configure each LSP with a setup priority and hold priority to provide a preemption strategy whereby a new LSP can claim resources from an existing LSP. Each LSP can claim resources from an existing LSP. Priority levels range from 0 (highest priority) through 7 (lowest priority). If traffic engineering admission control determines that there are insufficient resources available to accept a request to set up a new LSP, the setup priority is evaluated against the hold priority of the existing LSPs (per standard Junos OS behavior). An LSP with a hold priority lower than the setup priority of the new LSP can be preempted. The existing LSP is terminated to make resources available for the new LSP.

- Current Bandwidth—Bandwidth that is specified for the tunnel traffic (bandwidth applies for each direction)

4. Mouse over an LSP and click the LSP to display a menu.

When you mouse over an LSP, the name of the LSP is displayed on a pop-up menu. The following fields are displayed in the pop-up dialog box when you mouse over the LSP:

- Name—Name of the LSP. The names of all the LSPs that are configured for the particular link are displayed.
- View Details—Detailed information about the selected LSP.

Related Documentation

- [Filtering Devices, LSPs, and Services for Sorting and Segregating the Topology View on page 313](#)
- [Viewing Device Details of a CSD-Topology for Examining Traffic Transmission on page 316](#)
- [Viewing Link Details of a CSD-Topology for Determining the Operational Status on page 321](#)
- [Viewing Service Details of a CSD-Topology for Monitoring and Troubleshooting Service Parameters on page 323](#)

Viewing Link Details of a CSD-Topology for Determining the Operational Status

It is necessary to determine the operational status of links configured among devices in a topology to examine and troubleshoot data traffic loss and packet-forwarding problems. You can view the details of all the links configured for devices in the Topology View that are managed by the CSD-Topology. For explicit routing, from the Map view, click the links or nodes to define an alternate route between the source (Node A) and destination (Node Z) nodes to provide a path that is diverse from the path specified in the primary tunnel. When you schedule a maintenance event on nodes or links, the CSD-Topology routes delegated label-switched paths (LSPs) around those nodes and links that are scheduled for maintenance. After the completion of the maintenance event, delegated LSPs are reverted to optimal paths.

To view details of links in the Topology View:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

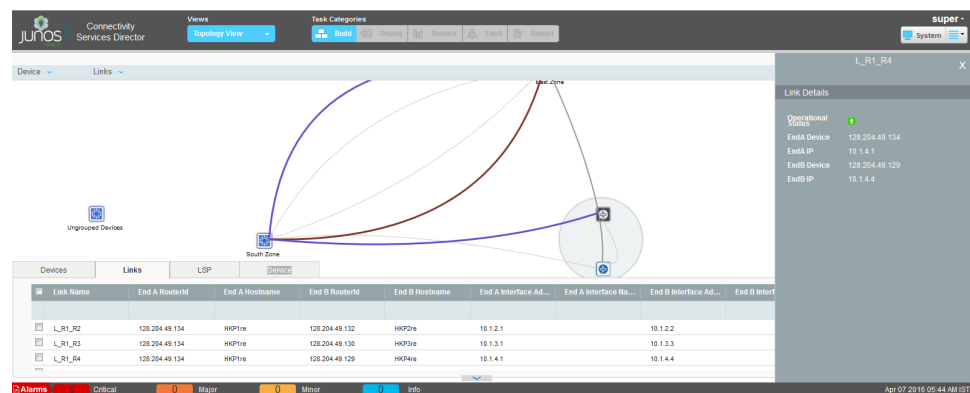
2. From the View selector, select **Topology View**.

The topology map of the sites or zones and the devices configured in each zone using the CSD-Topology is displayed on the upper portion of the page. A table with details of devices, services, links, and LSPs is displayed on the lower portion of the page.

3. Select the **Links** tab on the lower portion of the page.

The link details are displayed in a table as follows (see [Figure 26 on page 321](#)):

Figure 26: Link Details in the Topology Map Window



For columns in the table that contain an empty text field displayed at the top of the table on each tab, you can enter the search criterion that you want to use for that particular column or parameter to sort and classify the display of values in the table. For parameters that you can enable or disable, you can select or clear the check boxes respectively. The page is refreshed to display the devices that match the specified criterion. The search criteria that you have entered are displayed above the first row of the table. You can click Clear All displayed beside each of the search terms to remove the previously defined search terms.

- Link Name—Name of the configured link
- End A RouterId—Router ID of the starting node of the link. The router ID is used to uniquely identify a router and is the IP address of the loopback interface.
- End B RouterId—Router ID of the ending node of the link
- Endpoint A Hostname—Hostname of the router at the starting node of the link. Click in the first cell in the Endpoint A IP column to enter the IP address of the LSP head end that you want to use as the filter for viewing the links.
- End B Hostname—Hostname of the router at the ending node of the link. Click in the first cell in the Endpoint A IP column to enter the IP address of the LSP tail end that you want to use as the filter for viewing the links.
- End A Interface Name—Name of the interface on the router at the starting point of the link
- End B Interface Name—Name of the interface on the router at the ending point of the link
- End A Interface Address—IP address of the interface on the router at the starting point of the link
- End B Interface Address—IP address of the interface on the router at the ending point of the link
- Link Type—Whether the link is an IP link or an optical link
- Operational Status—Whether the link is active (up) or inactive (down). Click in the first cell in the Operational Status column to open the drop-down menu and select the type of operational status that you want as the filter for viewing for the links.

Related Documentation

- [Filtering Devices, LSPs, and Services for Sorting and Segregating the Topology View on page 313](#)
- [Viewing Device Details of a CSD-Topology for Examining Traffic Transmission on page 316](#)
- [Viewing LSP Details of a CSD-Topology for Analyzing Network Changes on page 318](#)
- [Viewing Service Details of a CSD-Topology for Monitoring and Troubleshooting Service Parameters on page 323](#)

Viewing Service Details of a CSD-Topology for Monitoring and Troubleshooting Service Parameters

You can view the consolidated and cumulative information pertaining to a service to examine and diagnose the deployment and fault statuses for debugging and corrective action. The overall information pertaining to the service that you can obtain from the Topology View enables you to navigate to the appropriate device or service settings page and modify the configuration parameters appropriately.

You can view the details of all the services configured for devices on a topology map that are managed by the CSD-Topology. This information display of service attributes is especially helpful if devices that are managed by the CSD-Topology are also added to the Connectivity Services Director database for administration and monitoring. You can view the topology map based on the services and other filter conditions, such as their deployment states, functional audit statuses, or customer name. Point-to-point, VPLS, and Layer 3 VPN services defined on devices can be viewed.

To view details of services on a topology map:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

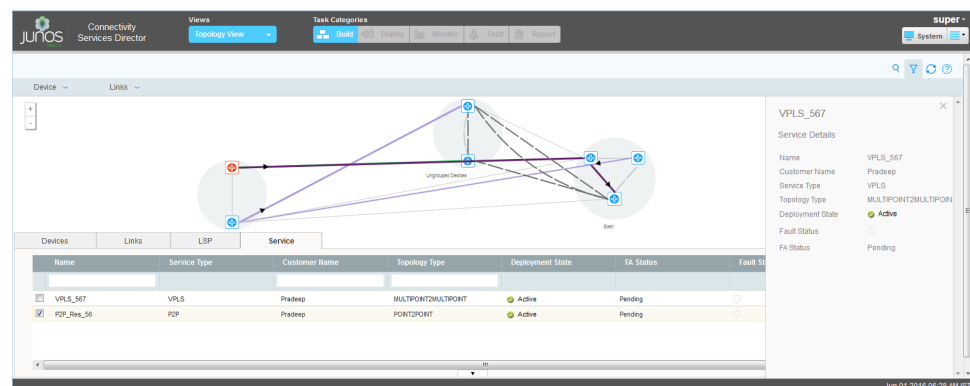
2. From the View selector, select **Topology View**.

The topology map of the sites or zones and the devices configured in each zone using the CSD-Topology is displayed on the upper portion of the page. A table with details of devices, services, links, and LSPs is displayed on the lower portion of the page.

3. Select the **Services** tab on the lower portion of the page.

The service details are displayed in a table as follows (see [Figure 27 on page 323](#)):

Figure 27: Service Details in the Topology Map Window



For columns in the table that contain an empty text field displayed at the top of the table on each tab, you can enter the search criterion that you want to use for that particular column or parameter to sort and classify the display of values in the table. For parameters that you can enable or disable, you can select or clear the check boxes respectively. The page is refreshed to display the devices that match the specified criterion. The search criteria that you have entered are displayed above the first row of the table. You can click Clear All displayed beside each of the search terms to remove the previously defined search terms.

- **Name**—Name of the service configured for a device. Click in the first cell in the Name column to enter the service name that you want to use as the filter for viewing the services.
- **Service Type**—Type of service, such as point-to-point, Layer 3 VPN, or VPLS. Click in the first cell in the Service Type column to select the type of service from the displayed drop-down menu that you want to use as the filter for viewing the services.
- **Customer Name**—Name of the customer associated with the service. Click in the first cell in the Customer Name column to enter the customer name that you want to use as the filter for viewing the services.
- **Topology Type**—Design of the network, such as a point-to-point topology, point-to-multipoint or hub-and-spoke format, and multipoint-to-multipoint or full-mesh format. Click in the first cell in the Topology Type column to select the type of topology from the displayed drop-down menu that you want to use as the filter for viewing the services. The following options are displayed on the drop-down menu:
 - POINT2POINT—Point-to-point topology type
 - POINT2MULTIPOINT—Point-to-multipoint topology type
 - MULTIPOINT2MULTIPOINT—Multipoint-to-multipoint topology type for VPLS services
 - FULLMESH—Full-mesh topology type for Layer 3 VPN services
 - HUBSPOKE1INTF—Hub-and-spoke topology type with one interface
 - HUBSPOKE2INTF—Hub-and-spoke topology type with two interfaces
- **Deployment State**—Status of deployment, such as whether the deployment is successful, failed, or pending. Click in the first cell in the Deployment State column to select the deployment status from the displayed drop-down menu that you want to use as the filter for viewing the services. The following values are displayed on the drop-down menu:
 - Deployed—The service is deployed and is in an active state (enabled) or inactive state (disabled).
 - Deployment-Pending—The service has not yet been deployed.
 - Failed Deploy—Attempt to modify the service failed.

- **Fault Status**—Fault management status of the service, such as whether a service fault is active on a device (red bell icon) or the service fault that was generated for the device has been cleared (green bell icon)
- **FA Status**—Whether the link is active (up) or inactive (down). Click in the first cell under the FA Status column to select the functional audit status from the displayed drop-down menu that you want to use as the filter for viewing the services. The following values are displayed on the drop-down menu:
 - **Pending**—Functional audit operation is pending to be performed for the service.
 - **Failed**—Functional audit operation has failed for the service.
 - **Up**—Functional audit completed successfully for the service.
- **Last Updated Date**—Date and time that the information for the service was last modified

**Related
Documentation**

- [Filtering Devices, LSPs, and Services for Sorting and Segregating the Topology View on page 313](#)
- [Viewing Device Details of a CSD-Topology for Examining Traffic Transmission on page 316](#)
- [Viewing LSP Details of a CSD-Topology for Analyzing Network Changes on page 318](#)
- [Viewing Link Details of a CSD-Topology for Determining the Operational Status on page 321](#)

Viewing Topology Map Group Details in a Pop-Up Dialog Box

In the Topology View of Build mode, the upper portion of the page, which shows the topology map, is the main display area. In this area, you can double-click the zones that are displayed to expand and display the devices contained in that zone. Mouse over a node, link, or group on the map to display a pop-up menu for that element. Mouse over a group to view the group information. When you mouse over a group, the name of the group is displayed on a pop-up menu.

In a large network that comprises devices or nodes situated in several groups, which denote the geographical locations or zones, it might be essential to view the details of a particular group that is of relevance for your network management needs. In such cases, apart from viewing the number of devices that are associated with a group, you can also view information on the alarms generated for these devices. For example, you might want to modify the grouping of devices by transferring devices to a different group or zone for better load-balancing of traffic or optimizing packet flows. Also, if you find that a particular group has recorded a large number of critical or major alarms, you can then navigate to the Alarm Detail widget in Monitor mode or the appropriate device settings page to correct and modify the attributes or diagnose the problems that might be generating the alarms.



NOTE: Right-clicking the map area displays a pop-up menu for more functions. You can move the map by holding down and dragging the left mouse button. You can zoom in and out by using the mouse scroll wheel. Double-click an element icon to collapse the devices or network elements and view the entire site or zone as an icon.

To view group details in a pop-up dialog box:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Topology View**.

The topology map of the sites or zones and the devices configured in each zone using the CSD-Topology is displayed on the upper portion of the page. A table with details of devices, services, links, and LSPs is displayed on the lower portion of the page.

3. In the graphical representation of the topology displayed, select the group for which you want to view the device details by double-clicking the group.

The group is expanded and the devices contained in the group are displayed within a circle.

Devices that are discovered as part of the topology acquisition by the CSD-Topology and are not managed devices in the Connectivity Services Director database are displayed in gray. Devices that are discovered by the CSD-Topology using BGP and

MPLS and are managed devices in the Connectivity Services Director database are displayed in blue.

4. Mouse over the group for which you want to view the configuration settings.

The group pop-up menu is displayed with the number of devices contained in the group.

5. Click the **View Details** link from the pop-up menu.

The Group Details pop-up dialog box is displayed, which displays the name of the group and the number of devices contained in the group. Also, the Fault Details field displays four colored circles—red, orange, yellow, and blue—to signify the four alarm severity levels as follows:

- Critical (red)—A critical condition exists for a device in the zone; immediate action is necessary.
- Major (orange)—A major error has occurred for a device in the zone; escalate or notify as necessary.
- Minor (yellow)—A minor error has occurred for a device in the zone; notify or monitor the condition.
- Info (blue)—An informational message has been generated for a device in the zone; no action is necessary. Informational alarms do not necessarily indicate an error. It could indicate that a device or entity has changed state.

6. Click the **Close** icon at the top-right corner of the pop-up dialog box to return to the topology map.

**Related
Documentation**

- [Viewing Topology Map Device Details in a Pop-Up Dialog Box on page 328](#)
- [Viewing Topology Map Link Details in a Pop-Up Dialog Box on page 330](#)
- [Viewing Topology Map LSP Details in a Pop-Up Dialog Box on page 332](#)
- [Viewing Topology Map Service Details in a Pop-Up Dialog Box on page 334](#)

Viewing Topology Map Device Details in a Pop-Up Dialog Box

In the Topology View of Build mode, the upper portion of the page shows the topology map, which is the main display area. In this area, you can double-click the zones that are displayed to expand and display the devices contained in that zone. The pop-up menu is accessed by double-clicking the group in the center pane that shows the topology map. Mouse over a device on the map to display a pop-up menu for that device.

In a geographically diverse network with several groups or zones, after you expand and view a particular group, you can also view the salient configuration details of devices contained in that group. Both the devices that are managed by Connectivity Services Director and the devices that are not managed by Connectivity Services Director, but have been only acquired as part of the CSD-Topology topology acquisition, are displayed in the expanded groups on the topology map. You can view important, high-level device details such as the Junos OS release that is running on a particular device for determining any Junos OS image upgrade as necessary and the device status. If you identify the status of the device to be down, you can then view the device configuration settings and take any corrective action.



NOTE: Right-clicking the map area displays a pop-up menu for more functions. You can move the map by holding down and dragging the left mouse button. You can zoom in and out by using the mouse scroll wheel. Double-click an element icon to collapse the devices or network elements and view the entire site or zone as an icon.

Devices that are discovered as part of the topology acquisition by the CSD-Topology and are not managed devices in the Connectivity Services Director database are displayed in gray. Devices that are discovered by the CSD-Topology using BGP and MPLS and are managed devices in the Connectivity Services Director database are displayed in blue.

Mouse over a node icon or set of nodes and double-click to display a menu. When you mouse over a device or a node, the name of the device is displayed on a pop-up menu. The following fields are displayed in the pop-up dialog box when you mouse over the device or node:

- Host Name—Hostname of the selected device or node
- IP Address—IP address of the selected device or node
- Device Status—Status of the selected device or node, such as Up or Down
- View Details—Detailed information about the selected device or node. Click the link in **View Details** to open a pop-up dialog box that displays these details.

When you select a particular device by expanding a group or zone and clicking the device, the device icon is highlighted and displayed.

To view device details in a pop-up dialog box:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Topology View**.

The topology map of the sites or zones and the devices configured in each zone using the CSD-Topology is displayed.

3. In the graphical representation of the topology displayed on the right pane, select the group for which you want to view the device details by double-clicking the group.

The group is expanded and the devices contained in the group are displayed within a circle.

4. Mouse over the device or node for which you want to view the configuration settings.

The device pop-up menu is displayed.

5. Click the **View Details** link from the pop-up menu.

The Device Details dialog box is displayed on the right pane, which contains the following fields:

- Host Name—Hostname of the device or node
 - Serial Number—Serial number of the chassis component. The serial number of the backplane is also the serial number of the router chassis. Use this serial number when you need to contact Juniper Networks Customer Support about the router or switch chassis.
 - OS Version—Operating system firmware version running on the device or node
 - Device Family—Device family of the device or node, such as JUNOS for MX Series routers
6. Click the **Close** icon at the top-right corner of the pop-up dialog box to return to the topology map.

**Related
Documentation**

- [Viewing Topology Map Group Details in a Pop-Up Dialog Box on page 326](#)
- [Viewing Topology Map Link Details in a Pop-Up Dialog Box on page 330](#)
- [Viewing Topology Map LSP Details in a Pop-Up Dialog Box on page 332](#)
- [Viewing Topology Map Service Details in a Pop-Up Dialog Box on page 334](#)

Viewing Topology Map Link Details in a Pop-Up Dialog Box

In the Topology View of Build mode, the upper portion of the page shows the topology map, which is the main display area. In this area, you can click or right-click the connecting lines, which represent the links that transmit traffic between devices, to view the link details. The pop-up menu is accessed by double-clicking in the center pane that shows the topology map. Mouse over a link on the map to display a pop-up menu for that link.

For a specific zone and a set of devices in that zone, you can view the links connecting the devices. You can view the link details, such as the node identifier and the node IP address of the head end or originating router and the tail end or the destination router. These link details are useful for diagnosing and troubleshooting any link problems that cause traffic drops or loss in transmission of packets.



NOTE: Right-clicking the map area displays a pop-up menu for more functions. You can move the map by holding down and dragging the left mouse button. You can zoom in and out by using the mouse scroll wheel. Double-click an element icon to collapse the devices or network elements and view the entire site or zone as an icon.

To view link details in a pop-up dialog box:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Topology View**.

The topology map of the sites or zones and the devices configured in each zone using the CSD-Topology is displayed.

3. In the graphical representation of the topology displayed on the page, select the link by clicking the link or right-clicking the link for which you want to view details.

The link is highlighted and displayed as a colored line.

4. Mouse over a link and click the link to display a menu.

When you mouse over a link, the name of the link is displayed on a pop-up menu. The following fields are displayed in the pop-up dialog box when you mouse over the link:

- Operational Status—Status of the link, such as Up or Down
- View Details—Detailed information about the selected link. Click the link in **View Details** to open a pop-up dialog box that displays these details.

5. Click the **View Details** link from the pop-up menu.

The Link Details pop-up dialog box is displayed on the right pane. The link details are displayed in a table as follows:

- End A Device—Node ID of the LSP head end
 - End B Device—Node ID of the LSP tail end
 - End A IP—IP address of the LSP head end
 - End B IP—IP address of the LSP tail end
 - Operational Status—Whether the link is active (up) or inactive (down)
6. Click the **Close** icon at the top-right corner of the pop-up dialog box to return to the topology map.

**Related
Documentation**

- [Viewing Topology Map Group Details in a Pop-Up Dialog Box on page 326](#)
- [Viewing Topology Map Device Details in a Pop-Up Dialog Box on page 328](#)
- [Viewing Topology Map LSP Details in a Pop-Up Dialog Box on page 332](#)
- [Viewing Topology Map Service Details in a Pop-Up Dialog Box on page 334](#)

Viewing Topology Map LSP Details in a Pop-Up Dialog Box

In the Topology View of Build mode, the upper portion of the page shows the topology map, which is the main display area. In this area, you can click or right-click the connecting lines, which represent the label-switched paths (LSPs) configured over pseudowire links, that transmit traffic between devices, to view the LSP details. Mouse over an LSP on the map to display a pop-up menu for that LSP.

For a specific zone and a set of devices in that zone, you can view the links and LSPs connecting the devices. When you view the LSP details, the link details are also displayed. You can determine the path type of the LSP—primary or backup. You can then decide whether you want to automatically configure a tunnel to have its secondary or standby paths diverse from its primary path. You can also design two different tunnels to have diverse primary paths, and set the primary and backup paths to perform explicit routing or dynamic routing. You can also verify the type of LSP—CSD-Topology managed (Delegated) LSP, path computation element protocol (PCEP) initiated LSP, or path computation client (PCC) or router initiated LSP—and change the type of delegation to be performed for the LSP.



NOTE: Right-clicking the map area displays a pop-up menu for more functions. You can move the map by holding down and dragging the left mouse button. You can zoom in and out by using the mouse scroll wheel. Double-click an element icon to collapse the devices or network elements and view the entire site or zone as an icon.

Mouse over an LSP and click the link to display a menu. When you mouse over an LSP, the name of the LSP is displayed on a pop-up menu. The following fields are displayed in the pop-up dialog box when you mouse over the LSP:

- **Name**—Name of the configured LSP. The names of all LSPs configured for a particular link are displayed.
- **View Details**—Detailed information about the selected LSP. Click the link in **View Details** to open a pop-up dialog box that displays these details.

To view LSP details in a pop-up dialog box:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Topology View**.

The topology map of the sites or zones and the devices configured in each zone using the CSD-Topology is displayed.

3. Select the **LSPs** tab on the lower portion of the page.

The configured LSP details are displayed in a table.

4. Select the check boxes beside the LSPs that you want to view on the topology map.

The selected LSPs are displayed as different color-coded lines on the map.

5. In the graphical representation of the topology displayed on the upper portion of the page, select the LSP by clicking the LSP or right-clicking the LSP for which you want to view details.

The LSP is highlighted and displayed as a colored line.

6. Click the **View Details** link from the pop-up menu.

The LSP Details and Link Details pop-up dialog boxes are displayed on the right pane.

The LSP details are displayed in a table as follows:

- Name—Name of the configured LSP on the specific link
- Status—Whether the LSP is active (up) or inactive (down)
- Path Type—Whether the path is a primary path (explicit or dynamic) or a secondary path (explicit or dynamic)
- Control Type—Whether the LSP is router-controlled or PCC-initiated, CSD-Topology-initiated or PCEP-initiated, or CSD-Topology managed or delegated LSP

The link details are displayed in a table as follows:

- End A Device—Node ID of the LSP head end
 - End B Device—Node ID of the LSP tail end
 - End A IP—IP address of the LSP head end
 - End B IP—IP address of the LSP tail end
 - Operational Status—Specifies whether the link is active (up) or inactive (down)
7. Click the **Close** icon at the top-right corner of the pop-up dialog box to return to the topology map.

**Related
Documentation**

- [Viewing Topology Map Group Details in a Pop-Up Dialog Box on page 326](#)
- [Viewing Topology Map Device Details in a Pop-Up Dialog Box on page 328](#)
- [Viewing Topology Map Link Details in a Pop-Up Dialog Box on page 330](#)
- [Viewing Topology Map Service Details in a Pop-Up Dialog Box on page 334](#)

Viewing Topology Map Service Details in a Pop-Up Dialog Box

In the Topology View of Build mode, the upper portion of the page shows the topology map, which is the main display area. In this area, you can click or right-click the dotted connecting links, which represent the services configured across devices, to view the service details. The pop-up menu is accessed by double-clicking a group in the center pane that shows the topology map. Mouse over a service on the map to display a pop-up menu for that service.

The topology map enables you to obtain a comprehensive view of services configured on devices in the entire network. Because you can narrow down to a specific service that is of relevance to you in the topology map, you can easily view important configuration specifications of a service, such as the type of service, the customer with which the service is associated, whether the service is successfully deployed or is pending deployment, and whether the service is in the requested, scheduled, or pending status. Such salient service-specific details enable you to obtain a comprehensive view of the health of services, and navigate to the Service View in Deploy mode to modify the service settings for debugging and corrective action.



NOTE: Right-clicking the map area displays a pop-up menu for more functions. You can move the map by holding down and dragging the left mouse button. You can zoom in and out by using the mouse scroll wheel. Double-click an element icon to collapse the devices or network elements and view the entire site or zone as an icon.

Mouse over the dotted lines that denote the services configured across different endpoints on the topology map and click the service to display a menu. The following fields are displayed in the pop-up dialog box when you mouse over the service:

- Name—Name of the configured service
- Customer Name—Name of the customer for which the service is configured
- Service Type—Type of the configured service, such as ELINE Martini, L3VPN, or VPLS
- Service State—State of the service, such as whether the service is deployed or not
- Service Status—Status of the service, such as whether the service is in requested, scheduled, or pending status
- View Details—Detailed information about the selected service. Click the link in **View Details** to open a pop-up dialog box that displays these details.

To view service details in a pop-up dialog box:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Topology View**.

The topology map of the sites or zones and the devices configured in each zone using the CSD-Topology is displayed.

3. Select the **Services** tab on the lower portion of the page.

The configured service details are displayed in a table.

4. Select the check box beside the services that you want to view on the topology map.

The selected services are displayed as different dotted color-coded lines on the map.

5. In the graphical representation of the topology displayed on the upper portion of the page, select the service by clicking the dotted lines or right-clicking the dotted lines for which you want to view details.

The service is highlighted and displayed as a colored dotted line.

6. Click the **View Details** link from the shortcut menu.

The Service Details pop-up dialog box is displayed on the right pane.

The service details are displayed in a table as follows:

- Customer Name—Name of the customer for which the service is configured
- Service Type—Type of the configured service, such as ELINE Martini, L3VPN, or VPLS
- Service State—State of the service, such as whether the service is deployed or not
- Service Status—Status of the service, such as whether the service is in requested, scheduled, or pending status

7. Click the **Close** icon at the top-right corner of the pop-up dialog box to return to the topology map.

Related Documentation

- [Viewing Topology Map Group Details in a Pop-Up Dialog Box on page 326](#)
- [Viewing Topology Map Device Details in a Pop-Up Dialog Box on page 328](#)
- [Viewing Topology Map Link Details in a Pop-Up Dialog Box on page 330](#)
- [Viewing Topology Map LSP Details in a Pop-Up Dialog Box on page 332](#)

Enabling the Collection of LSP and Service Association Details

From the **Monitoring** tab of the Preferences page (which you can launch by clicking the down arrow beside the System button on the Connectivity Services Director banner and selecting Preferences), you can enable the collection of LSPs configured on the links of the PCC devices in a topology and also to enable retrieval of service association details with the LSPs. When you enable this functionality, the details are obtained from the devices at periodic polling intervals.

To specify the monitoring setting for Topology:

1. From the Junos Space user interface, click the **System** icon in the Connectivity Services Director banner.

The options that you can configure in System mode are displayed in a drop-down menu.

2. Select **Preferences** from the drop-down menu to open the Preferences page.

The Preferences page opens with User Preferences as the default tab.

3. Click the **Monitoring** tab to configure the frequency at which the association between LSPs and services must be retrieved for the topology.

The settings that you can configure on the Monitoring tab are displayed.

4. Select the **ProvisioningMonitorLSPToServiceAssociationCollector** check box to enable the collection of LSPs configured on the links of the PCC devices in a topology and also to enable retrieval of service association details with the LSPs.

When you select this check box, the details are obtained from the devices at periodic polling intervals. By default, the polling interval is 5 minutes.

Related Documentation • [Configuring PCEP on a PE Router \(from CLI\) on page 289](#)

Using Custom Grouping for Devices in a CSD Topology

You can use the custom grouping methodology in Connectivity Services Director to cluster the devices that the CSD-Topology provisions PCEP for establishing LSPs between the PCC routers. Custom group is way of grouping your devices based on your business needs. You can create custom groups and add devices to each custom group. You can manually add devices to a custom group or you can define rules to add devices, that match the rule condition, to the custom group once they are discovered by Connectivity Services Director. You can view the custom groups and devices that are assigned to each group in the Custom Group view.

Using the custom groups feature, you can control how the group is displayed on the topology map—as a single group entity or as individual member nodes. When you expand

a group on the topology map by double-clicking the group icon, all the member nodes are listed in a circle with interconnecting links and are displayed on the map. When you collapse a group on the topology map by double-clicking the circle that contains the member nodes, only the group is displayed and represented by a single icon on the map.

Related Documentation

- [Configuring PCEP on a PE Router \(from CLI\) on page 289](#)

Viewing Generated Alarms for Services in the Topology View

Apart from displaying a graphical representation of the nodes and interconnecting links in a network deployment, the Topology View also displays the alarms of each severity level generated for services configured on nodes in the network topology at the top-left corner of the View Topology page. Information is displayed about the alarms generated by different devices for which services, such as point-to-point, Layer 3 VPN, RSVP LSPs, and VPLS, are configured. The summarized way in which you can view alarm details enables you to examine the health and operating-efficiency of devices, and the performance of services. These alarm details enable effective and simplified troubleshooting and administration.

For example, if you find that a particular device has recorded a large number of critical or major alarms for a service, you can then navigate to the design and provisioning pages of the type of service to correct and modify the attributes or diagnose the problems that might be generating the alarms. You can then clear the appropriate alarm from the Alarm Detail monitor in Fault mode of Service View after examining the alarm and associated events, and taking any corrective action needed to resolve the alarm condition on the corresponding device.



NOTE: Only service-level alarms are displayed; alarms generated for LSPs configured on the links connecting the nodes are not shown.

Related Documentation

- [Configuring PCEP on a PE Router \(from CLI\) on page 289](#)

Viewing the Optical Link Details for Examining the Performance of Optical Links

In the Topology View of Build mode, in addition to the Layer 3 links configured for services (such as Layer 3 VPNs), you can view the optical links or connections that are configured on optical interfaces of devices such as PTX Series Packet Transport Routers. You can sort and filter the optical links for viewing only the links of interest for your network. You can easily identify the type of links—Layer 3 or optical—by using the Type field on the Links tab displayed on the lower portion of the View Topology page.

Selecting a particular optical link on the Links tab highlights the link with a color-coded connector line in the Topology View. Also, the optical inline amplifiers (optical ILAs) that are installed on the PTX3000 routers are displayed on the topology map when you select an optical link that connects two optical ILAs. The optical ILAs are not plotted on the topology map unless you select an optical link on the Links tab.

To view optical links on a topology map:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

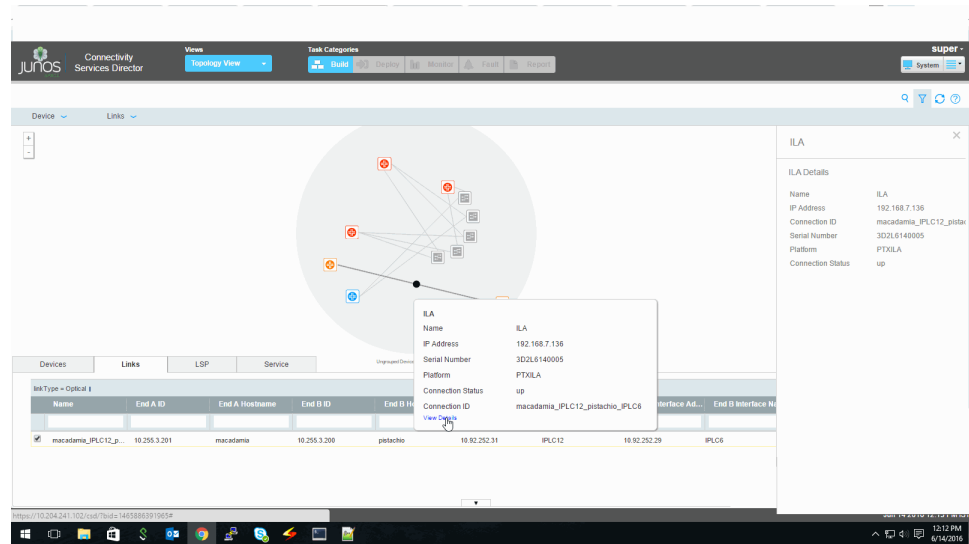
2. From the View selector, select **Topology View**.

The topology map of the sites or zones and the devices configured in each zone using the CSD-Topology is displayed on the upper portion of the page. A table with details of devices, services, links, and LSPs is displayed on the lower portion of the page.

3. Select the **Links** tab on the lower portion of the page.

The link details are displayed in a table.

4. Select the check box next to the link for which the value in the Type column is displayed as Optical.



The selected optical link is displayed as a color-coded line on the topology map. Also, the optical ILAs on PTX3000 routers that are present on either sides of the selected optical links are displayed on the topology map.

5. (Optional) Mouse over an optical ILA and click **View Details** from the pop-up menu to open a pop-up dialog box that displays detailed information about the optical ILA.
6. (Optional) Mouse over an optical link and click **View Details** from the pop-up menu to open a pop-up dialog box that displays detailed information about the optical link.
7. (Optional) Click the **Filter** icon at the top right of the topology map, and select the **Show Optical Links** check box from the Links drop-down menu.

Only the optical connections, and any optical ILAs between which the links exist, on the topology map are filtered and displayed in the topology window.

Related Documentation

- [Enabling the Collection of LSP and Service Association Details on page 336](#)
- [Using Custom Grouping for Devices in a CSD Topology on page 336](#)
- [Viewing Generated Alarms for Services in the Topology View on page 337](#)

PART 6

Prestaging

- [Prestaging Devices Overview on page 343](#)
- [Prestaging: Managing Devices and Device Roles on page 369](#)
- [Prestaging: Managing IP Addresses on page 389](#)
- [Device Configuration Prerequisites to Prestaging Examples on page 397](#)
- [Prestaging Services on page 405](#)

CHAPTER 19

Prestaging Devices Overview

- [Prestaging Devices Process Overview on page 344](#)
- [Prestaging Workflow in Connectivity Services Director on page 347](#)
- [Prerequisites for Prestaging Devices in Connectivity Services Director on page 350](#)
- [Discovering and Assigning All N-PE Devices on page 351](#)
- [Discovering and Assigning N-PE Devices with Exceptions on page 353](#)
- [Prestaging ATM and TDM Pseudowire Devices on page 356](#)
- [Discovering and Assigning Provider Role or LSP Role for Devices with Exceptions on page 359](#)
- [Discovering and Assigning All Provider or LSP Devices on page 362](#)
- [Prestaging Rules on page 364](#)

Prestaging Devices Process Overview

After Junos Space has discovered the devices, a two- or three-stage process to prestage devices is performed automatically in the backend by the Connectivity Services Director application. The following events occur in a sequential manner for preparing the devices to be compatible and qualified for configuration of services:

1. Discover roles. In this stage, the Junos Space software searches the database for N-PE devices that have not yet been assigned.
2. Examine the results of the role discovery and make any exceptions to the system recommendations. Specifically, you might:
 - Exclude specified devices from N-PE role assignment.

You might need to exclude a device that you know is not a PE device. For example, Provider (P) devices that have loopback addresses pass the rules for N-PE role assignment. For devices that you know are not PE devices, you can edit the configuration out-of-band, and then run role discovery again.
 - Select a different loopback address for a device.
 - Exclude interfaces from UNI assignment.
3. Confirm the assignments.

When device assignments are confirmed internally by the Connectivity Services Director application, those devices are removed from the list of recommendations. If, initially, you exclude devices from assignment, you can return to the list of recommendations later and make further assignments.

When you add more devices to your network, the role discovery operation runs again. Running role discovery again overwrites any devices remaining in the role discovery results list of recommended assignments, but has no effect on devices with confirmed assignments.

- The Prestage Devices screen shows a device inventory of N-PE routers that Connectivity Services Director has discovered in its database that have not yet been assigned. You can perform the following operations from the Prestage Devices screen:
 - Select multiple devices to assign roles—The most common and recommended prestaging workflow is to select all devices in the Assign Roles screen and assign them all. See [“Discovering and Assigning All N-PE Devices” on page 351](#) for step-by-step instructions for assigning all Junos Space recommendations.
 - Select a single device to assign a role—You must select a single device to change the the UNI assignments on that device. For step-by-step instructions on changing UNI assignments, see [“Excluding Interfaces from UNI Role Assignments” on page 376](#).

You can also exclude a single device using this screen.
 - Exclude specified devices from the N-PE role. See [“Discovering and Assigning N-PE Devices with Exceptions” on page 353](#) for step-by-step instructions.

- The Manage Interface Roles screen is an inventory of UNI-qualified interfaces for a specific discovered device. You can view a separate Manage Interface Roles screen for each discovered N-PE device. You can also exclude multiple interfaces from qualification as UNIs. For step-by-step instructions on excluding interfaces from the list of qualified UNIs, see [“Excluding Interfaces from UNI Role Assignments” on page 376](#).



NOTE: The UNI role is assigned to an interface by a notification from the managed device that is sent to the Connectivity Services Director application, even when you unassign the UNI role from the interface using the Prestage Devices workspace. For example, if you unassign the UNI role on an interface of a managed device, that interface is available for provisioning services on devices, when you attempt to create a service order. For the same interface, if you configure encapsulation on it directly from the device and navigate to the Prestaging workspace in Connectivity Services Director after a few minutes, the interface status indicates that UNI role is configured on it. This behavior occurs because the UNI role is assigned to the interface by a device notification.



NOTE: After a device is prestaged in Connectivity Services Director, the prestaging job is not initiated on the same device again. When a device notification is received by the application, Connectivity Services Director synchronizes the prestaging database on the UI interfaces. If a mismatch is detected in the UNI status of the interface in Connectivity Services Director database and the UNI status of the interface on the device (caused by the application being down or network accessibility problems), the synchronization of the UNI interface might not occur. In such a case, the synchronization operation occurs when a configuration- commit on the device is done the next time. To manually resolve this discrepancy in the UNI status of the interface, you can unassign the UNI role of the interface, which causes prestaging to perform a synchronization.

The VPLS service needs to be enabled in a network device, to make the static pseudowire functionality active in the device. You can activate the static pseudowire functionality by configuring the network device through the CLI window. You need to enter the CLI configuration mode of a network element and run the command

```
set protocols vpls static-vpls no-tunnel-services
```

```
commit
```

If the device is not configured through CLI, a warning message appears in the application server log, that is the **JBOSS Log**:

<Device name> should be configured with static VPLS no tunnel service rule.

To discover the roles of the various network elements configured:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. In the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.
4. Click **Manage Device Roles** and from the drop-down list, select **Discover Roles** to retrieve the roles of the devices. A dialog box is displayed with the job ID of the discovery job that is created to obtain the latest roles of the devices.

To remove the role of the network elements configured:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.
5. Click **Manage Device Roles** and from the drop-down list, select **Unassign Role** to remove the role capability of a network element. You are prompted to confirm the operation. If you click **OK**, a request is submitted to remove the latest role of the network element or device.

The device is removed from the list of network elements displayed on the Devices Chart page.

To resynchronize the role of the network elements configured:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.
5. Click **Manage Device Roles** and from the drop-down list, select **Re-sync Role Capability** to resynchronize the role capability of a network element. You are prompted to confirm the operation. If you click **OK**, request is submitted to retrieve the latest role of the network element or device.

The role is re-synced with the same device now.

**Related
Documentation**

- [Prerequisites for Prestaging Devices in Connectivity Services Director on page 350](#)
- [Discovering and Assigning All N-PE Devices on page 351](#)

- [Discovering and Assigning N-PE Devices with Exceptions on page 353](#)
- [Prestaging ATM and TDM Pseudowire Devices on page 356](#)
- [Prestaging Rules on page 364](#)

Prestaging Workflow in Connectivity Services Director

Prestaging of devices using the Services Activation Director GUI comprises the process of discovering capabilities of devices in the network. Certain classifications are made, depending on the result of the device prestaging process. Service provisioning is made possible on the device based on the discovered capabilities and classification. The devices that do not confirm to an expected configuration are not made available for selection, when you attempt to provision services. These capability discoveries of devices are prone to errors on certain occasions. A second level of control for the user to classify the device above the prestaging classification is implemented in Connectivity Services Director. This additional level of segregation and selection enables you to choose to override the capabilities discovered by the prestaging workflow. The information discovered by the prestaging workflow serves as a tip for you to modify the device-capability classification accordingly. Device prestaging using the Services Activation Director GUI is a manual process in which you need to prestage the device, before you can configure services on the device. Design enhancements have been made to automate this process using the automated prestaging mechanism, where the devices are prestaged automatically when concerned events occur on the device, in the Junos Space Platform database, or the deployment of the Connectivity Services Director application. Using this effective and streamlined automated prestaging methodology, the devices are always prestaged with latest configuration when you attempt to configure services on them.

The device prestaging workflow in Services Activation Director is slightly redundant and also error-prone. An additional step of prestaging the devices before a service can be configured on them is also not transparent and beneficial. As a result of this redundant implementation, the service configuration on a particular device is impacted. The service capabilities discovered for a service can be erroneous, owing to anomalies with device prestaging. Additionally, the process of confirming a role discovered by the prestaging workflow is regarded as an unnecessary step and is discarded in the redesigned and optimized workflow. In Services Activation Director, the changes that affect the service capability of the device are not automatically discovered. In Connectivity Services Director, the devices are always prestaged services are configured on them to enable the latest configuration to be synchronized between the device and the application. Auto-discovering the devices, based on changes occurring on the device and Junos Space Platform is highly efficient and user-friendly.

Auto-Discovery and Auto Prestaging of Devices

The process of automatically synchronizing device configuration and service capability discovery, based on the configuration setting changes made on the device and using the Junos Space Platform software application, is called device automatic prestaging. The auto prestaging mechanism is triggered based on events occurring on the device and the Junos Space Platform software. Certain events that occur on the devices are identified

as conditions for triggering the auto prestaging workflow. The following are some of the events that impact the capability of the device to enable Network Services to function:

- Device addition and deletion using the Junos Space Platform GUI
- Interface status alternating between up and down
- Loopback address change
- Interface addition and deletion
- Service type-related configuration (in scenarios when additional configuration such as BGP or LDP changes are made, which updates the service capability (L2, L3) of the device)
- Management IP address or hostname change
- Changes to the interface family
- Changes in the interface encapsulation type

Parallel Prestaging Jobs

Because auto prestaging is an automated process triggered by the change events from the device and platform, there can be multiple parallel prestaging jobs from a single device and from multiple devices. These jobs update the corresponding device information on completion. Service creation and deployment is not impacted by the prestaging jobs and picks up the available configuration at the given point of time. In the older version of Services Activation Director, only one prestaging job can run at any point of time, which is valid with only manual prestaging because the prestaging job scans the whole device inventory and prestages device which are not already been assigned a role. Having a second job run in parallel does not result in any advantage. With the introduction of auto device prestaging feature, the scenario is different because auto-prestaging is mostly per-device, and therefore, it is essential to have parallel prestaging jobs running for different devices.

Auto Prestaging Jobs When a Manual Prestaging Job is Running

Manual prestaging process prestages the entire device inventory and auto assigns device roles to them. Therefore, having a per-device auto prestaging job running in parallel might be redundant for the functionality because the concerned device could most likely be taken care of by the manual prestaging job. However, possibilities arise in which the concerned device is prestaged before the new event and the latest configuration is not synced. To avoid such race condition, the auto prestaging job has to run after the manual job completes. For this sequencing of the types of prestaging jobs, auto prestaging event request is stored in a memory queue against a particular device ID and is run by the scheduler after the manual prestaging job completes.

Manual Prestaging Jobs When an Auto Prestaging Job is Running.

Manual prestaging jobs are queued if there are auto prestaging jobs currently running. The manual prestaging job for a particular device is discarded if an auto prestaging job is already in progress.

Multiple Auto Prestaging Jobs for a Device

In cases where there are multiple events generated for a single device the event are queued for execution, a validation is performed to determine if there are current jobs in execution for the particular device and queue the request in which case. There can only be one prestaging request per device in queue at any point in time.

Multiple Auto Prestaging Jobs for a Device

In this case, all the prestaging jobs has to run in parallel. With Services Activation Director (only manual re-sync), the prestaging data in overwritten when a new prestage jobs runs, until the role is assigned. However, with the latest changes, the role assignment happens as part of manual or auto prestaging, and enhancements are made to support parallel processing.

Scenarios With a Clustered Environment

There are possibilities of race conditions in a clustered Junos Space appliance environment where there can be parallel prestaging jobs queued up for the same type of devices as the jobs because the queue context is local to each instance in the cluster. These scenarios are prevented by using a cluster-level context for the queues is present.

Types of Prestaging

Because of scenarios where the manual and auto prestaging has to be identified specifically, the support for distinguishing both the types needs to be added. Instead of the handling of the auto prestaging and manual prestaging jobs by a single job API in which the job data does not contain any information regarding the nature of the job being manual or auto prestaging, the distinction is achieved by comparing the device ID against null from the database job data and by running two separate jobs, one for manual prestaging and the other for auto prestaging.

Prestaging takes the devices already under Junos Space management and prepares them for service activation. The prestaging process discovers network provider edge (N-PE) devices in the Junos Space database and assigns roles to those devices and their interfaces. In Connectivity Services Director, device discovery and prestaging done automatically whenever a device is added or updated.

Related Documentation

- [Prestaging Devices Process Overview on page 344](#)
- [Prerequisites for Prestaging Devices in Connectivity Services Director on page 350](#)

Prerequisites for Prestaging Devices in Connectivity Services Director

Before you can perform prestaging on your network devices, each device must meet specific configuration requirements, and must be brought under Junos Space management through device discovery.

The following configuration requirements must be met before beginning the provisioning process. Otherwise, service deployment fails:

- MPLS must run on each N-PE device and on each P device.
- LDP signaling must be established between N-PE devices that participate in the same point-to-point Ethernet (LDP) service.
- MPBGP must run on each N-PE device that participates in a Layer 2 multipoint or Layer 3 full mesh service.
- To run Layer 2, Layer 3, or VPLS services on an N-PE device, ensure that an autonomous system (AS) number is configured on the device.

Before you can prestage devices, you must perform device discovery to import all Juniper Networks devices on your network that Junos Space can manage. The Connectivity Services Director prestaging workspace works on devices that have already been discovered and imported into the Junos Space database, but have not yet been prestaged.

The VPLS service needs to be enabled in a network device, to make the static pseudowire functionality active in the device. You can activate the static pseudowire functionality by configuring the network device through the CLI window. You need to enter the CLI configuration mode of a network element and run the command

```
set protocols vpls static-vpls no-tunnel-services
```

```
commit
```

If the device is not configured through CLI, a warning message appears in the application server log, that is the **JBOSS Log**:

<Device name> should be configured with static VPLS no tunnel service rule.

To discover the roles of the various network elements configured:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. In the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.
4. Click **Manage Device Roles** and from the drop-down list, select **Discover Roles** to retrieve the roles of the devices. A dialog box is displayed with the job ID of the discovery job that is created to obtain the latest roles of the devices.

To remove the role of the network elements configured:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.
5. Click **Manage Device Roles** and from the drop-down list, select **Unassign Role** to remove the role capability of a network element. You are prompted to confirm the operation. If you click **OK**, a request is submitted to remove the latest role of the network element or device.

The device is removed from the list of network elements displayed on the Devices Chart page.

To resynchronize the role of the network elements configured:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.
5. Click **Manage Device Roles** and from the drop-down list, select **Re-sync Role Capability** to resynchronize the role capability of a network element. You are prompted to confirm the operation. If you click **OK**, request is submitted to retrieve the latest role of the network element or device.

The role is re-synced with the same device now.

Related Documentation

- *Discovering Devices* in the *Junos Space Network Application Platform User Guide*

Discovering and Assigning All N-PE Devices

Prestaging all Connectivity Services Director assignment recommendations is a powerful yet simple way to prepare your devices for provisioning. This procedure provides the prestaging steps that accept all system recommendations. To prestage devices and make exceptions to the system recommendations, see [“Discovering and Assigning N-PE Devices with Exceptions” on page 353](#).

Before discovering and assigning N-PE devices, you must have already run device discovery. See the “Discovering Devices” section in the *Junos Space Network Application Platform User Guide*.

Prestaging has two parts:

1. [Discovering Device Roles on page 352](#)
2. [Assigning Device Roles on page 352](#)

Discovering Device Roles

To discover the roles of devices found during element discovery:

To discover the roles of the various network elements configured:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. In the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.
4. View the values displayed under the Roles column of the discovered devices.
5. Click **Manage Device Roles** and from the drop-down list, select **Discover Roles** to retrieve the roles of the devices. A dialog box is displayed with the job ID of the discovery job that is created to obtain the latest roles of the devices.



NOTE: You cannot discover a device as a PE device if no user-to-network interfaces (UNIs) are available in the device.

The Connectivity Services Director application throws the following error message:

```
2012-06-08 10:17:23,446 ERROR [PreStageDeviceManagerBean]
(PreStageDeviceManagerBean#savePreStageDeviceList Thread-6894
(group:HornetQ-client-global-threads-1332782448):) No ge/fe/at/tl
interfaces in this PE device: junos-mx480-space; it can only be used for virtual
routers
```

Assigning Device Roles

If you need to exclude devices from role assignment, or you need to exclude interfaces from the list of interfaces that can be used as UNIs, use the procedures documented in [“Discovering and Assigning N-PE Devices with Exceptions” on page 353](#).

To discover the roles of the various network elements configured:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.

3. In the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.

4. View the values displayed under the Roles column of the discovered devices.

5. Click **Manage Device Roles** and from the drop-down list, select **Discover Roles** to retrieve the roles of the devices. A dialog box is displayed with the job ID of the discovery job that is created to obtain the latest roles of the devices.

The **Job Management** page shows the progress and status of the role assignment job. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details.

While the job is ongoing, you cannot make additional assignments from the **Assign Roles** page. The Assign NPE Role action is dimmed to indicate you cannot select it.

Related Documentation

- [Prestaging Devices Process Overview on page 344](#)
- [Prerequisites for Prestaging Devices in Connectivity Services Director on page 350](#)
- [Discovering and Assigning N-PE Devices with Exceptions on page 353](#)
- [Prestaging ATM and TDM Pseudowire Devices on page 356](#)
- [Prestaging Rules on page 364](#)

Discovering and Assigning N-PE Devices with Exceptions

Preparing network devices for service activation is usually a simple process which directs the Connectivity Services Director application to prepare your devices automatically. When you prestage devices, the Connectivity Services Director application scans the database for devices that have already been discovered but have no MPLS role assigned, and recommends a role for each device it finds, based on the device configuration data and a set of predefined rules. You can then display those devices and their recommended settings for:

- MPLS role for the device (PE only)
- Loopback interface
- UNI interfaces

The Connectivity Services Director application allows you to exclude specific recommended devices from being assigned the N-PE role and to exclude interfaces from use as UNIs during service provisioning. You can also change the loopback address of a PE device..

For step-by-step instructions on how to prepare devices for network activation using all the recommendations for N-PE role assignment and UNI assignment that the Connectivity Services Director application makes, see [“Discovering and Assigning All N-PE Devices” on page 351](#). These topics describe how to prestage devices with exceptions:

- [Including Interfaces in UNI Role Assignments on page 354](#)
- [Committing Your Prestaging Choices on page 354](#)

Including Interfaces in UNI Role Assignments

To include interfaces from the list of interfaces that the prestaging rules determined were suitable for use as UNIs:

1. In the address bar of your browser window, enter: `https://<1.1.1.1>/mainui/` where `<1.1.1.1>` is the Web IP address for Web access to the Services Activation Director GUI. Alternatively, from the Connectivity Services Director GUI, click the Junos Space icon in the Connectivity Services Director banner. The Junos Space Network Management Platform page is displayed.

2. In the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices > Manage Device Roles**.

The results of the most recent role discovery operation appear, including any changes you have subsequently made to your prestaging data.

Repeat Step 2 through Step 7 for each device for which you want to include some recommended UNI selections:

3. In the **Devices Chart** page, select the device for which you want to manage UNIs.

4. Select a device and click **Manage Interface Roles**.

The **Manage Interface Roles** window shows all the device interfaces for the selected device and indicates those that the Connectivity Services Director application recommends for use as UNIs.

5. In the **Manage Interface Roles** window, select the check box under the UNI column that you want to assign to the device.

To assign more than one UNI, use the multiple selection capability.

6. Click **OK** to submit the selection and return to the Devices Chart page.

See Also • [Excluding Devices from N-PE Role Assignment on page 375](#)

Committing Your Prestaging Choices

This procedure provides instructions for assigning the N-PE role to selected devices and committing all device prestaging information to the database.

Before performing these steps, you must complete the following tasks:

- Discover devices that have not yet been assigned an MPLS role.
- Exclude from the list of discovered devices those devices that you do not want to assign the N-PE role to.
- On each device, exclude the interfaces you do not want used as UNIs.

To commit your prestaging choices to the database:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services > Connectivity** task pane, select **Prestage Devices > Manage Device Roles > Assign Roles**.
4. Examine the list of devices to be sure these are the devices you want to assign the N-PE role.
5. Select all devices.
6. Click **Manage Device Roles** and select **Discover Roles**. A job is submitted to obtain the roles of the devices.
7. To view the assignment status, in the Job Management screen, click the job ID of the assignment job.

The **Job Management** page shows the progress and status of the role assignment job.



NOTE: Alternatively, to display the Job Management page, click the **System** icon on the Connectivity Services Director banner, and select **Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

While the job is ongoing, you cannot make additional assignments from the **Assign Roles** page. The Assign NPE Role action is dimmed to indicate you cannot select it.



NOTE: If you modify the configuration of a device after the device is prestaged, remove the device from prestaged status and then **Discover Roles** and prestage the device again.

Related Documentation

- [Prestaging Devices Process Overview on page 344](#)
- [Prerequisites for Prestaging Devices in Connectivity Services Director on page 350](#)
- [Discovering and Assigning All N-PE Devices on page 351](#)
- [Prestaging ATM and TDM Pseudowire Devices on page 356](#)
- [Prestaging Rules on page 364](#)

Prestaging ATM and TDM Pseudowire Devices

Junos Space supports ATM and TDM pseudowires in IP/MPLS networks on M Series Multiservice Edge Routers with Circuit Emulation Service (CES) Physical Interface Cards (PICs). The ATM and TDM pseudowires run over an LSP connection.

Static pseudowires are designed for networks that do not support LDP or do not have LDP enabled. You define pseudowires by configuring static values for the inbound and outbound labels of the connection. For details on configuring pseudowire connections in Junos OS, see the [Junos OS VPNs Configuration Guide](#), the *Layer 2 VPN Configuration Example*, and *Configuring Layer 2 Circuit and Layer 2 VPN Pseudowires*.

Prerequisites for M Series Routers

One of the following CES PICs is required:

- 4-Port ChOC3/STM1 CES PIC
- 12-Port T1/E1 CES PIC

Prerequisites for the BX Series Gateway

The BX Series devices have a fixed configuration with 3 Gigabit Ethernet (GE) interfaces and 16 T1/E1 ports that can be used by ATM/TDM pseudowire services. The correct level of firmware is required. Refer to the release notes that correspond to the release of Junos Space that you are running for the correct level information.

RFCs Supported

RFC 4553, *Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)*

Before discovering and assigning N-PE devices, you must have already have run device discovery. See the "Discovering Devices" section in the *Junos Space Network Application Platform User Guide*.

When you run the discovery process for ATM and TDM devices, they need to be discovered as N-PE devices. In addition, the BX Series devices require an additional device role defined as a cell site router (CSR). This figure shows the discovered devices.

Devices > Manage Devices

0 Items Selected

Actions

Name	Physic...	Logical...	OS Ver...	Device...	Platform	Schem...	IP Add...	Connec...	Manag...	AIS In...
access-bt750	View	View	3.0.0	tcaos	B-7510	3.0.0	10.216...	up	Out Of Sync	---
access-hd-bgm	View	View	3.0.0	tcaos	C-2030	3.0.0	10.216...	up	Out Of Sync	---
access1-bt750	View	View	3.0.0	tcaos	B-7510	3.0.0	10.216...	up	Out Of Sync	---
access2-bt750	View	View	3.0.0	tcaos	B-7510	3.0.0	10.216...	up	Out Of Sync	---
access3-bt750	View	View	3.0.0	tcaos	B-7510	3.0.0	10.216...	up	Out Of Sync	---
access4-bt750	View	View	3.0.0	tcaos	B-6010	3.0.0	10.216...	up	Out Of Sync	---
access5-bt750	View	View	3.0.0	tcaos	B-7510	3.0.0	10.216...	up	Out Of Sync	---
access6-bt750	View	View	3.0.0	tcaos	B-7510	3.0.0	10.216...	up	Out Of Sync	---
access7-bt750	View	View	3.0.0	tcaos	B-7510	3.0.0	10.216...	up	Out Of Sync	---
junos-m10-1-space	View	View	12.2R1.8	junos	M10I	12.1R3.5	10.216...	up	In Sync	---
junos-m10-2-space	View	View	12.2R1.8	junos	M10I	12.1R3.5	10.216...	up	In Sync	---

Page 1 of 1 | Displaying 1 - 30 of 30 | Show 60 items

After you discover the devices, use Connectivity Services Director Prestaging feature to bring the PE and CSR devices into Network Services together with their UNI interfaces. In the **Network Services > Connectivity** task pane, select **Prestage Devices > Manage Device Roles**.

Prestage Devices > Manage Device Roles

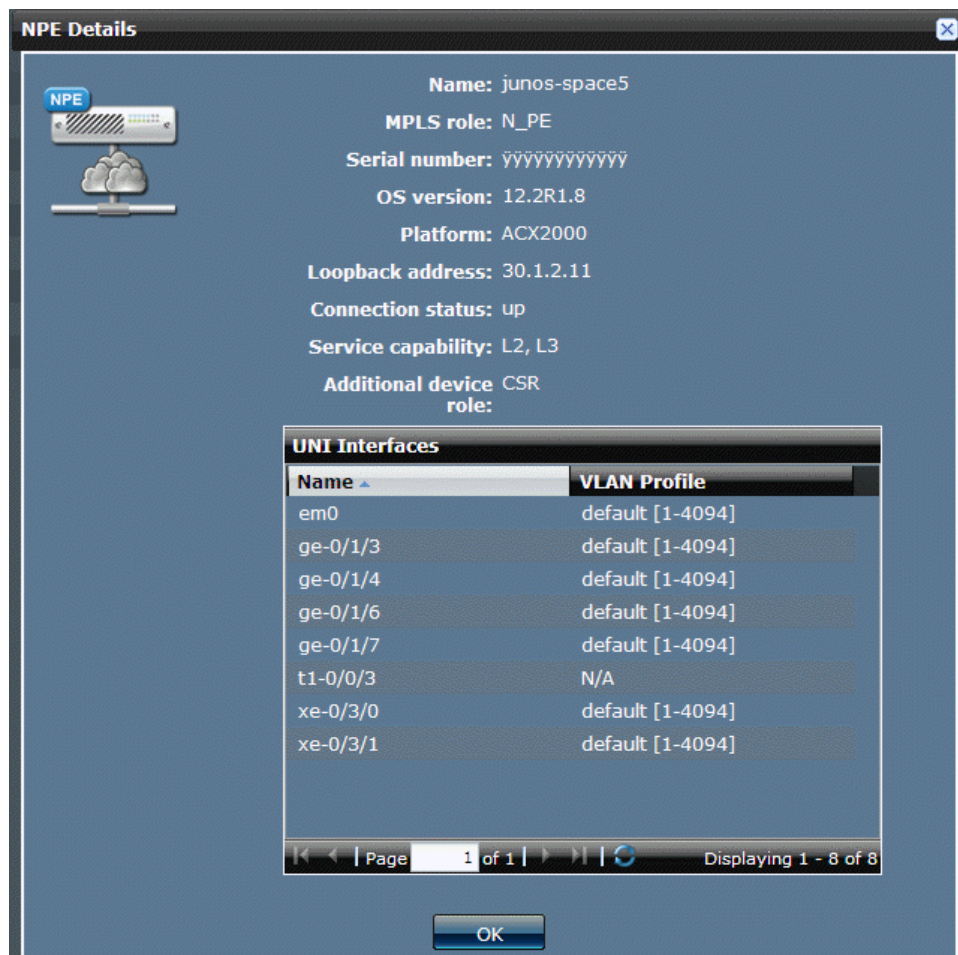
0 Items Selected

Actions

Name	Management Address	Loopback Address
vjx-junos-mx80-2-space	10.213.52.119	40.1.255.9
vjx-junos-mx80-1-space	10.213.53.57	40.1.255.1
vjx-junos-mx480-space	10.213.50.234	40.1.255.3
vjx-junos-mx240-space	10.213.51.206	40.1.255.8
vjx-junos-m10-2-space	10.213.51.130	40.1.255.4
vjx-junos-m10-1-space	10.213.53.151	40.1.255.10
vjx-embassy-mx80-space	10.213.51.177	40.1.255.7
vjx-acx4-space	10.213.52.148	40.1.255.2
vjx-acx3-space	10.213.53.203	40.1.255.11
vjx-acx2-space	10.213.53.68	40.1.255.6
vjx-acx1-space	10.213.50.227	40.1.255.5
junos-space5	10.216.114.123	30.1.2.11
junos-space3	10.216.114.121	30.1.2.9
junos-space2	10.216.114.120	30.1.2.8
junos-space1	10.216.114.119	30.1.2.7
junos-mx80-2-space	10.216.114.105	30.1.2.3
junos-mx80-1-space	10.216.114.104	30.1.2.5
junos-mx480-space	10.216.114.100	30.1.2.6
junos-mx240-space	10.216.114.101	30.1.2.1

Page 1 of 1 | Displaying 1 - 21 of 21 | Show 30 items

Double-click a listed device. In this example; you can see that an MPLS role and an additional device role as a CSR are assigned.



Double-click another listed device. In this example, the details window shows the channelized ATM and T1 interfaces.



Related Documentation

- [Prestaging Devices Process Overview on page 344](#)
- [Prerequisites for Prestaging Devices in Connectivity Services Director on page 350](#)
- [Discovering and Assigning All N-PE Devices on page 351](#)
- [Discovering and Assigning N-PE Devices with Exceptions on page 353](#)
- [Prestaging ATM and TDM Pseudowire Devices on page 356](#)

Discovering and Assigning Provider Role or LSP Role for Devices with Exceptions

Preparing network devices for service activation is usually a simple process which directs the Connectivity Services Director application to prepare your devices automatically. When you prestage devices, the Connectivity Services Director application scans the database for devices that have already been discovered but have no MPLS role assigned, and recommends a role for each device it finds, based on the device configuration data and a set of predefined rules. You can then display those devices and their recommended settings for:

- MPLS role for the device (PE only)
- Loopback interface
- UNI interfaces

The Connectivity Services Director application allows you to exclude specific recommended devices from being assigned the P or LSP role and to exclude interfaces from use as UNIs during service provisioning. You can also change the loopback address of an LSP device..

For step-by-step instructions on how to prepare devices for network activation using all the recommendations for P or LSP role assignment and UNI assignment that the Connectivity Services Director application makes, see [“Discovering and Assigning All N-PE Devices” on page 351](#). These topics describe how to prestage devices with exceptions:

- [Including Interfaces in UNI Role Assignments on page 360](#)
- [Committing Your Prestaging Choices on page 361](#)

Including Interfaces in UNI Role Assignments

To include interfaces from the list of interfaces that the prestaging rules determined were suitable for use as UNIs:

1. In the address bar of your browser window, enter: `https://<1.1.1.1>/mainui/` where `<1.1.1.1>` is the Web IP address for Web access to the Services Activation Director GUI. Alternatively, from the Connectivity Services Director GUI, click the Junos Space icon in the Connectivity Services Director banner. The Junos Space Network Management Platform page is displayed.

2. In the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices > Manage Device Roles**.

The results of the most recent role discovery operation appear, including any changes you have subsequently made to your prestaging data.

Repeat Step 2 through Step 7 for each device for which you want to include some recommended UNI selections:

3. Select a device and click **Manage Interface Roles**.

The **Manage Interface Roles** window shows all the device interfaces for the selected device and indicates those that the Connectivity Services Director application recommends for use as UNIs.

4. In the **Manage Interface Roles** window, select the check box under the UNI column that you want to assign to the device.

To assign more than one UNI, use the multiple selection capability.

5. Click **OK** to submit the selection and return to the Devices Chart page.

See Also • [Excluding Devices from N-PE Role Assignment on page 375](#)

Committing Your Prestaging Choices

This procedure provides instructions for assigning the P or LSP role to selected devices and committing all device prestaging information to the database.

Before performing these steps, you must complete the following tasks:

- Discover devices that have not yet been assigned an MPLS role.
- Exclude from the list of discovered devices those devices that you do not want to assign the P or LSP role to.
- On each device, exclude the interfaces you do not want used as UNIs.

To commit your prestaging choices to the database:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services > Connectivity** task pane, select **Prestage Devices > Manage Device Roles > Assign Roles**.
4. Examine the list of devices to be sure these are the devices you want to assign the P or LSP role.
5. Select all devices.
6. Click **Manage Device Roles** and select **Discover Roles**. A job is submitted to obtain the roles of the devices.
7. To view the assignment status, in the Job Management screen, click the job ID of the assignment job.

The **Job Management** page shows the progress and status of the role assignment job.



NOTE: Alternatively, to display the Job Management page, click the **System** icon on the Connectivity Services Director banner, and select **Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

While the job is ongoing, you cannot make additional assignments from the **Assign Roles** page. The Assign NPE Role action is dimmed to indicate you cannot select it.



NOTE: If you modify the configuration of a device after the device is prestaged, remove the device from prestaged status and then Discover Roles and prestage the device again.

Related Documentation

- [Prestaging Devices Process Overview on page 344](#)
- [Prerequisites for Prestaging Devices in Connectivity Services Director on page 350](#)
- [Discovering and Assigning All N-PE Devices on page 351](#)
- [Prestaging ATM and TDM Pseudowire Devices on page 356](#)
- [Prestaging Rules on page 364](#)

Discovering and Assigning All Provider or LSP Devices

Prestaging all Connectivity Services Director assignment recommendations is a powerful yet simple way to prepare your tunneling or label-switched path (LSP) devices for provisioning. This procedure provides the prestaging steps that accept all system recommendations. To prestage LSP or tunneling devices and make exceptions to the system recommendations, see [“Discovering and Assigning Provider Role or LSP Role for Devices with Exceptions” on page 359](#).

Before discovering and assigning provider (P) or LSP devices, you must have already run device discovery. See the “Discovering Devices” section in the *Junos Space Network Application Platform User Guide*.

Prestaging has two parts:

1. [Discovering LSP Device Roles on page 362](#)
2. [Assigning Provider Device Roles on page 363](#)

Discovering LSP Device Roles

To discover the roles of LSP devices found during element discovery:

To discover the roles of the various network elements configured:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. In the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.
4. View the values displayed under the Roles column of the discovered devices.

5. Click **Manage Device Roles** and from the drop-down list, select **Discover Roles** to retrieve the roles of the devices. A dialog box is displayed with the job ID of the discovery job that is created to obtain the latest roles of the devices.



NOTE: You cannot discover a device as a PE device if no user-to-network interfaces (UNIs) are available in the device.

The Connectivity Services Director application throws the following error message:

```
2012-06-08 10:17:23,446 ERROR [PreStageDeviceManagerBean]
(PreStageDeviceManagerBean#savePreStageDeviceList Thread-6894
(group:HornetQ-client-global-threads-1332782448):) No ge/fe/at/t1
interfaces in this PE device: junos-mx480-space; it can only be used for virtual
routers
```

Assigning Provider Device Roles

If you need to exclude devices from role assignment, or you need to exclude interfaces from the list of interfaces that can be used as UNIs, use the procedures documented in [“Discovering and Assigning Provider Role or LSP Role for Devices with Exceptions” on page 359](#).

To discover the roles of the various network elements configured:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. In the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.
4. View the values displayed under the Roles column of the discovered devices.
5. Click **Manage Device Roles** and from the drop-down list, select **Discover Roles** to retrieve the roles of the devices. A dialog box is displayed with the job ID of the discovery job that is created to obtain the latest roles of the devices.

The **Job Management** page shows the progress and status of the role assignment job. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details.



NOTE: Alternatively, to display the Job Management page, click the **System** icon on the Connectivity Services Director banner, and select **Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

While the job is ongoing, you cannot make additional assignments from the **Assign Roles** page. The Assign LSP Role action is dimmed to indicate you cannot select it.

**Related
Documentation**

- [Prestaging Devices Process Overview on page 344](#)
- [Prerequisites for Prestaging Devices in Connectivity Services Director on page 350](#)
- [Discovering and Assigning N-PE Devices with Exceptions on page 353](#)
- [Prestaging ATM and TDM Pseudowire Devices on page 356](#)
- [Prestaging Rules on page 364](#)

Prestaging Rules

Prestaging rules are predefined. These rules contain criteria for classifying the MPLS role of each device, in addition to recommending which physical interfaces should be UNI interfaces. For each recommended UNI interface, the system recommends its primary loopback address and its VLAN pool profile.

Correctly assigning MPLS roles to devices is critical for provisioning the correct MPLS behavior. Each MPLS role has a different behavior. For example, N-PE is the only role allowed to terminate MPLS sessions..

The rules used by the Junos Space software to determine the recommended role assignment are described for devices, UNIs, and VLAN pool profiles in the following sections:

N-PE Device Classification Rules

The system recommends the N-PE role for devices that satisfy the following criteria:

- The comment field in the device configuration identifies the device as an N-PE device.
- The device role is set to N-PE unless EBGp is enabled for the device. Specifically, the device role is set to N-PE unless the device configuration has **configuration/protocols/bgp/group/type** set to external. If EBGp is enabled, the device role is set to P.
- The device is assigned a loopback address. A device that has no loopback address cannot function as an N-PE device.
- LDP is enabled on the loopback interface for the device. LDP must be enabled on the loopback interface if the device is to be assigned the PE MPLS role. (Required point-to-point Ethernet services.)
- L2 VPN signaling for BGP is enabled. Specifically, the rule checks whether the device configuration has **configuration/protocols/bgp/family/l2vpn/signaling** or **configuration/protocols/bgp/group/l2vpn/signaling** set. (Required for Layer 2 Ethernet services.)
- inet-vpn unicast for BGP is enabled. Specifically, the rule checks whether the device configuration has **configuration/protocols/bgp/family/inet-vpn/unicast** set. (Required for Layer 3 VPN services.)

UNI Classification Rules

Before an interface on an N-PE device can be provisioned as a UNI, it must satisfy the following criteria:

- The interface must be Gigabit Ethernet (ge), 10-Gigabit Ethernet (xe), Aggregated Ethernet (ae), or Fast Ethernet (fe) type.

Fast Ethernet (fe) interfaces are supported for the Ethernet service configurations (on M Series devices with Junos OS Release 10.2R1.6).

- Checks for Gigabit Ethernet (ge) interfaces within an Aggregated Ethernet (ae) interface. Excludes Gigabit Ethernet interfaces that are configured within an Aggregated Ethernet interface from UNI assignment.
- Checks for bridge family on logical interfaces. Excludes interfaces from UNI assignment if interface configuration on the device has `/interface/unit/family/bridge` set.
- Checks for the following configurations on a device interface. An interface is excluded from UNI assignment when *all* of the following configurations are present and the logical interface is Unit 0:
 - An IP address is defined on the physical interface. The interface configuration on the device has `interface/unit/name/./family/inet/address/name` set. For example:

```
interfaces {
  ge-0/1/0 {
    unit 0 {
      family inet {
        address 10.10.30.52;
      }
    }
  }
}
```

- MPLS is enabled on the physical port. The interface configuration on the device has `interface/unit/name/./family/mpls` set. For example:

```
interfaces {
  ge-0/1/0 {
    unit 0 {
      family mpls;
    }
  }
}
```

- OSPF is running on the logical interface. The interface configuration on the device has `configuration/protocols/ospf/area/interface` set. For example:

```
interfaces {
  ge-5/0/0 {
    unit 0 {
      family inet {
        address 10.10.34/30;
      }
    }
  }
}
```

```
    }
    family mpls;
  }
}
protocols {
  ospf {
    traffic-engineering;
    area 0.0.0.0. {
      interface ge-5/0/0.0;
    }
  }
}
```

- MPLS is running on the physical interface. The interface configuration on the device has **configuration/protocols/mpls/interface** set. For example:

```
interfaces {
  ge-5/0/0 {
    unit 0 {
      family inet {
        address 10.10.34/30;
      }
      family mpls;
    }
  }
}
protocols {
  mpls {
    interface ge-5/0/0.0;
  }
}
```

VLAN Pool Profile Classification Rules

The Junos Space software assigns VLAN pool ranges to the UNIs, depending on the configured encapsulation.

Auto Discovery Only

The Junos Space software enables the router to process only the autodiscovery network layer reachability information (NLRI) update messages for LDP-based VPLS update messages.

Related Documentation

- [Deleting UNIs on page 373](#)
- [Discovering Device Roles on page 374](#)
- [Excluding Devices from N-PE Role Assignment on page 375](#)
- [Excluding Interfaces from UNI Role Assignments on page 376](#)
- [Unassigning N-PE Devices on page 378](#)
- [Viewing N-PE Devices on page 378](#)

- [Viewing Prestaging Statistics on page 381](#)
- [Viewing Prestaging Rules on page 383](#)

CHAPTER 20

Prestaging: Managing Devices and Device Roles

- [Discovering Tunnel Devices on page 369](#)
- [Adding a UNI on page 371](#)
- [Unassigning Device Roles on page 372](#)
- [Deleting UNIs on page 373](#)
- [Discovering Device Roles on page 374](#)
- [Excluding Devices from N-PE Role Assignment on page 375](#)
- [Excluding Interfaces from UNI Role Assignments on page 376](#)
- [Unassigning N-PE Devices on page 378](#)
- [Viewing N-PE Devices on page 378](#)
- [Viewing Prestaging Statistics on page 381](#)
- [Viewing Prestaging Rules on page 383](#)
- [Managing Prestage Device Jobs on page 385](#)
- [Specifying the Wait and Idle Times for Prestaging Devices on page 387](#)

Discovering Tunnel Devices

When you start Connectivity Services Director for the first time, the system does not have any devices. The first step is to build your network. Even with large networks, Connectivity Services Director has made this step relatively easy and straightforward. You will add devices to Connectivity Services Director and the database by using a process called *device discovery*. Once a device is discovered, it shows in the interface and Connectivity Services Director begins to monitor the device.

Connectivity Services Director provides a wizard for device discovery. The following example shows the path for device discovery through the wizard. For an alternate path, you can get a step-by-step instruction from the help system.

Before you discover tunneling devices:

- Ensure that the devices that you want to discover are configured for MPLS with the required interface in the Junos OS configuration hierarchy [edit protocols mpls]. See the *Junos Software MPLS Configuration Guide*.

In this example, we provide an IP address range, and Connectivity Services Director populates the database with all supported devices within that range.

1. While in the **Build** mode, select **Device View** or **Custom Group View** from the View selector.
2. To discover physical devices, click **Discover Devices** in the Tasks pane. Each mode has a Tasks Pane that displays the actions you can take while in that mode and that particular network view.
3. (Optional) Type a name for the discovery job. The default name is ND Discovery.
4. Click **Add** in the Device Targets window. You can add a single device IP address, a range of IP addresses, an IP subnet, or a hostname. In this example, we select an IP address range.
5. Provide the initial or the lowest IP address value and the ending or highest IP address value for the range and click **Add**. You can have up to 1024 devices in a range. After you click Add, the address range is listed in the Device Targets window.
6. Click **Next** or click **Discovery Options** to proceed to specify the device credentials and method of discovery.
7. Click **Add** in the Device Credentials window and enter the username and password assigned for administrative access.
8. Select **Ping**, **SNMP**, or both as the method of device discovery. Selecting both is the preferred method if the device is configured for SNMP.

If you select SNMP, the Add SNMP Settings dialog box is displayed. In this example, because we run SNMP version 2, we need to provide the community string. Click **Add** to save the setting.



NOTE: You cannot choose a method for device discovery for virtual network discovery.

9. Click **Next** or **Schedule Options** to proceed to schedule the time when discovery is run.



NOTE: Scheduling options are not available for virtual network discovery.

10. Indicate whether to run the device discovery now or set up a schedule to minimize network traffic. In this example, we set the schedule to run during off hours.
11. Click **Review** to review the settings before you exit the wizard.
12. Click **Finish** to complete the discovery setup and to save the settings.
13. Click **View Discovery Status** to view all scheduled and completed jobs. After a job completes, you can click **Show Details** to view further information on any unexpected results.

Adding a UNI

To add a UNI to the list of UNIs that can be assigned to a service on a specific device:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.
4. In the **Devices Chart** window, select the device on which you want to add an interface to the list of potential UNIs.
5. Click **Manage Interface Roles** to assign UNI interfaces to the specified device.
6. The **Manage Interface Roles** window appears, displaying all interfaces on the device that have not been assigned.
7. Select the check box under the UNI column to specify the interface you want to make available for assignment as a UNI. To select multiple interfaces, use the multiple selection feature.
8. Click **OK** to submit the configuration changes. You are returned to the Devices Chart page.

Related Documentation

- [Unassigning Device Roles on page 372](#)
- [Deleting UNIs on page 373](#)
- [Discovering Device Roles on page 374](#)
- [Excluding Devices from N-PE Role Assignment on page 375](#)
- [Excluding Interfaces from UNI Role Assignments on page 376](#)
- [Unassigning N-PE Devices on page 378](#)
- [Viewing N-PE Devices on page 378](#)
- [Viewing Prestaging Statistics on page 381](#)
- [Viewing Prestaging Rules on page 383](#)

Unassigning Device Roles

If you need to exclude devices from role assignment, or you need to exclude interfaces from the list of interfaces that can be used as UNIs, use the procedures documented in [“Discovering and Assigning N-PE Devices with Exceptions” on page 353](#).

To unassign all discovered roles and interfaces:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.
4. In the **Devices Chart** window, select the device on which you want to add an interface to the list of potential UNIs.
5. Click **Manage Device Roles** and from the drop-down list, select **Unassign Role** to remove the role capability of a network element. You are prompted to confirm the operation. If you click **OK**, a request is submitted to remove the latest role of the network element or device.

The device is removed from the list of network elements displayed on the Devices Chart page.

6. To view the assignment status, in the **Job Management** window from the Junos Space Platform UI, click the job ID of the assignment job.



NOTE: Alternatively, to display the Job Management page, click the **System** icon on the Connectivity Services Director banner, and select **Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

Related Documentation

- [Adding a UNI on page 371](#)
- [Deleting UNIs on page 373](#)
- [Discovering Device Roles on page 374](#)
- [Excluding Devices from N-PE Role Assignment on page 375](#)
- [Excluding Interfaces from UNI Role Assignments on page 376](#)
- [Unassigning N-PE Devices on page 378](#)
- [Viewing N-PE Devices on page 378](#)
- [Viewing Prestaging Statistics on page 381](#)
- [Viewing Prestaging Rules on page 383](#)

Deleting UNIs

After performing the initial assignment of N-PE devices and UNIs, you can still exclude additional interfaces from the list of UNIs so long as those UNIs are not assigned to services.

To remove an interface from consideration as a UNI:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.
4. In the **Devices Chart** window, select the device on which you want to add an interface to the list of potential UNIs.
5. Click **Manage Interface Roles**.

The **Manage Interface Roles** window appears, showing all interfaces assigned the UNI role.

6. Select the interface you no longer want to have the UNI role. To unassign multiple interfaces, use the multiple selection feature.



NOTE: The UNI role is assigned to an interface by a notification from the managed device that is sent to the Connectivity Services Director application, even when you unassign the UNI role from the interface using the Prestage Devices workspace. For example, if you unassign the UNI role on an interface of a managed device, that interface is available for provisioning services on devices, when you attempt to create a service order. For the same interface, if you configure encapsulation on it directly from the device and navigate to the Prestaging workspace in Connectivity Services Director after a few minutes, the interface status indicates that UNI role is configured on it. This behavior occurs because the UNI role is assigned to the interface by a device notification.

7. Click **OK** to submit the selection. You are returned to the Devices Chart page.

Related Documentation

- [Adding a UNI on page 371](#)
- [Unassigning Device Roles on page 372](#)
- [Discovering Device Roles on page 374](#)
- [Excluding Devices from N-PE Role Assignment on page 375](#)
- [Excluding Interfaces from UNI Role Assignments on page 376](#)
- [Unassigning N-PE Devices on page 378](#)
- [Viewing N-PE Devices on page 378](#)
- [Viewing Prestaging Statistics on page 381](#)
- [Viewing Prestaging Rules on page 383](#)

Discovering Device Roles

To discover the roles of devices found during element discovery:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.

4. In the **Devices Chart** window, select the device on which you want to add an interface to the list of potential UNIs.
5. Click **Manage Device Roles** and from the drop-down list, select **Discover Role** to retrieve the role capability of a network element. A job is created to obtain the latest role of the network element or device.

Device role discovery is now complete. To assign device and interface roles, follow the steps in the next section, [“Discovering and Assigning All N-PE Devices” on page 351](#).

Related Documentation

- [Adding a UNI on page 371](#)
- [Unassigning Device Roles on page 372](#)
- [Deleting UNIs on page 373](#)
- [Excluding Devices from N-PE Role Assignment on page 375](#)
- [Excluding Interfaces from UNI Role Assignments on page 376](#)
- [Unassigning N-PE Devices on page 378](#)
- [Viewing N-PE Devices on page 378](#)
- [Viewing Prestaging Statistics on page 381](#)
- [Viewing Prestaging Rules on page 383](#)

Excluding Devices from N-PE Role Assignment

The rules-driven process that the Connectivity Services Director application uses to discover device roles recommends the correct roles in most cases. To exclude a device from N-PE role assignment:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.
4. In the **Devices Chart** window, select the device on which you want to add an interface to the list of potential UNIs.
5. Click **Manage Device Roles** and from the drop-down list, select **Unassign Role** to remove the role capability of a network element. You are prompted to confirm the operation. If you click **OK**, a request is submitted to remove the latest role of the network element or device.

The device is removed from the list of network elements displayed on the Device Statistics page.

**Related
Documentation**

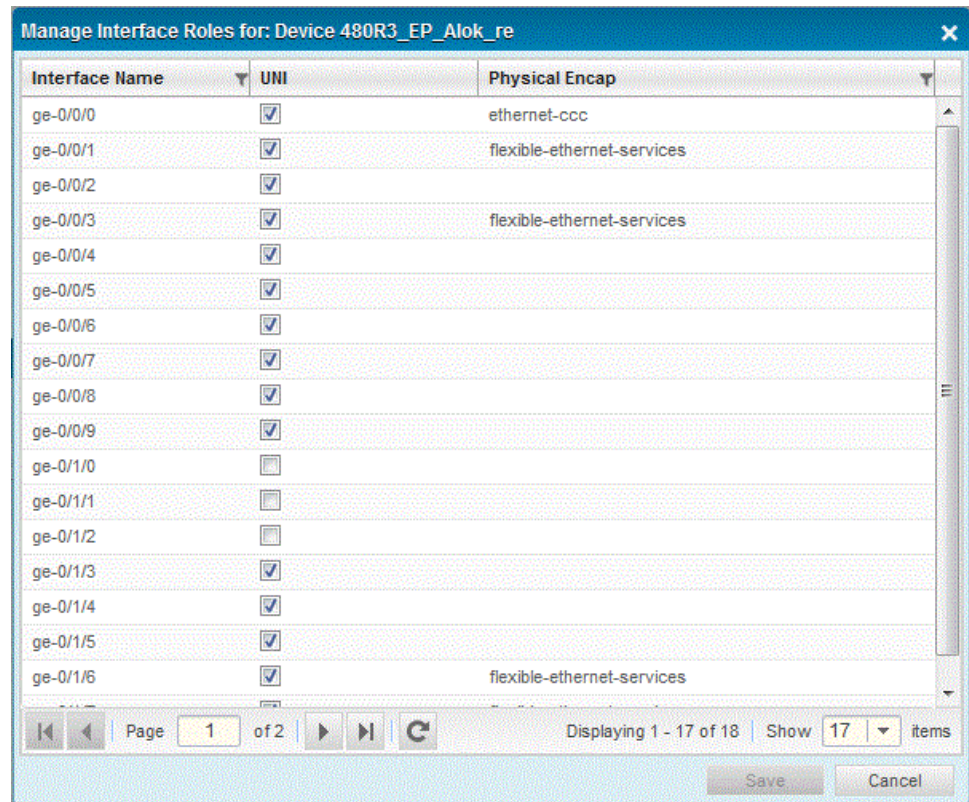
- [Adding a UNI on page 371](#)
- [Unassigning Device Roles on page 372](#)
- [Deleting UNIs on page 373](#)
- [Discovering Device Roles on page 374](#)
- [Excluding Interfaces from UNI Role Assignments on page 376](#)
- [Unassigning N-PE Devices on page 378](#)
- [Viewing N-PE Devices on page 378](#)
- [Viewing Prestaging Statistics on page 381](#)
- [Viewing Prestaging Rules on page 383](#)

Excluding Interfaces from UNI Role Assignments

To exclude interfaces from the list of interfaces that the prestaging rules determined were suitable for use as UNIs:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.
4. In the **Devices Chart** window, select the device on which you want to add an interface to the list of potential UNIs.
5. Click **Manage Interface Roles**.

The **Manage Interface Roles** window appears, showing all interfaces assigned the UNI role.



6. Deselect the check box under the UNI Role column for the interface you no longer want to have the UNI role. To unassign multiple interfaces, use the multiple selection feature.
7. Click **OK** to submit the selection. You are returned to the Device Statistics page.

Related Documentation

- [Adding a UNI on page 371](#)
- [Unassigning Device Roles on page 372](#)
- [Deleting UNIs on page 373](#)
- [Discovering Device Roles on page 374](#)
- [Excluding Devices from N-PE Role Assignment on page 375](#)
- [Unassigning N-PE Devices on page 378](#)
- [Viewing N-PE Devices on page 378](#)
- [Viewing Prestaging Statistics on page 381](#)
- [Viewing Prestaging Rules on page 383](#)

Unassigning N-PE Devices

To unassign an N-PE device so that it can no longer be assigned to a service:



NOTE: Before you unassign an N-PE device, it must not be assigned to any deployed service.

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.
4. In the **Devices Chart** window, select the device on which you want to add an interface to the list of potential UNIs.
5. Click **Manage Device Roles** and from the drop-down list, select **Unassign Role** to remove the role capability of a network element. You are prompted to confirm the operation. If you click **OK**, a request is submitted to remove the latest role of the network element or device.

The device is removed from the list of network elements displayed on the Devices Chart page.

Related Documentation

- [Adding a UNI on page 371](#)
- [Unassigning Device Roles on page 372](#)
- [Deleting UNIs on page 373](#)
- [Discovering Device Roles on page 374](#)
- [Excluding Devices from N-PE Role Assignment on page 375](#)
- [Excluding Interfaces from UNI Role Assignments on page 376](#)
- [Viewing N-PE Devices on page 378](#)
- [Viewing Prestaging Statistics on page 381](#)
- [Viewing Prestaging Rules on page 383](#)

Viewing N-PE Devices

You can view network devices that have been assigned the N-PE role or provider (P) role.

The following topic provides a procedure for viewing N-PE devices:

- [Viewing N-PE Devices in a Table on page 379](#)

Viewing N-PE Devices in a Table

To view N-PE devices in a table:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.

The **Devices Chart** page displays the following information about all N-PE devices on your network:

- Name—The assigned device name.
 - Roles—The role assigned to the device.
 - Management address—The IP address to which the Junos Space fabric connects to the device.
 - Loopback address—The IP address type used by a device to send a packet to itself.
4. To view more device details and UNI information, double-click the table row for the device. Alternatively, select a service, and click **Device Details** at the top of the table. The **NPE Details** window appears. The detailed view lists all UNIs discovered on the

device with the applied VLAN pool profile and includes the following device information:

Prestaged Device Details: 480R3_EP_Alok_re

Name: 480R3_EP_Alok_re
 Version: 14.2-20140916.0
 Platform: MX480
 Connection: up
 Loopback Address: 128.216.194.108

UNI	NNI	Admin Group	Path
UNI Name	Physical Encap		
ge-0/0/0	flexible-ethernet-services		
ge-0/0/1	none		
ge-0/0/2	none		
ge-0/0/3	none		
ge-0/0/4	none		
ge-0/0/5	none		
ge-0/0/6	none		
ge-0/0/7	none		
ge-0/0/8	none		
ge-0/0/9	none		

Page 1 of 2 | Displaying 1 - 14 of 24 | Show 14 items

Close

- Name—The name assigned to the device
- Version—Operating system firmware version running on the device. For example, 13.1X49D29.1.
- Platform—Device model number or the platform type of the discovered device. For example, MX480.
- Loopback address—The IP address type used by a device to send a packet to itself.
- Connection status—up or down.
- Service capability—N-PE device role: L2 or L3.

The following tabs are displayed:

- **UNI**—All assigned user-to-network interfaces (UNIs) on the device with the applied VLAN pool profile. “0” in the Encapsulation field means that no encapsulation has been applied and the UNI is available for allocation.
- **NNI**—All the assigned network-to-network interfaces (NNIs) on the device. Also, the encapsulation types defined for the NNI interfaces are shown.
- **Admin Groups**—Names of the administrative groups configured for the interfaces on the device. Administrative groups, also known as link coloring or resource class, are manually assigned attributes that describe the “color” of links, such that links with the same color conceptually belong to the same class. You can use administrative groups to implement a variety of policy-based LSP setups. Administrative groups are meaningful only when constrained-path LSP computation is enabled.
- **Path**—The path name, IP address, and type are shown.

Related Documentation

- [Adding a UNI on page 371](#)
- [Unassigning Device Roles on page 372](#)
- [Deleting UNIs on page 373](#)
- [Discovering Device Roles on page 374](#)
- [Excluding Devices from N-PE Role Assignment on page 375](#)
- [Excluding Interfaces from UNI Role Assignments on page 376](#)
- [Unassigning N-PE Devices on page 378](#)
- [Viewing Prestaging Statistics on page 381](#)
- [Viewing Prestaging Rules on page 383](#)

Viewing Prestaging Statistics

The landing page for the Prestage Devices workspace contains charts and graphs that provide information about available capacity on discovered N-PE devices. You can determine which devices have UNIs available, or which devices have plenty of available capacity for routing services.

The following topics describe viewing statistics in the Prestage Devices workspace landing page:

- [Viewing the Prestaged Device Details on page 381](#)
- [Viewing Services for Devices and Device Roles in a Graphical Form on page 382](#)

Viewing the Prestaged Device Details

To view the details of the prestaged devices:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.

The **Prestage Devices** page in the lower part of the right pane displays the following information about all N-PE devices on your network:

- Name—The assigned device name.
 - Roles—The role assigned to the device.
 - Service Capability—Indicates whether the device is capable of supporting Layer 2, Layer 3, or MPLS services.
 - Management address—The IP address to which the Junos Space fabric connects to the device.
 - Loopback address—The IP address type used by a device to send a packet to itself.
4. Enter a criterion in the Search box and press Enter to sort and filter the devices that match the search condition.

Viewing Services for Devices and Device Roles in a Graphical Form

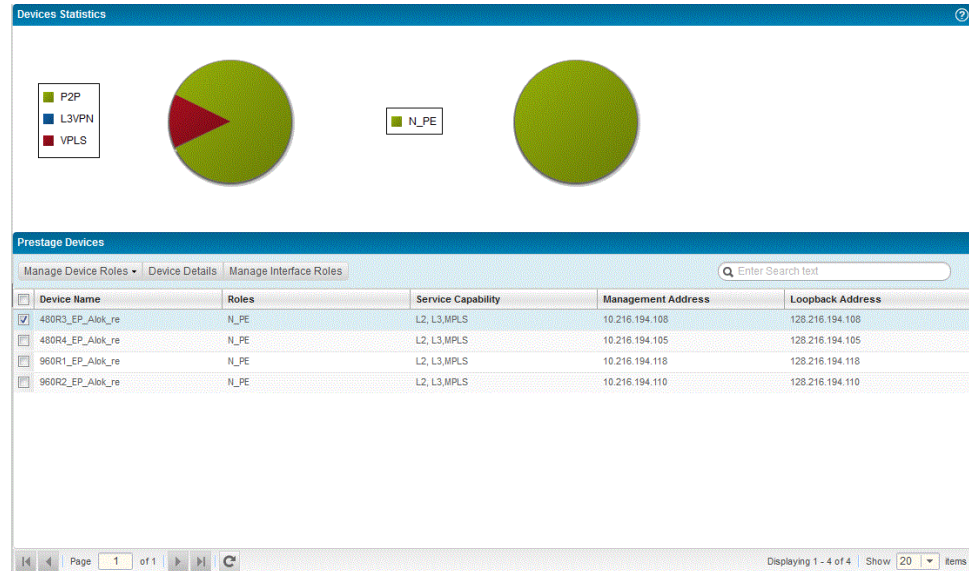
To view the number of services provisioned on each N-PE device and the number of devices with different roles in your network:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.

The **Device Statistics** page in the upper part of the right pane displays two pie charts. One of the pie charts represents the different types of services configured on devices in your network. You can remove or restore a category (segment) from the pie chart by clicking that segment in the chart. A color-code is used to denote different portions of the pie chart for the service types. Mouse over each portion of the pie to view the number of services corresponding to the percentage of each service type. The color-coding legends reference the service types, such as E-LINE Martini, E-LINE Kompella, L3VPN, VPLS, and P2P services.

The other pie chart displays the roles of devices, such as network provider edge (N-PE) and provider (P) roles. A color-code is used to denote different portions of the pie

chart for the device roles. Mouse over each portion of the pie to view the number of devices corresponding to the percentage of each device role. The color-coding legends reference the device roles, such as N-PE or P.



Related Documentation

- [Adding a UNI on page 371](#)
- [Unassigning Device Roles on page 372](#)
- [Deleting UNIs on page 373](#)
- [Discovering Device Roles on page 374](#)
- [Excluding Devices from N-PE Role Assignment on page 375](#)
- [Excluding Interfaces from UNI Role Assignments on page 376](#)
- [Unassigning N-PE Devices on page 378](#)
- [Viewing N-PE Devices on page 378](#)

Viewing Prestaging Rules

Prestaging rules contain criteria for classifying the MPLS role of each device and recommending which physical interfaces should be UNI interfaces. For each recommended UNI interface, the system recommends its primary loopback address.

These prestaging rules are predefined and cannot be configured. They are neither selectable nor configurable. However, you can modify the results of the rules before committing the recommended assignments to the database.

The following topic shows how to view prestaging rules. You can view a summary of all prestaging rules, see a summary, or view details of a specific prestaging rule.

- [Viewing Prestaging Rules in a Table on page 384](#)

Viewing Prestaging Rules in a Table

To view prestaging rules in a tabular format:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Rules**.

The **Rules** window appears.

Prestage Rules		
Name	Rule Type	Description
BX match	NPE_Rule	If BX device, check for ldp enable
Loopback check	NPE_Rule	If no loopback interface is detected or no IP address is configured on the loopback interface do not assign NPE role to the device
I2vpn/vpls enabling check	NPE_Rule	Check if I2vpn signaling is enabled for bgp for I2vpn or vpls
I2vpn auto-discovery check	NPE_Rule	Check if I2vpn auto discovery is enabled for bgp based VPLS
Comment match	NPE_Rule	If keyword NPE is found in the configuration interface lo0 description field assign NPE role to the device
AS Number check	NPE_Rule	Check if AS Number is configured on the device
MPLS check	NPE_Rule	Check if MPLS is enabled on an interface
I2VPN signaling check	NPE_Rule	Check if I2vpn signaling is enabled for bgp for I2vpn or vpls
LDP check	NPE_Rule	Check if LDP is enabled on loopback interface
L3vpn enabling check	NPE_Rule	Check if inet-vpn anyunicast/multicast is enabled for bgp
Filter for ge participating AE port	UNI_Rule	If GE participating AE interfaces are detected drop it from UNI role
Filter for bridge family on logical interface	UNI_Rule	Do not assign UNI role to interface with bridge family on logical interface
Filter for MPLS enabled physical ports	UNI_Rule	Do not assign UNI role to interfaces with family mpls on unit 0
Filter for irb Ports	UNI_Rule	If IRB interface is detected
Filter for lt Ports	UNI_Rule	If LT interface is detected
Filter for AE port	NNI_Rule	If AE interfaces are detected
Filter for Ethernet Ports	NNI_Rule	If GE-100g, GE, GE-10g, SONET interfaces are detected
Filter for used IP port-based interfaces	UNI_Rule	Do not assign UNI role to interfaces with IP addresses on unit 0
Filter for fe participating AE port	UNI_Rule	If FE participating AE interfaces are detected drop it from UNI role
VLAN pool assignment	VLAN_CCC_Rule	Depending on encapsulation detected on the UNIs, correct VLAN pool ranges are assigned to the UNIs. [vlan-ccc:512-4094] [flexible-ethernet-...
L2E check	L2E_Rule	Check if L2 Extension is enabled on the device
L2Ring check	L2B0_Rule	Check if L2 Ring is configured on a device
No tunnel services	VPLS_PVW_Label...	Enables static partitioning of vpls labels
Filter for GRE port	NNI_Rule	If GR interfaces are detected
Check if static LSP is configured	MPLS_DEVICE_Rule	Filter those devices on which MPLS is not running, cant be part of TA
Check for MPLS enabled interfaces	MPLS_DEVICE_Rule	Check if any of the interfaces are enabled with MPLS

The **Rules** window lists all the prestaging rules by type, along with the name and a brief description of each rule.

- Name—The name of the prestaging rule.
- Rule Type—The category of the rule, such as an NNI rule or a UNI rule.
- Description—Textual description that illustrates the purpose and functionality of the rule.
- Loopback address—The IP address type used by a device to send a packet to itself.

Related Documentation

- [Adding a UNI on page 371](#)
- [Unassigning Device Roles on page 372](#)
- [Deleting UNIs on page 373](#)
- [Discovering Device Roles on page 374](#)

- [Excluding Devices from N-PE Role Assignment on page 375](#)
- [Excluding Interfaces from UNI Role Assignments on page 376](#)
- [Unassigning N-PE Devices on page 378](#)
- [Viewing N-PE Devices on page 378](#)

Managing Prestage Device Jobs

Connectivity Services Director enables you to view and manage device prestaging jobs. You can view the status of completed prestaging jobs and cancel the prestaging jobs that are scheduled to execute at a later time or jobs that are in progress.

After Junos Space has discovered the devices, a two- or three-stage process to prestage devices is performed automatically in the backend by the Connectivity Services Director application. Prestaging is the process of preparing the devices to be compatible and qualified for configuration of services, by discovering the roles of devices and assigning network-provider edge (N-PE) roles as necessary. Because auto prestaging is an automated process triggered by the change events from the device and platform, there can be multiple parallel prestaging jobs from a single device and from multiple devices. These jobs update the corresponding device information on completion.

Manual prestaging process prestages the entire device inventory and automatically assign device roles to them. Therefore, having a per-device auto prestaging job running in parallel might be redundant for the functionality because the concerned device could most likely be taken care by the manual prestaging job.

The Prestage Device Jobs page shows the progress and status of the role assignment job. Although you can view details about the status of all the jobs initiated in the Connectivity Services Director application from the Prestage Device Jobs page accessible as a System task, you can use the Prestage Device Jobs page in Build mode of Service view to obtain a filtered display of only the prestaging jobs for easy analysis and debugging.

To display the Prestage Device Jobs page:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services > Connectivity** task pane, select **Prestage Devices > View Prestage Jobs**.

The **Prestage Device Jobs** window appears.

4. To view the details of a job, select a row and click **Show Details** or double-click a row.
5. To cancel a scheduled job, select a job that is scheduled for a later time or a job that is in progress and click **Cancel**.

The fields in the Prestaging Device Jobs page are described in [Table 59 on page 386](#). To view any hidden column, keep the mouse on any column heading and select the down arrow and then click Columns. Select the check box to display the hidden columns.



NOTE: Details of jobs initiated from Connectivity Services Director will be available only from Connectivity Services Director. These jobs will not be listed in the Prestage Device Jobs pane in Junos Space platform and vice-versa.

Table 59: Prestage Device Jobs Page Fields

Field	Description
Job ID	The unique ID assigned to the job
Name	The name of the job
Percent	The percentage of completion of the job
State	The status of the job: <ul style="list-style-type: none"> • Success—Job completed successfully • Failure—Job failed and was terminated • Job Scheduled—Job is scheduled but has not yet started • In progress—Job is has started, but not completed • Cancelled—Job is cancelled
Job Type	The type of the job
Summary	Summary of the job scheduled and executed with status
Scheduled Start Time	The time when the job is scheduled to start
Actual Start Time	The actual time when the job started
End Time	The time when the job was completed
User	The login ID of the user that initiated the task
Recurrence	The recurrent time when the job will be restarted.

- Related Documentation**
- [Managing Service Configuration Deployment Jobs on page 1003](#)
 - [Deploying Services Configuration to Devices on page 1005](#)

Specifying the Wait and Idle Times for Prestaging Devices

After Junos Space has discovered the devices, a two- or three-stage process to prestage devices is performed automatically in the backend by the Connectivity Services Director application. Prestaging takes the devices already under Junos Space management and prepares them for service activation by assigning roles to those devices and their interfaces..

To specify the wait and idle times to be used for triggering jobs for prestaging devices:

1. From the Junos Space user interface, click the **System** icon on the Connectivity Services Director banner.

The options that you can configure in System mode are displayed in a drop-down menu.

2. Select **Preferences** from the drop-down menu to open the Preferences page.

The Preferences page opens with User Preferences as the default tab.

3. Click the **Services Activation** tab to configure the services activation-related settings.

The settings that you can configure on the Services Activation tab are displayed.

4. Click the right arrow beside the **Prestage Device** section to expand it.

The parameters that you can configure for prestaging devices are displayed.

5. In the **Pre-stage Wait Time (Sec)** field, specify the number of seconds for which the task to trigger a job for prestaging devices must wait after receiving the first notification for prestaging devices. For example, if you specify the prestage wait time as 20 seconds, the prestaging task waits for a period of 20 seconds, after receiving the first notification for prestaging devices, and then initiates the prestaging-devices job.

6. In the **Pre-stage Idle Time (Sec)** field, specify the number of seconds after which the job for prestaging devices is initiated, if no notification is received during the idle period. For example, if you specify the prestage idle time as 10 seconds and if no notification for prestaging devices is received within this period, the job for prestaging devices is triggered immediately after 10 seconds. The prestage idle time value takes precedence over the prestage wait time value.

7. Click **OK** to save the settings. You are prompted to confirm the changes you made to services-activation preferences.
8. Click **Yes** to confirm. The Preferences page is closed. A dialog box is displayed to confirm the successful saving of the preferences. Click **OK** to close the dialog box.

**Related
Documentation**

- [Modifying the Application Settings of Connectivity Services Director on page 1082](#)

Prestaging: Managing IP Addresses

- [Creating an IP Address Pool on page 389](#)
- [Managing Resources on page 391](#)
- [Specifying IPv4 Addressing Assignment in Layer 3 VPN Service Definitions on page 394](#)

Creating an IP Address Pool

You, the Service Designer, can create consistent IP address pools for Layer 3 VPNs by selecting **Prestage Devices > Resources > Add IP Address Pools** from the Network Services > Connectivity task pane in Build mode of Service View. The IP addresses assigned to each PE/CE link need to allow routing across the customer's entire Layer 3 VPN, as long as the PE/CE addresses are not exposed outside of that VPN. If the PE/CE link addresses are accessible from outside the customer's VPN, then those IP addresses may also need to be globally unique across the internet, instead of just within the customer's VPN.

When you create an IP address pool, it appears in the **Prestage Devices > Resources** inventory page. See [“Creating an IP Address Pool” on page 389](#)



NOTE: Preferably, create all IPv4 address pools at the beginning of the prestaging process (see [“Prestaging Devices Overview” on page 53](#)), before you run Role Discovery (see [“Discovering and Assigning All N-PE Devices” on page 351](#)), so that any IPv4 IP addresses found on devices during the role discovery process can be marked as already allocated in the corresponding IPv4 IP address pools.

To create an IPv4 IP address pool:

1. In the **Network Services > Connectivity** task pane, select **Prestage Devices > Manage Resources**. The Resource Utilization Status page is displayed. The status of various resources such as VLAN, virtual circuit, route target, route distinguisher, and IP address pool are displayed in a tabular format. You can create a customized IP pool based on your network deployment needs.
2. Under the Allocated column, click the link in the displayed number to open the Resource Allocated Details dialog box. If the resource pool is an IP address pool, the IP addresses allocated from the selected resource pool are displayed in a table.

Similarly, for other resources such as VLAN or virtual circuit, information regarding the element or device to which the resource is allocated is displayed.

3. Click **Add** at the top of the table of displayed resources. The **Add IP Address Pool** dialog box appears.

Figure 28: Add New IP Pool Dialog Box

4. In the **Pool Type** drop-down list box, select the IP pool type as either **Global** or **Customer**.
 - A **Global** IP address pool pertains to the service provider. There can be more than one global IPv4 address pool. However, each global pool must have its own unique name and its set of IPv4 addresses must not overlap with those of any other global pool. You can allocate addresses from global pools across multiple Layer 3 VPNs across multiple customers.
 - A **Customer** IP address pool pertains to an existing customer. These pools are associated with the corresponding customer. You can associate more than one customer IPv4 pool with each customer. However, each customer pool must have its own set of IPv4 addresses which must not overlap with those of any other pool belonging to the same customer. You can allocate addresses from customer pools across multiple Layer 3 VPNs for a particular customer.
5. In the **Pool Name** field, enter a unique name.
An IP address pool name can be no more than 50 characters.
6. In the **IP Address Pool** field, enter an IPv4 IP address pool.

Any IPv4 address pool in Junos Space maps directly onto the Classless Interdomain Routing (CIDR) notation for IPv4 network addresses. The CIDR network address, 192.168.1.0/24 is a contiguous block of 256 individual IPv4 addresses: 192.168.1.0/32 through 192.168.1.255/32, inclusive. The network address 10.0.99.20/30 is a contiguous block of 4 individual IPv4 addresses: 10.0.99.20/32 through 10.0.99.23/32, inclusive. As a consequence, any Junos Space IPv4 address pool directly maps to (and is identified by) its CIDR network address. The Junos Space IPv4 address pool, 192.168.1.0/24, contains all of the addresses from 192.168.1.0/32 to 192.168.1.255/32,

while the IPv4 address pool, 10.0.99.20/30 contains all of the addresses from 10.0.99.20/32 to 10.0.99.23/32.

7. In the **Subnet (/)** field, enter the destination IP prefix length or the subnet mask. The subnet mask indicates the number of bits used for the network portion of the address (for example, 10.10.20.0/24).
8. If you are creating a **Customer** IP address pool, the **Associate with customer** drop-down list box appears. Select an existing customer name. To create a customer, see [“Adding a New Customer” on page 737](#).
9. Click **Create**.

Junos Space saves the IP address pool information in the database. The IP address pool appears in the **Resources** inventory page. The **Pool Type** column differentiates global from customer IP address pools.



NOTE: You need to create IP address pools only if the operation of your network requires it. Alternatively, you can use the global IP pools provided by the Connectivity Services Director application for Layer 3 VPN services.



NOTE: When you delete an IP address pool, you must ensure that such a pool is not being currently utilized or allocated to a managed element. Otherwise, you cannot delete such an allocated IP address pool.

Related Documentation

- [Managing Resources on page 391](#)
- [Specifying IPv4 Addressing Assignment in Layer 3 VPN Service Definitions on page 394](#)

Managing Resources

You can use the Manage Resource page to view existing IP address pools created for global use or for specific customers. Besides the IP address pool information, the status of various other resources such as VLAN IDs, virtual circuit IDs, route distinguisher, and route targets that are created for utilization in services is also displayed. You can also view the details of allocated or utilized resources, such as the VLAN ID allocated to the corresponding interface and the logical unit association with a particular interface on a device. For more information about creating an IPv4 IP address pool, see [“Creating an IP Address Pool” on page 389](#).

Viewing Resources

Starting in Connectivity Services Director Release 2.1R1, you can view and manage a particular pool of resources by selecting an option from the **Pool Type** list. The **Manage Resource** page displays the list of resource pools that can be configured. You can filter

the resources displayed on this page by device name, interfaces on the device, and a customer associated with the device.

Figure 29: Manage Resource Page

Pool Name	Description	Allocated
global-vcid-pool	Global pool of VC-Ids	2
IPv4 Resource Pool:10.0.77.0/24	Pool of IPv4 Addresses: 10.0.77.0/24	0
IPv4 Resource Pool:10.0.88.0/24	Pool of IPv4 Addresses: 10.0.88.0/24	0
IPv4 Resource Pool:10.0.99.0/24	Pool of IPv4 Addresses: 10.0.99.0/24	0
AsRTPool36000	RT Pool for AS36000	10
AsRDPool36000	RD Pool for AS36000	5
AsRTPool6810	RT Pool for AS6810	1
AsRDPool6810	RD Pool for AS6810	1
AsRTPool107	RT Pool for AS107	0
AsRDPool107	RD Pool for AS107	0
AsRTPool65501	RT Pool for AS65501	0
AsRDPool65501	RD Pool for AS65501	0

Viewing Detailed Resources Information

To view and manage detailed information about resources:

1. In the Connectivity Services Director application, select **Service View** from the Views list.
2. From the Tasks pane, select **Prestage Devices > Manage Resource**.
The Manage Resource page is displayed.
3. Fill in the fields in the Manage Resource page as indicated in [Table 60 on page 392](#).

Table 60: Resource Pool Landing Page Details

Detail	Description
Pool Type	<p>Select one of the following options from the list:</p> <ul style="list-style-type: none"> • Global Pool—to manage pools of IPv4 addresses related to the service provider. • Unit Pool—to manage units for interfaces in a resource pool. • VLAN Pool—to manage pools of IPv4 address for a VLAN. • Customer IP Pool—to manage pools of IPv4 addresses applicable to a particular customer.
Device Name	<p>Select a device from the list to view resource types specific to interfaces on that device.</p> <p>NOTE: This field is available only if you select Unit Pool or VLAN Pool from the Pool Type list.</p>

Table 60: Resource Pool Landing Page Details (continued)

Detail	Description
Interface Name	Choose an interface of the selected device from the list. NOTE: This field is available only if you select Unit Pool or VLAN Pool from the Pool Type list.
Customer	Click Select to view the list of customers. The Choose Customer window is displayed. To choose a customer, select the check box next to the customer and click OK .
Filter	Click Filter to execute the search.
Add	Click Add to add a new IPv4 address pool.
Delete	Click Delete to delete an existing IPv4 address pool.
Pool Name	This column displays the names of IPv4 address pools.
Description	This column displays the user-defined description of the resource pool.
Allocated	This column displays the number of resources allocated from the pool.

**Related
Documentation**

- [Creating an IP Address Pool on page 389](#)
- [Specifying IPv4 Addressing Assignment in Layer 3 VPN Service Definitions on page 394](#)

Specifying IPv4 Addressing Assignment in Layer 3 VPN Service Definitions

You, the Service Designer, can specify the IPv4 IP address settings to use for PE/CE link when provisioning Layer 3 VPN service definitions.

When configuring Layer 3 VPNs, it is necessary to assign consistent IP addresses to the logical interfaces on both sides of each PE/CE link. The IP addresses assigned to each PE/CE link need to allow routing across the customer's entire Layer 3 VPN, and only need to be unique within the confines of the customer's VPN, as long as the PE/CE addresses are not exposed outside of that VPN. If the PE/CE link addresses are accessible from outside of the customer's VPN, then those IP addresses may also need to be globally unique across the Internet, instead of just within the customer's VPN.

The Connectivity Services Director application automatically assigns IPv4 addresses to both sides of each PE/CE link, as well as keeps track of which IPv4 addresses are already in use. It ensures the correct assignment of IP addresses and prevents the reuse of IP addresses.

To specify auto-assigning of the PE/CE link addresses from IPv4 pools, you select the **Auto Pick** option, the **IP pool type—global** or **customer**, and the number of contiguous IPv4 addresses—**size of the IPV4 address block** that is allocated for each PE/CE link. Which particular global or customer IPv4 address pool to use is chosen during service provisioning when filling out the L3VPN Service Order.

For auto-assignment scenarios, the service designer can always select the **Allow editing in Service Order** option at the right of each service definition setting to allow the corresponding IPv4 pool setting to be overridden later when filling out the L3VPN Service Order.

To specify manual assignment of PE/CE link addresses, the designer simply selects the manual-assignment option.

To specify IP address settings in a Layer 3 VPN service definition:

1. In the **IP Address Settings** area **PE Interface IP Address** check boxes, select one of the following:
 - **Auto Pick**—Specifies whether PE/CE link addresses are automatically assigned from an IPv4 IP address pool.
 - **Select Manually**—Specifies whether the service designer manually assigns PE/CE link addresses from the same IPv4 IP address pool.
2. In the **IP Pool Types** drop-down list box, select one of the following:
 - **Global**—Pools of IPv4 addresses pertaining to the Service Provider. There can be more than one global IPv4 address pool. However, each global pool must have its own unique name and its set of IPv4 addresses must not overlap with those of any other global pool. You can allocate addresses from global pools across multiple Layer 3 VPN across multiple customers.

- **Customer**—Pools of IPv4 addresses pertaining to a particular customer. These pools are associated with the corresponding customer. There can be more than one customer IPv4 pool associated with each customer. However, each customer pool must have its own set of IPv4 addresses which must not overlap with those of any other pool belonging to the same customer. Addresses from customer pools can be allocated across multiple Layer 3 VPNs for a particular customer.
3. In the **IP Address Block Size** field, enter the size of the IPv4 IP address block allocated for each PE/CE link.
 4. Select the **Editable in service order** check box on the right of each IP address setting to overwrite the corresponding IPv4 IP address pool setting when creating the service order.
 5. Click another Layer 3 VPN Settings link to continue specifying settings or click **Finish**.
If you click **Finish**, the custom Layer 3 VPN service definition appears on the **Manage Service Definitions** inventory page.

- Related Documentation**
- [Creating an IP Address Pool on page 389](#)
 - [Managing Resources on page 391](#)

CHAPTER 22

Device Configuration Prerequisites to Prestaging Examples

- [Example: Base Configuration for N-PE Device in a Multipoint Service on page 397](#)
- [Example: Base Configuration for N-PE Device in a Point-to-Point Ethernet \(LDP\) Service on page 399](#)
- [Example: Base Configuration for N-PE Device in a Point-to-Point Ethernet \(LDP\) Service on page 400](#)
- [Example: Base Configuration for a P Router on page 401](#)

Example: Base Configuration for N-PE Device in a Multipoint Service

An N-PE device to be used in a multipoint service must have the following entities configured before you assign the N-PE role to the device:

- Gigabit Ethernet interfaces to the network core
- Loopback interface
- Routing options
- MPLS protocol
- BGP protocol
- OSPF protocol
- LDP protocol

The N-PE device in this configuration example has just one interface to the network core. In a more complex network in which the N-PE device connects to more than one P device, you need to configure multiple interfaces.

```
interfaces {
  ge-0/0/0 {
    unit 0 {
      family inet {
        address 10.1.22.2/30;
      }
      family mpls;
    }
  }
}
```

```

    }

    }
    lo0 {
        unit 0 {
            family inet {
                address 192.168.1.30/32;
            }
        }
    }
}
routing-options {
    autonomous-system 65410;
}
protocols {
    mpls {
        interface ge-0/0/0.0;
        interface lo0.0;
    }
    bgp {
        group CA-Peer {
            type internal;
            local-address 192.168.1.30;
            family l2vpn {
                signaling;
            }
            neighbor 192.168.1.40;
            neighbor 192.168.1.10;
            neighbor 192.168.1.20;
            neighbor 192.168.1.50;
            neighbor 192.168.1.60;
        }
    }
    ospf {
        traffic-engineering;
        area 0.0.0.0 {
            interface lo0.0 {
                passive;
            }
            interface ge-0/0/0.0;
        }
    }
    ldp {
        interface ge-0/0/0.0;
        interface lo0.0;
    }
}

```

Related Documentation

- [Example: Base Configuration for N-PE Device in a Point-to-Point Ethernet \(LDP\) Service on page 399](#)
- [Example: Base Configuration for N-PE Device in a Point-to-Point Ethernet \(LDP\) Service on page 399](#)
- [Example: Base Configuration for a P Router on page 401](#)

Example: Base Configuration for N-PE Device in a Point-to-Point Ethernet (LDP) Service

An N-PE device to be used in a point-to-point service must have the following entities configured before you assign the N-PE role to the device:

- Gigabit Ethernet interfaces to the network core
- Loopback interface
- MPLS protocol
- OSPF protocol
- LDP protocol

The N-PE device in this configuration example has just one interface to the network core. In a more complex network in which the N-PE device connects to more than one P device, you need to configure multiple interfaces.

```

interfaces {
  ge-0/0/0 {
    unit 0 {
      family inet {
        address 10.1.18.2/30;
      }
      family mpls;
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 192.168.1.20/32;
      }
    }
  }
}
protocols {
  mpls {
    interface ge-0/0/0.0;
    interface lo0.0;
  }
  ospf {
    traffic-engineering;
    area 0.0.0.0 {
      interface lo0.0 {
        passive;
      }
      interface ge-0/0/0.0;
    }
  }
  ldp {
    interface ge-0/0/0.0;
    interface lo0.0;
  }
}

```



NOTE: If the N-PE router will also be used in multipoint services, do not use this base configuration. Instead, use the base configuration for multipoint services.

Related Documentation

- [Example: Base Configuration for N-PE Device in a Multipoint Service on page 397](#)
- [Example: Base Configuration for N-PE Device in a Point-to-Point Ethernet \(LDP\) Service on page 399](#)
- [Example: Base Configuration for a P Router on page 401](#)

Example: Base Configuration for N-PE Device in a Point-to-Point Ethernet (LDP) Service

An N-PE device to be used in a point-to-point service must have the following entities configured before you assign the N-PE role to the device:

- Gigabit Ethernet interfaces to the network core
- Loopback interface
- MPLS protocol
- OSPF protocol
- LDP protocol

The N-PE device in this configuration example has just one interface to the network core. In a more complex network in which the N-PE device connects to more than one P device, you need to configure multiple interfaces.

```

interfaces {
  ge-0/0/0 {
    unit 0 {
      family inet {
        address 10.1.18.2/30;
      }
      family mpls;
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 192.168.1.20/32;
      }
    }
  }
}
protocols {
  mpls {
    interface ge-0/0/0.0;
    interface lo0.0;
  }
}

```



```

}
ospf {
  traffic-engineering;
  area 0.0.0.0 {
    interface lo0.0 {
      passive;
    }
    interface ge-0/0/0.0;
  }
}
ldp {
  interface ge-0/0/0.0;
  interface lo0.0;
}

```



NOTE: If the N-PE router will also be used in multipoint services, do not use this base configuration. Instead, use the base configuration for multipoint services.

Related Documentation

- [Example: Base Configuration for N-PE Device in a Multipoint Service on page 397](#)
- [Example: Base Configuration for N-PE Device in a Point-to-Point Ethernet \(LDP\) Service on page 399](#)
- [Example: Base Configuration for a P Router on page 401](#)

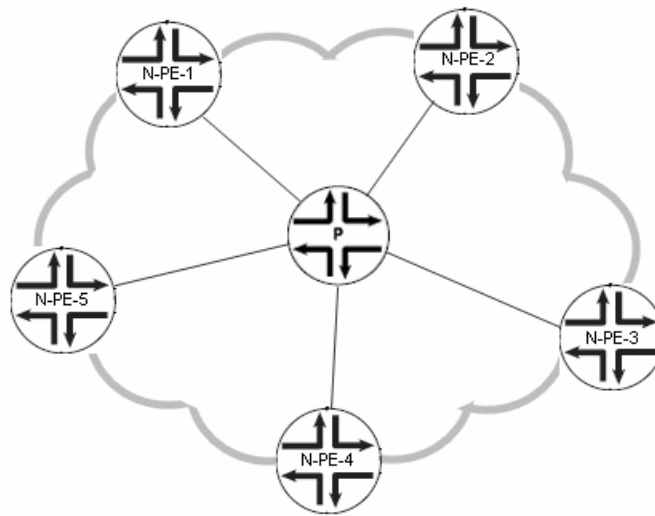
Example: Base Configuration for a P Router

P routers in your MPLS network must have the following entities configured before these devices are prestaged:

- A Gigabit Ethernet interface to each router in the network
- Loopback interface
- MPLS protocol
- OSPF protocol
- LDP protocol

[Figure 30 on page 402](#) shows a simple network with one P router connecting five N-PE routers.

Figure 30: Connectivity in a Simple Network



The following example shows a P router configuration for the simple network shown in [Figure 30 on page 402](#).

```

interfaces {
    ge-0/0/2 {
        unit 0 {
            family inet {
                address 10.1.14.1/30;
            }
            family mpls;
        }
    }
    ge-0/0/3 {
        unit 0 {
            family inet {
                address 10.1.15.2/30;
            }
            family mpls;
        }
    }
    ge-5/0/0 {
        unit 0 {
            family inet {
                address 10.1.17.1/30;
            }
            family mpls;
        }
    }
    ge-5/0/1 {
        unit 0 {
            family inet {
                address 10.1.18.1/30;
            }
            family mpls;
        }
    }
    lo0 {

```

```

        unit 0 {
            family inet {
                address 192.168.1.1/32;
            }
        }
    }
}

protocols {
    mpls {
        interface ge-0/0/2.0;
        interface ge-0/0/3.0;
        interface ge-5/0/0.0;
        interface ge-5/0/1.0;
        interface lo0.0;
    }
    ospf {
        traffic-engineering;
        area 0.0.0.0 {
            interface ge-0/0/2.0;
            interface ge-0/0/3.0;
            interface ge-5/0/0.0;
            interface ge-5/0/1.0;
            interface lo0.0 {
                passive;
            }
        }
    }
    ldp {
        interface ge-0/0/2.0;
        interface ge-0/0/3.0;
        interface ge-5/0/0.0;
        interface ge-5/0/1.0;
    }
}

```

Related Documentation

- [Example: Base Configuration for N-PE Device in a Multipoint Service on page 397](#)
- [Example: Base Configuration for N-PE Device in a Point-to-Point Ethernet \(LDP\) Service on page 399](#)
- [Example: Base Configuration for N-PE Device in a Point-to-Point Ethernet \(LDP\) Service on page 399](#)

CHAPTER 23

Prestaging Services

- [Creating and Handling a Service Recovery Request on page 406](#)
- [Selecting a Service Definition in the Wizard for Creating a Service Recovery Request on page 409](#)
- [Specifying Devices and Filters in the Wizard for Creating a Service Recovery Request on page 410](#)
- [Reviewing the Configured Settings in the Wizard for Creating a Service Recovery Request on page 413](#)
- [Viewing Service Recovery Report on page 415](#)
- [Performing a Service Recovery on a Defined Service on page 416](#)
- [Processing of Device Change Notifications Overview on page 417](#)
- [Handling of Out-of-Band Notifications for Service Recovery on page 420](#)
- [Viewing Service Recovery Instance Details on page 421](#)
- [Managing Out-of-Band Notifications for Recovered Services on page 425](#)
- [Viewing Details of an Out-of-Band Notification for Recovered Services on page 427](#)
- [Viewing Services Rejected During a Service Recovery on page 429](#)
- [Viewing Service Recovery Jobs on page 431](#)
- [Performing a Configuration Audit for Recovered Services on page 434](#)
- [Viewing Configuration Audit Results of Recovered Services on page 437](#)
- [Recovering Modifications and Deletions Performed for Existing Endpoints on page 441](#)
- [REST API Changes in Connectivity Services Director for Service Recovery on page 445](#)
- [Sample XPath Notifications Received on Devices for Deleted Endpoints on page 446](#)
- [Sample XPath Notifications Received on Devices for a Modified VPLS Service on page 449](#)
- [Sample XPath Notifications Received on Devices for a Created VPLS Service on page 453](#)
- [Sample XPath Notifications Received on Devices for a Created Layer 3 VPN Service on page 457](#)
- [Sample XPath Notifications Received on Devices for a Created Point-to-Point Service on page 458](#)

- [Sample XPath Notifications Received on Devices for CFM Profiles Associated with a P2P Service on page 459](#)
- [Sample XPath Notifications Received on Devices for CoS Profiles Associated with a P2P Service on page 461](#)

Creating and Handling a Service Recovery Request

The Service Recovery feature functions within the pre-staging operation of the Network Activate application. Service Recovery has two parts.

First, Service Recovery parses each device's configuration searching for service configurations and existing Network Activate service elements (P2P services, Layer 2 circuits, routing instances, firewalls, policy options, routing options, and OAM interface branches of Junos Space configurations that are being processed).

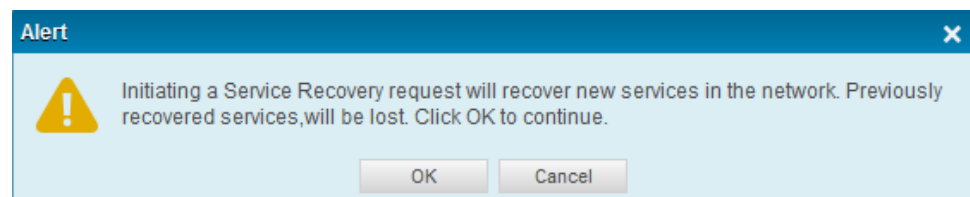
Second, Service Recovery stitches the service elements by identifying related service attributes across devices, such as VCIDs for Martini services and route targets for Kompella (L2VPN) services, to form Network Activate services.



NOTE: When you attempt to recover VPLS and L3VPN services using the Service Recovery feature, you must not select any service templates that are attached with such services for recovery. The basic configuration of services is recovered in such a scenario. This is an expected behavior with performing a service recovery for VPLS and L3VPN services. For P2P services, you can recover QoS templates that are attached with such services.

A wizard is available to create a Service Recovery request in an intuitive and easily-navigable format. The settings that you can configure in the service order are organized in separate pages of the wizard, which you can launch by clicking the appropriate buttons at the top of the Create Service Recovery Request page. Alternatively, you can proceed to the corresponding setting-related pages by clicking the Back and Next buttons at any point in the wizard during the creation of the Service Recovery request.

To perform Service Recovery, in the Network Services > Connectivity task pane, select **Service Recovery > Recover Services**. Initially, Service Recovery generates the following Alert message, which describes the process you are about to start and recommends saving previously recovered services.



To create a service recovery request:

1. From the View selector, select **Service View**.

The workspaces that are applicable to routing and tunnel services are displayed.

2. Click the **Build** icon in Service View of the Connectivity Services Director banner.

The functionalities that you can configure in Build mode are displayed on the Tasks pane.

3. From the View pane, select the **Network Services > Connectivity** node without expanding the tree and selecting a type of service.

The tasks that are applicable for the different connectivity services are displayed on the Tasks pane.

4. From the Network Services > Connectivity Tasks pane, select **Service Recovery > View Recovered Services**.

The Service Recovery page is displayed with a list of recovered services.



NOTE: The Latest Recovery Job field at the top of the page displays the job ID and job status in blue hyperlink. Click the hyperlink in the job ID and status to open the Job Details dialog box. The job ID, start and end times of the job, percentage of completion, and status of the job are displayed. Click Close to close the job dialog box.

5. The **Create Service Recovery Request** wizard contains two pages— **Select Service Recovery Options** and **Review**.

In the **Select Service Definition** page of the wizard, you can select one or more service types: P2P, VPLS, and L3VPN.

The **Select Service Definition** table on the of the **Select Service Recovery Options** page of the wizard also presents a table that lists the names of all services of the selected **Service Type**.

The **Select Devices** and **Filter Criteria** sections of the **Select Service Recovery Options** page of the wizard displays the devices and filters, with the devices listed in the **Name** column. You can specify a **VCID Range** and **Route target range** to complete the definition of the service recovery profile search.

The following topics describe the different pages of the Create Service Recovery Request wizard:

- [Selecting a Service Definition in the Wizard for Creating a Service Recovery Request on page 409](#)
- [Specifying Devices and Filters in the Wizard for Creating a Service Recovery Request on page 410](#)
- [Reviewing the Configured Settings in the Wizard for Creating a Service Recovery Request on page 413](#)

Related Documentation

- [Viewing Service Recovery Report on page 415](#)
- [Performing a Service Recovery on a Defined Service on page 416](#)

Selecting a Service Definition in the Wizard for Creating a Service Recovery Request

On the first page of the wizard to create a service recovery request, you can select the service type, which causes the page to be populated with the services that match the selected service type. For example, if you want to recover point-to-point services, you can select this service type to view the relevant services of this type. You can also select multiple service types, based on your network needs. You can select a service definition for which you want to create a service recovery request.

To select a service type and definition in the service recovery request creation wizard:

1. From the View selector, select **Service View**.

The workspaces that are applicable to routing and tunnel services are displayed.

2. Click the **Build** icon in Service View of the Connectivity Services Director banner.

The functionalities that you can configure in Build mode are displayed on the Tasks pane.

3. In the View pane, select the **Network Services > Connectivity** node without expanding the tree and selecting a type of service.

The tasks that are applicable for the different connectivity services are displayed on the Tasks pane.

4. From the Network Services > Connectivity Tasks pane, select **Service Recovery > View Recovered Services**.

The Service Recovery page is displayed with a list of recovered services.



NOTE: The Latest Recovery Job field at the top of the page displays the job ID and job status in blue hyperlink. Click the hyperlink in the job ID and status to open the Job Details dialog box. The job ID, start and end times of the job, percentage of completion, and status of the job are displayed. Click Close to close the job dialog box.

5. Click the **New** icon above the table of listed service names and service definitions.

The Select Service Recovery Options page of the Create Service Recovery Request wizard is displayed.

6. In the Select Service Definition table of the Select Service Recovery Options page, fill in the fields as described in the following table.

Field	Action
Add	<p>Click the Add button to open the Choose Service Definition page. The Choose Service Definition inventory page displays only those published service definitions designed to work with the type of services you need.</p> <p>Select the check boxes beside the types of service definitions for which you want to create a service recovery request. The search utility that is present in the Choose Service Definition dialog box that is displayed when you click Select beside the Service Definition field enables you to search by Name, Created by, and Signaling columns; the search utility is not supported for other columns in the dialog box.</p> <p>Click OK to add the selected definitions to the service recovery request. The dialog box closes and you are returned to the Select Service Definition table that lists the service definitions you selected.</p>
Delete	Select the check boxes beside the service definitions you want to remove from the service recovery request, and click the Delete button to remove the service definitions from the table.
Name	<p>Select the check boxes for the service definitions whose services you want to recover.</p> <p>All the published service definitions based on service type selected are listed.</p>

7. Proceed to [“Specifying Devices and Filters in the Wizard for Creating a Service Recovery Request” on page 410](#).

- Related Documentation**
- [Viewing Service Recovery Report on page 415](#)
 - [Performing a Service Recovery on a Defined Service on page 416](#)

Specifying Devices and Filters in the Wizard for Creating a Service Recovery Request

After you select a service definition to create a service recovery request, you can specify the devices and filters to associate with the service recovery request. The **Rule Parameters** page of the wizard displays the devices and filters, with the devices listed in the **Name** column. You can specify a **VCID Range** and **RouteTarget Range** to complete the definition of the service recovery profile search.

To specify the rule parameters in the service recovery request creation wizard:

- From the View selector, select **Service View**.
The workspaces that are applicable to routing and tunnel services are displayed.
- Click the **Build** icon in Service View of the Connectivity Services Director banner.
The functionalities that you can configure in Build mode are displayed on the Tasks pane.
- In the View pane, select the **Network Services > Connectivity** node without expanding the tree and selecting a type of service.

The tasks that are applicable for the different connectivity services are displayed on the Tasks pane.

4. From the Network Services > Connectivity Tasks pane, select **Service Recovery > View Recovered Services**.

The Service Recovery page is displayed with a list of recovered services.

5. Click the **New** icon above the table of listed service orders and service definitions.

The Select Service Recovery Options page of the Create Service Recovery Request wizard is displayed.

6. In the **Select Devices** and **Filter Criteria** sections of the wizard page, specify the devices and filters for the service recovery operation.

7. Fill in the fields as described in the following table.

Field	Action
Select Devices	
Devices	Select the check boxes beside the devices whose services you want to recover. The hostnames, IP addresses, managed states, OS versions, and roles of the devices are displayed in a table.
Add	<p>Click the Add button to open a dialog box to select the N-PE device you want to associate with the service recovery request. From the Choose Endpoints dialog box that appears, select the devices that you want to participate in the service. Use the multiple selection feature to select one or more devices. The search box that is present in the Choose Endpoints dialog box enables search across all the columns displayed in the dialog box.</p> <p>Click OK to add the devices to the service recovery request. The dialog box closes and you are returned to the Select Devices table that lists the endpoints that you selected.</p>
Delete	Select the check boxes beside the devices you want to remove from the service recovery request, and click the Delete button to remove the devices from the table.
Filter Criteria	
Recover Templates	Select this check box to recover service templates during the service recovery operation for the associated devices.
Recover Deleted EndPoints	Select this check box to recover the deleted endpoints during the service recovery operation.
Recover Modified EndPoints	Select this check box to recover the modified endpoints during the service recovery operation.

Field	Action
VCID Range	<p>This field is displayed if you have selected a point-to-point service definition.</p> <p>Specify the VCID range within which services are to be recovered.</p> <p>Range: 1 through 2147483647</p> <p>NOTE: The VCID Range parameter enables you to change the VCID range for services that had been configured previously outside of the context of Junos Space.</p>
Route Target Range	<p>This field is displayed for all the service types.</p> <p>Specify the route target range within which services are to be recovered. You can express the range in Autonomous System number format or IPv4 format:</p> <ul style="list-style-type: none"> AS number format—Autonomous system (AS) number format: <code><l2vpn-id:as-number:2-byte-number></code>. For example, 100:200. The AS number can be in the range from 1 through 65,535. IPv4 format—<code><l2vpn-id:ip-address:2-byte-number></code>. For example, l2vpn-id:10.1.1.2. Make sure that this value is lower than the value specified as the maximum route target allowed. <p>NOTE: The Route target parameter enables you to change the route target range for services that had been configured previously outside of the context of Junos Space.</p>
VPLS ID Range	<p>This field is displayed if you have selected a VPLS service definition.</p> <p>Specify the VPLS ID range within which the services are to be recovered.</p> <p>Range: 1 through 2147483647</p>
Hub-Route Target Range	<p>This field is displayed if you have you have selected a VPLS or Layer 3 VPN service definition.</p> <p>Specify the Hub-Route target range within which services are to be recovered. You can express the range in Autonomous System number format or IPv4 format:</p> <ul style="list-style-type: none"> AS number format—Autonomous system (AS) number format: <code><l2vpn-id:as-number:2-byte-number></code>. For example, 100:200. The AS number can be in the range from 1 through 65,535. IPv4 format—<code><l2vpn-id:ip-address:2-byte-number></code>. For example, l2vpn-id:10.1.1.2. Make sure that this value is lower than the value specified as the maximum route target allowed.
Spoke-Route Target Range	<p>This field is displayed if you have selected a VPLS or Layer 3 VPN service definition.</p> <p>Specify the Spoke-Route target range within which services are to be recovered. You can express the range in Autonomous System number format or IPv4 format:</p> <ul style="list-style-type: none"> AS number format—Autonomous system (AS) number format: <code><l2vpn-id:as-number:2-byte-number></code>. For example, 100:200. The AS number can be in the range from 1 through 65,535. IPv4 format—<code><l2vpn-id:ip-address:2-byte-number></code>. For example, l2vpn-id:10.1.1.2. Make sure that this value is lower than the value specified as the maximum route target allowed.

- When you complete defining the Service Recovery Profile, proceed to [“Reviewing the Configured Settings in the Wizard for Creating a Service Recovery Request” on page 413.](#)

Alternatively, click **Done** to trigger the service recovery operation.

The Connectivity Services Director application fetches the latest device configuration. It then processes the device configuration to derive the configuration of selected

service types. A message is displayed to denote that the service recovery request is being saved in the database.



NOTE:

- In case of a Layer 3 VPN service with pseudowire attached, you have to first recover the Layer 3 VPN service, and then the point-to-point service.

When the service recovery operation completes, the **Service Recovery Report** window appears. The service recovery report for each service is displayed in different tabs.

- Related Documentation**
- [Viewing Service Recovery Report on page 415](#)
 - [Performing a Service Recovery on a Defined Service on page 416](#)

Reviewing the Configured Settings in the Wizard for Creating a Service Recovery Request

The Review page of the service recovery job creation and modification wizards enable you to view and evaluate the service parameters and components you configured in preceding steps or pages of the wizard. This page provides a comprehensive, single-page view of all the service elements configured in the different pages of the wizard. You can either click the buttons corresponding to the various settings at the top of the wizard page to directly traverse to the page you want to modify or click the navigation buttons at the bottom of the wizard page to go to the different pages of the wizard.

After you click **Start** on the Review page of the service recovery request creation wizard, the Service Recovery Request job starts. After the job is completed, all the configuration parameters for all the devices are retrieved, but only those configurations that match the filter are processed and are populated in the Service Recovery page. Also, when a service recovery request job starts, the action denotes that only a discovery is initiated of all the possible services that can be recovered from the device. They are not yet stored in the Connectivity Services Director application database. Their status is initially marked as Partial as shown on the Service Recovery page.

To examine the configured service recovery request settings in the service recovery request creation wizard:

1. From the View selector, select **Service View**.
The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in Service View of the Connectivity Services Director banner.
The functionalities that you can configure in Build mode are displayed on the Tasks pane.
3. In the View pane, select the **Network Services > Connectivity** node without expanding the tree and selecting a type of service.

The tasks that are applicable for the different connectivity services are displayed on the Tasks pane.

4. From the Network Services > Connectivity Tasks pane, select **Service Recovery > View Recovered Services**.

The Service Recovery page is displayed with a list of recovered services.

5. Click the **New** icon above the table of listed service definitions.

The Select Service Recovery Options page of the Create Service Recovery Request wizard is displayed.

6. Click the **Review** button at the top of the wizard page to examine the configured settings. Alternatively, click **Next** after you specify the rule parameters.

7. You can examine and modify the created service recovery request parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify.

8. Click **Edit** next to the section that contains the parameter you want to modify. You are navigated to the corresponding page of the wizard in which the parameter settings are defined.

9. Click **Finish** to save the service recovery request.

10. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes. The Service Recovery page appears.

11. When you complete defining the service recovery profile, click **Done** To submit the service recovery request.

The Connectivity Services Director application fetches the latest device configuration. It then processes the device configuration to derive the configuration of selected service types. A message is displayed to denote that the service recovery request is being saved in the database.



NOTE:

- In case of a Layer 3 VPN service with pseudowire attached, you have to first recover the Layer 3 VPN service, and then the point-to-point service.

When the service recovery operation completes, the **Service Recovery Report** window appears. The service recovery report for each service is displayed in different tabs.

Related Documentation

- [Viewing Service Recovery Report on page 415](#)
- [Performing a Service Recovery on a Defined Service on page 416](#)

Viewing Service Recovery Report

When the service recovery operation completes, the **Service Recovery** window appears.

The **Service Recovery** window displays the recovered services according to service type. The service recovery report for all services is displayed in a table.

To view the service recovery report:

1. From the View selector, select **Service View**.

The workspaces that are applicable to routing and tunnel services are displayed.

2. Click the **Build** icon in Service View of the Connectivity Services Director banner.

The functionalities that you can configure in Build mode are displayed on the Tasks pane.

3. In the View pane, select the **Network Services > Connectivity** node without expanding the tree and selecting a type of service.

The tasks that are applicable for the different connectivity services are displayed on the Tasks pane.

4. In the **Network Services > Connectivity** task pane, select **Service Recovery > Recover Services**.

The Service Recovery window is displayed.

The following fields are displayed in the window:

Column	Description
Recovered Services —Lists the recovered service instances for the different services.	
Service Name	Name of the recovered service instance.
Service Definition	Name of the service definition attached to a service.
Service Type	One of the following: <ul style="list-style-type: none"> • P2P • VPLS • L3VPN
Status	Partial or Recovered
Customer	Customer for which the service is created
Comments	Comments to describe the service.

- Related Documentation**
- [Creating and Handling a Service Recovery Request on page 406](#)
 - [Performing a Service Recovery on a Defined Service on page 416](#)

Performing a Service Recovery on a Defined Service

You can perform a service recovery operation on a service instance that you have previously configured in the Service Recovery page, instead of running the recovery job during the process of creation of the recovery request. In certain situations, you might require a set of service instances to be defined separately, before you want to run the recovery task on all such services. In such cases, you can perform the recovery, independent of the recovery job creation, at a future time.

Partially recovered services are available on the Recover Service landing page, from which you can select one or more services and click on Recover button. After you click the Recover button, a pop-up dialog box is displayed, in which you need to provide the necessary attributes such as the customer for which the service is created and a meaningful description of the service. Once the user clicks on Start the Service Recovery Request job starts. After the job is completed, all the configurations for all the devices will be retrieved, but only those configurations that match the filter are processed and populated in Service Recovery page.

An important point to note here is that the recover action only discovers all the possible services that can be recovered from the device. They are not yet stored in the Connectivity Services Director application database. Their status will be initially marked as Partial as shown in grid.

To trigger a service recovery request on a previously configured service instance:

1. From the View selector, select **Service View**.

The workspaces that are applicable to routing and tunnel services are displayed.

2. Click the **Build** icon in Service View of the Connectivity Services Director banner.

The functionalities that you can configure in Build mode are displayed on the Tasks pane.

3. In the View pane, select the **Network Services > Connectivity** node without expanding the tree and selecting a type of service.

The tasks that are applicable for the different connectivity services are displayed on the Tasks pane.

4. From the Network Services > Connectivity Tasks pane, select **Service Recovery > View Recovered Services**.

The Service Recovery page is displayed with a list of recovered services with the Recovered Services tab selected.



NOTE: The Latest Recovery Job field at the top of the page displays the job ID and job status in blue. Click the the job ID and status to open the Job Details dialog box. The job ID, start and end times of the job, percentage of completion, and status of the job are displayed. Click Close to close the job dialog box.

5. Select the check box next to the service for which you want to perform the recovery operation again.
6. Click the **Manage** button above the table of listed service instances.
The Manage Recovery of a Service dialog box is displayed.
7. Select a customer from the Customer list to be associated with the service recovery job.
8. Enter a meaningful, easily-identifiable description in the Comments box.
9. For Layer 3 VPN services, select a hub of a full-mesh or a hub-and-spoke Layer 3 VPN service from the **Select Hub** list.
10. Click **Manage** to initiate the recovery job. Alternatively, click **Cancel** to discard the job.

If you click **Manage**, a dialog box is displayed stating that a service recovery job has been initiated. Click the link in the job ID to view the job details. Click **OK** to close the dialog box.

You can view the details of the recovered service from the Service Recovery page.

- Related Documentation**
- [Creating and Handling a Service Recovery Request on page 406](#)
 - [Viewing Service Recovery Report on page 415](#)

Processing of Device Change Notifications Overview

All the device change notifications are processed by the following EJB:

```
net.juniper.jmp.cm.notification.inventory.device.cmp.CMDeviceChangeNotificationMDB
```

The method `handleDeviceChange()` is called passing a result of type `DeviceChangeDiffResult`, which provides the following parts of information:

- Device ID—The ID of the device in the notification
- Notification Meta Data—The type of update—whether the configuration has been modified out-of-band or using Connectivity Services Director.

- DiffResults—A map containing the changed configuration from different configuration parameters on the CLI. The map contains the following keys:
 - Configuration
 - hardware-inventory
 - interface-inventory
 - software-inventory
 - license-inventory
 - system-information
 - logical-interface-inventory
 - configuration-version
- Device ID—The ID of the device in the notification
- Changed XPath List—The changed XPath list can be retrieved by querying `getChangedXPathList()` on result object.

For Service Recovery, Connectivity Services Director examines notifications that will match following criteria:

- Type of update is OutOfBand.
- DiffResults for “configuration” is not empty.
- Changed XPath list is from the interested XPath list for services supported in Connectivity Services Director. For the Connectivity Services Director application, an interested XPath list is maintained. If the changed XPath list contains any XPath from the interested XPath list, the configuration difference is processed.
- [XPaths of Relevance to Connectivity Services Director on page 418](#)
- [Processing of XPath Notifications for Out-of-Band Configuration Changes on page 419](#)

XPaths of Relevance to Connectivity Services Director

All the XPathS are not processed for service recovery. Instead, an interested or relevant XPath list is maintained for Connectivity Services Director. If the changed XPath list contains any of the following XPath attributes, the configuration differential-set is processed to determine the impacted service because of an update to service settings.

```
/configuration/routing-instances/instance  
/configuration/firewall/family/vpls  
/configuration/firewall/family/cc  
/configuration/firewall/policer/  
/configuration/interfaces/interface  
/configuration/interfaces/interface/unit  
/configuration/policy-options/  
/configuration/protocol/12circuit  
/configuration/protocol/local-switching
```

Processing of XPath Notifications for Out-of-Band Configuration Changes

A network managed by Connectivity Services Director has three repositories of information about the configuration of a network device—the configuration stored on the device itself, the device configuration record maintained by Junos Space, and the Build mode configuration maintained by Connectivity Services Director. When the configuration contained in all three repositories match, the device configuration state is shown as In Sync in Connectivity Services Director. When the repositories do not match, the configuration state is shown as Out of Sync. A common cause for this state is out-of-band configuration changes—that is, configuration changes made to a device outside of Connectivity Services Director.

When a device state is Out of Sync, you cannot deploy configuration changes on the device in Deploy mode. Use the Resynchronize Device Configuration task to resynchronize the three configuration repositories and change the device configuration state back to In Sync.

This section describes the different scenarios for out-of-band configuration change on the device and the approach to determine the service impacted by the change. Any XPath change list and configuration differences can belong to any of the following categories:

- Change to the existing endpoint on the service
- Missing or new endpoint on the service
- Endpoint for the new service
- Deleted endpoint for the existing service

The following list of attributes is used to identify neighbor service elements:

When serviceType is ServiceTypeEnum.ELINEMARTINI

```
vcID
lsName
lsEndName/LsEndIf:
deviceID
```

When serviceType is ServiceTypeEnum.ELINEKOMPELLA

```
routeTarget
```

When serviceType is ServiceTypeEnum.VPLS

```
vp1sID
```

```
routeTarget
hubRouteTarget
spokeRouteTarget
```

When serviceType is ServiceTypeEnum.L3VPN

```
routeTarget
hubRouteTarget
spokeRouteTarget
```

Related Documentation • [Creating and Handling a Service Recovery Request on page 406](#)

Handling of Out-of-Band Notifications for Service Recovery

After a device goes into the Out Of Sync state, a notification is displayed in the status bar at the bottom of the Connectivity Services Director GUI with the count of devices currently out of sync due to out-of-band notifications. The action to be taken when an out-of-band notification is received for the device can be defined using the Preferences page (which you can launch by clicking the down arrow beside the System button on the Connectivity Services Director banner and selecting Preferences).

The Service Activation tab of the Preferences page contains the following check box in the Deployments section for service recovery:

- **Block deployment on pending notifications**—Select this check box to cause a validation to be performed to determine if any of the selected devices have pending out-of-band notification, before deploying a service order. If a pending out-of-band notification exists for a device, deployment is blocked with the following message:

Cannot deploy service order, since pending notification exists for device(s) : <dev-1>, <dev-2>,<dev-3>

Related Documentation • [Creating and Handling a Service Recovery Request on page 406](#)

Viewing Service Recovery Instance Details

The **Service Recovery** window displays the recovered services according to service type. The service recovery report for each service is displayed in a table. You can view the individual and fine-grained details of the services recovered by double-clicking the name of a service instance from the table displayed in the Service Recovery window.

To view the details of a service recovery instance:

1. From the View selector, select **Service View**.

The workspaces that are applicable to routing and tunnel services are displayed.

2. Click the **Build** icon in Service View of the Connectivity Services Director banner.

The functionalities that you can configure in Build mode are displayed on the Tasks pane.

3. In the View pane, select the **Network Services > Connectivity** node without expanding the tree and selecting a type of service.

The tasks that are applicable for the different connectivity services are displayed on the Tasks pane.

4. In the **Network Services > Connectivity** Tasks pane, select **Service Recovery > Recover Services**. The Service Recovery window is displayed.

The **Details** button enables you to view information about a service selected in the **Recovered Services** tab of the Service Recovery window.

5. Double-click a service instance in the **Service Recovery** window to open the **View Service Details** window. This window contains several sections or panels that provide details about the recovered services.

The **View Service Details** window displays information about a service selected in the **Recovered Services** tab of the Service Recovery window. You can view detailed, in-depth information about a selected service.

The Service Details window is divided into three sections—Basic Details, Advanced Details, and Endpoint Details. The service tree contains the service name as the root node. The device node is the child of the service node and it contains the provisioned UNIs as the child nodes. The details panel in the Endpoint Details table displays configuration parameters and their corresponding values for the service in the tree and based on the service type.

Under the Basic Details section, the general details about the node details are shown. Also, the device configuration parameters are displayed. Under the Advanced Details section, which you can open or close by clicking the View Less or View More toggle links, the advanced connectivity settings between sites in the service provider network are shown, such as route distinguisher and VRF route label details. Under the Endpoint Details table, the configuration parameters of the UNI are displayed. The right pane

displays the details corresponding to the node or element you selected on the left pane.

Basic Details

This section is applicable for all types of services and displays the following details.

- **Name**—Name of the selected service
- **Customer**—Name of the customer associated with the service.
- **Service Definition**—Name of the service definition that is used to create the service.
- **Service Type**—Selected service type, such as P2P, L3VPN, or VPLS.
- **Comments**—User-defined description of the recovered service.
- **Signalling**—Type of signaling, namely, BGP or LDP.
- **Order Type**—Type of the service order, which is indicated as Recovery to signify a recovered service.
- **Status**—Status of the recovered service, such as Partial or Recovered.
- **Recovered By**—Name of the user that performed the service recovery operation.

Advanced Details

This section displays the advanced, fine-grained connectivity settings between sites, such as the configured route distinguisher, VRF route label. The parameters displayed under this section are similar to the advanced parameters displayed in the wizard for service order creation.

Column	Description
Advanced Details	
VCID	Virtual channel identifier number This field is displayed for P2P services only.
Service Order Type	Type of the service order, such as Ethernet, VPLS, or Layer 3 VPN.
MTU (Bytes)	Maximum transmission unit number This field is displayed for P2P and VPLS services.
MTU (Factor)	The factor by which the MTU value that you specify for the service is multiplied.
Route Target	Route target of the recovered service.
Route Distinguisher	Route distinguisher of the recovered service.
VLAN Normalization	Type of normalization for VLAN IDs, such as Q-in-Q or dot1q.
Customer Traffic Type	Type of restrictions placed on the traffic that can be transported across the network by the associated service, such as whether the associated service is restricted to transporting just one VLAN across the network or transporting a VLAN range.

Column	Description
Unmanaged IP	<p>If the Unmanaged IP field includes a valid IP address, the selected service is valid but the other end is an unmanaged device. If the field displays Unmanaged IP, the IP address of the unmanaged device is unknown. You must provide the IP address.</p> <p>NOTE: If Service Recovery finds an endpoint attached to a recovered service for a device that was not selected for Service Recovery, the endpoint is reported as an Unmanaged IP. The endpoint is recovered and attached to the service when Service Recovery is executed on the particular device.</p> <p>This field is displayed for P2P services only.</p>
Unmanaged Interface	<p>If one endpoint is an unmanaged device, the interface information is unknown. You must provide the interface for the endpoint.</p> <p>This field is displayed for P2P services only.</p>
VPLS ID	<p>VPLS ID of the recovered service</p> <p>This field is displayed for VPLS services only.</p>
L2VPN ID	<p>Layer 2 VPN ID of the recovered service</p> <p>This field is displayed for VPLS services only.</p>
Hub Route Target	<p>Route target of the hub.</p> <p>This field is displayed only for VPLS and L3VPN services.</p>
Spoke Route Target	<p>Route target of the spoke.</p> <p>This field is displayed for VPLS and L3VPN services only.</p>
VRF Table	<p>When this check box is selected, the VPN facilitates VRF table lookup, based on MPLS labels.</p> <p>This field is displayed for L3VPN services only.</p>
Routing Protocol	<p>Provider edge (PE) and customer edge (CE) routing protocol configured for the service.</p> <p>This field is displayed for L3VPN services only.</p>
Hub	<p>Hub device for the hub-and-spoke Layer 3 VPN service.</p> <p>This field is displayed for L3VPN services only. This is applicable for hub-and-spoke Layer 3 VPN service only.</p>
Auto Discovery	<p>Denotes whether auto discovery is enabled, which indicates that route target, route distinguisher, and VPN ID are provisionable. This field is applicable only if signaling is LDP.</p>
Normalized Vlan ID	<p>The VLAN to push at the relevant end points. This should be the same VLAN specified as the VLAN ID.</p>
Revert Time	<p>Revert time for redundant Layer 2 circuits and VPLS pseudowires. This field is applicable only if signaling is LDP.</p>

Column	Description
Switch Over Delay	Delay to wait before the backup pseudowire takes over.
Dot1QVLANTag	Tag number of the dot1q VLAN.
AS Override	Indicates whether the service provisioner can override the AS number or not.
Export Direct Routes	Indicates whether the functionality to export direct routes to remote sites is enabled.
VRF Table Label	Indicates whether mapping of the inner label of a packet to a specific VRF, thereby allowing the examination of the encapsulated IP header, is enabled.

Endpoint Details

A tabular view is displayed of the configured device and UNI Details that are part for the service. Each row in the table displays the basic, salient parameters, such as Device Name, Interface Name, Unit ID, Encapsulation and Description. You can use the paging controls to navigate across multiple pages of endpoints as necessary. A minimum of 20 endpoints per page are displayed.

The following fields are displayed in the End Points table:

- End Point—Name of the device configured as the source or origin (A) endpoint and the destination or target (Z) endpoint. This field is displayed for point-to-point services. Click the plus sign beside the device name for P2P services to expand the device-related parameters and view the detailed settings.
 - Device Name—Name of the device for which the service is created. Click the plus sign beside the device name for VPLS and L3VPN services to expand the device-related parameters and view the detailed settings.
 - Interface—Name of the physical interface associated with the service
 - Tagging—Type of packet tagging for the interface, such as Ethernet, dot1Q, or Q-in-Q
 - UnitId—Logical unit identifier of the interface
 - VlanId—VLAN identifier of the interface
 - Role—Indicates whether the node is a hub or a spoke
 - Template—Name of the service template that is used to create the service order
 - CoS Profiles—Name of the COS profile associated with the service
6. View the information of a recovered service in the **Basic Details** and **Advanced Details** panel. Click **Close** to close the View Service Details window and return to the Service Recovery window.

The **Service Recovery** window displays the status of all the recovered services. It also indicates the configuration that are converted to service orders. You can view the status of a recovered service in its corresponding tab. The **Service Recovery** window displays one of the following status indications:

- **Managed**—The service is now managed successfully
- **Failed**—Service Recovery did not convert the service to a service order
- **Partial**—The service cannot be managed yet



NOTE: You can access the **Recovered Service Status** window whenever you want to attempt to recover additional services.

Related Documentation

- [Creating and Handling a Service Recovery Request on page 406](#)
- [Performing a Service Recovery on a Defined Service on page 416](#)

Managing Out-of-Band Notifications for Recovered Services

The service recovery module contains a landing page for out of band device change notifications where all the device change notifications are listed. You can perform the following actions with the Service Recovery—Recover Out of Band Changes page:

- View the out-of-band notifications for recovered services and detailed information for each notification.
- Accept an out-of-band notification
- Delete an existing out-of-band notification
- Ignore an out-of-band notification

The **Service Recovery Report** window displays the recovered services according to service type. The service recovery report for each service is displayed in a table. You can view the individual and fine-grained details of the services recovered by double-clicking the name of a service instance from the table displayed in the Service Recovery window.

To view and manage out-of-band notifications for a service recovery instance:

1. From the View selector, select **Service View**.

The workspaces that are applicable to routing and tunnel services are displayed.

2. Click the **Build** icon in Service View of the Connectivity Services Director banner.

The functionalities that you can configure in Build mode are displayed on the Tasks pane.

3. In the View pane, select the **Network Services > Connectivity** node without expanding the tree and selecting a type of service.

The tasks that are applicable for the different connectivity services are displayed on the Tasks pane.

4. In the **Network Services > Connectivity** task pane, select **Service Recovery > Manage Out of Band Changes**.

The Manage Out of Band Changes window is displayed.

Device Name	Status	Notification XML	Create TimeStamp	Update TimeStamp
SG4re	IGNORED	View	2016-04-05 16:12:45.0	2016-04-20 13:03:31.0
SG1re	PENDING	View	2016-04-19 16:13:02.0	2016-04-21 17:17:26.0

The following fields are displayed in this window:

- Device Name—Name of the device to which the notification belongs
 - State—Indicates whether the notification is processed or not. One of the following states is displayed:
 - Ignored—Notification is ignored and device changes to InSync again.
 - Failed—Processing failed and services was not recovered. The device remains in the OutOfSync state.
 - Pending—Notifications are not processed. The device continues to remain OutOfSync. Notifications for successfully recovered services are removed from grid and device are brought to InSync state.
 - Notification XML— A **View** link shows the configuration difference for all the out of band notifications received for that device. Each time a notification is received, it is merged with earlier out-of-band notifications received. A single copy of each notification is maintained per device. Click **View** to view the configuration differences in XML format.
 - Create Timestamp—Date and time at which the record was created. The record will be created when the first out-of-band notification is received for the device.
 - Update Timestamp—Date and time at which the most recent out-of-band notification is received for the device
5. Select the check box beside a device for which an out-of-band notification is displayed, and click **Accept** above the table to navigate to the Create Service Recovery Request wizard with the devices and service definitions preselected on the landing page. The

out-of-band notification is accepted and removed from the table of out-of-band entries.

You can select a notification and click **Accept** to recover endpoints. The following two options are available for recovering endpoints:

- When Connectivity Services Director is able to determine the service to which the endpoint belongs— Here, the service type and service definition in use are identified. In that case, the service is recovered only for the selected endpoint. You can select multiple endpoints and say recover service and all the selected endpoints will be recovered.
 - When Connectivity Services Director is unable to determine the service to which the endpoint belongs—Here, the service type and service definition are not identified, and therefore, the existing service recovery flow is invoked. Only devices are preselected and you must select the appropriate service definition. If the recovery of the service fails, the operator can use existing option of force-deploy from Connectivity Services Director to make the service on device in-sync with the service in Connectivity Services Director and then discard the notification on out-of-band changes landing page to make device In Sync again.
6. Select the check box beside a device for which an out-of-band notification is displayed, and click **Ignore** above the table to ignore the notification.

The notification is discarded and device is marked as In-Sync. The notification is not removed from the table.
 7. Select the check box beside a device for which an out-of-band notification is displayed, and click **Delete** above the table to delete the record from the table.

Only processed or discarded records are enabled to be deleted.
 8. Select the check box beside a device for which an out-of-band notification is displayed, and click **Details** above the table to open a pop-up dialog box that displays the type of update performed on the device that caused the out-of-band notification.

- Related Documentation**
- [Creating and Handling a Service Recovery Request on page 406](#)
 - [Performing a Service Recovery on a Defined Service on page 416](#)

Viewing Details of an Out-of-Band Notification for Recovered Services

On the Manage Out of Band Changes page, the **Details** button displays granular and comprehensive information for a selected service recovery notification.

The Manage Out of Band Changes page displays the devices for which the configuration settings have been modified outside of the Connectivity Services Director application. The configuration state of a device is shown as In Sync when the configuration information in all three repositories match (settings made using the devices CLI, Connectivity Services Director in Build mode, or Junos Space Network Management Platform). If there is a conflict between the configuration information in one or more of the repositories, the device configuration state is Out of Sync. An Out of Sync state is usually the result of out-of-band configuration changes—that is, configuration changes made to a device using a management tool other than Connectivity Services Director.

To view detailed information that pertains to an out-of-band notification of a service recovery instance:

1. From the View selector, select **Service View**.

The workspaces that are applicable to routing and tunnel services are displayed.

2. Click the **Build** icon in Service View of the Connectivity Services Director banner.

The functionalities that you can configure in Build mode are displayed on the Tasks pane.

3. In the View pane, select the **Network Services > Connectivity** node without expanding the tree and selecting a type of service.

The tasks that are applicable for the different connectivity services are displayed on the Tasks pane.

4. In the **Network Services > Connectivity** task pane, select **Service Recovery > Manage Out of Band Changes**.

The Manage Out of Band Changes window is displayed.

5. Select the check box beside a device for which an out-of-band notification is displayed, and click **Details** above the table.

The Details pop-up dialog box appears that contains the following fields:

- Service Name—The configuration difference received in the device change notification will be processed to see if we are able to determine the name of service. If name of service can be determined it will displayed.
- Service Type—The type of service (P2P, VPLS, or L3VPN)
- Service Definition—The definition associated with service
- Customer—The customer associated with service
- Type of update—Indicates the type of modification performed as follows:
 - CREATE—Missing endpoint added to the service
 - MODIFY—Existing endpoint modified for the service
 - DELETE—Endpoint deleted for the service

- You are returned to the Out of band Changes page.

Related Documentation

- [Creating and Handling a Service Recovery Request on page 406](#)
- [Performing a Service Recovery on a Defined Service on page 416](#)

Viewing Services Rejected During a Service Recovery

You can view the services that were rejected during the service recovery operation. The reason for the failure of the service recovery operation is also displayed, which enables you to analyze and resolve the problem and perform a service recovery task again.

To view services that are rejected during a service recovery operation:

1. From the View selector, select **Service View**.

The workspaces that are applicable to routing and tunnel services are displayed.

2. Click the **Build** icon in Service View of the Connectivity Services Director banner.

The functionalities that you can configure in Build mode are displayed on the Tasks pane.

3. In the View pane, select the **Network Services > Connectivity** node without expanding the tree and selecting a type of service.

The tasks that are applicable for the different connectivity services are displayed on the **Tasks** pane.

4. In the **Network Services > Connectivity** task pane, select **Service Recovery > View Recovered Services**.

The Service Recovery page is displayed with a list of recovered services with the Recovered Services tab selected.

5. Select the **Rejected Endpoints** tab. The Service Recovery—Rejected Services window is displayed.

Service Name	Configuration XML	Service Type	Device Name	Interface	Unit	Rejected Reason
Group: ELan-BGP-PortBased-Test						
ELan-BGP-PortBased-Test	View	VPLS	Unknown	ge-0/1/3	0	No Service Definition Available. Cannot proce...
Group: ELan-BGP-PortBased						
ELan-BGP-PortBased	View	VPLS	Unknown	ge-0/1/6	0	No Service Definition Available. Cannot proce...
Group: VPLS-PW-Extension						
VPLS-PW-Extension	View	VPLS	Unknown	ge-0/0/7	0	No Service Definition Available. Cannot proce...
Group: VPLS_PW_Extension						
VPLS_PW_Extension	View	VPLS	Unknown	ge-0/0/8	0	No Service Definition Available. Cannot proce...
Group: vpls_coslatest1						
vpls_coslatest1	View	VPLS	SG4re	ge-0/1/9	2	No Service Definition Available. Cannot proce...
Group: vpls_coslatest4						
vpls_coslatest4	View	VPLS	SG4re	ge-0/1/5	5	No Service Definition Available. Cannot proce...

The following fields are displayed in a table:

- Service Name—Name of the rejected service
- Configuration XML—Click **View** to open a dialog box that displays the configuration differences in XML format for the corresponding device on which out-of-band changes have been made. Close the dialog box after viewing the out-of-band configuration changes. Configuration changes are shown only when the device configuration differs from the Junos Space configuration record—that is, when the device configuration state in Junos Space is not In Sync.



NOTE: The Junos XML API is an XML representation of Junos configuration statements and operational mode. It defines an XML equivalent for all statements in the Junos configuration hierarchy and many of the commands that you issue in CLI operational mode. Each operational mode command with a Junos XML counterpart maps to a request tag element and, if necessary, a response tag element.

- Service Type—Type of the rejected service, such as point-to-point, Layer 3 VPN, or VPLS
- Device Name—Name of the device for which the service was rejected

- Interface—Name of the interface on the device for which the service was rejected
 - Unit—Logical unit number of the interface associated with the device
 - Rejected Reason—Cause for the service recovery operation to reject the service
6. For each device displayed under the Devices column, you can view detailed information regarding the services for which out-of-band notification was generated.

From the Manage Out of Band Changes page, select the check box beside a device for which an out-of-band notification is displayed, and click **Details** above the table to open a pop-up dialog box that displays the following fields:

- Service Name—The configuration difference received in the device change notification will be processed to see if we are able to determine the name of service. If name of service can be determined it will displayed.
- Service Definition—Name of the definition associated with the service
- Customer—Name of the customer associated with the service
- Type of update—Indicates the type of modification performed as follows:
 - CREATE—Missing endpoint added to the service
 - MODIFY—Existing endpoint modified for the service
 - DELETE—Endpoint deleted for the service

**Related
Documentation**

- [Creating and Handling a Service Recovery Request on page 406](#)
- [Performing a Service Recovery on a Defined Service on page 416](#)

Viewing Service Recovery Jobs

You can perform a service recovery operation on a service instance that you have previously configured in the Service Recovery page, instead of running the recovery job during the process of creation of the recovery request. In certain situations, you might require a set of service instances to be defined separately, before you want to run the recovery task on all such services. In such cases, you can perform the recovery, independent of the recovery job creation, at a future time.

The Service Recovery Jobs page shows the progress and status of the service recovery job. Although you can view details about the status of all the jobs initiated in the Connectivity Services Director application from the Jobs page accessible as a System task, you can use the Service Recovery Jobs page in Build mode of Service view to obtain a filtered display of only the service recovery jobs for easy analysis and debugging.

To the service recovery jobs:

1. From the View selector, select **Service View**.

The workspaces that are applicable to routing and tunnel services are displayed.

2. Click the **Build** icon in Service View of the Connectivity Services Director banner.

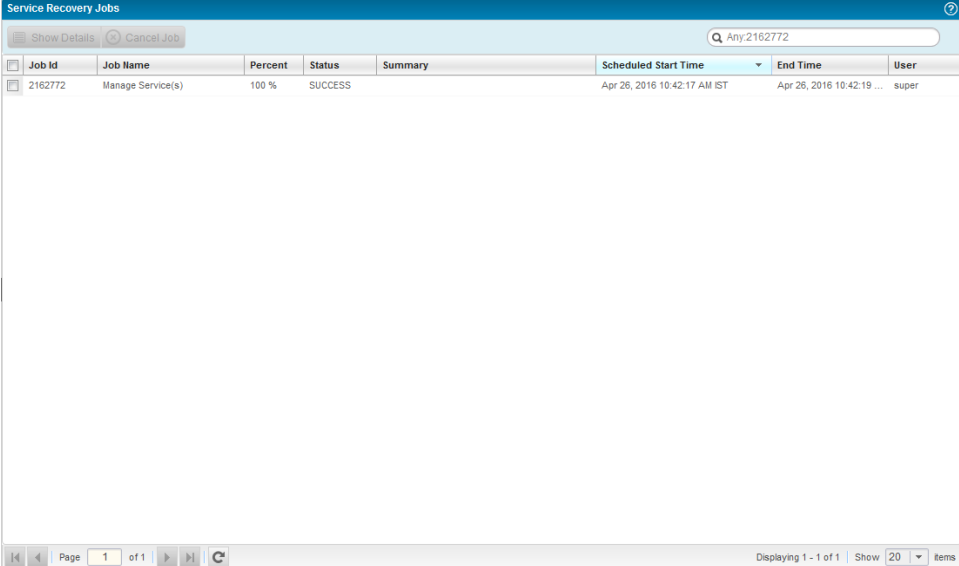
The functionalities that you can configure in Build mode are displayed on the Tasks pane.

3. In the View pane, select the **Network Services > Connectivity** node without expanding the tree and selecting a type of service.

The tasks that are applicable for the different connectivity services are displayed on the Tasks pane.

4. In the **Network Services > Connectivity** task pane, select **Service Recovery > View Service Recovery Jobs**.

The **Service Recovery Jobs** window appears.



The screenshot shows the 'Service Recovery Jobs' window. At the top, there are buttons for 'Show Details' and 'Cancel Job', and a search bar containing 'Any:2162772'. Below is a table with the following data:

Job Id	Job Name	Percent	Status	Summary	Scheduled Start Time	End Time	User
2162772	Manage Service(s)	100 %	SUCCESS		Apr 26, 2016 10:42:17 AM IST	Apr 26, 2016 10:42:19 ...	super

At the bottom, there is a pagination bar showing 'Page 1 of 1' and 'Displaying 1 - 1 of 1'.

5. To view the details of a job, select a row and click **Show Details** or double-click a row.
6. To cancel a scheduled job, select a job that is scheduled for a later time or a job that is in progress and click **Cancel**.

The fields in the Prestaging Device Jobs page are described in [Table 59 on page 386](#). To view any hidden column, keep the mouse on any column heading and select the down arrow and then click Columns. Select the check box to display the hidden columns.



NOTE: Details of jobs initiated from Connectivity Services Director will be available only from Connectivity Services Director. These jobs will not be listed in the Jobs pane in Junos Space platform and vice-versa.

Table 61: Service Recovery Jobs Page Fields

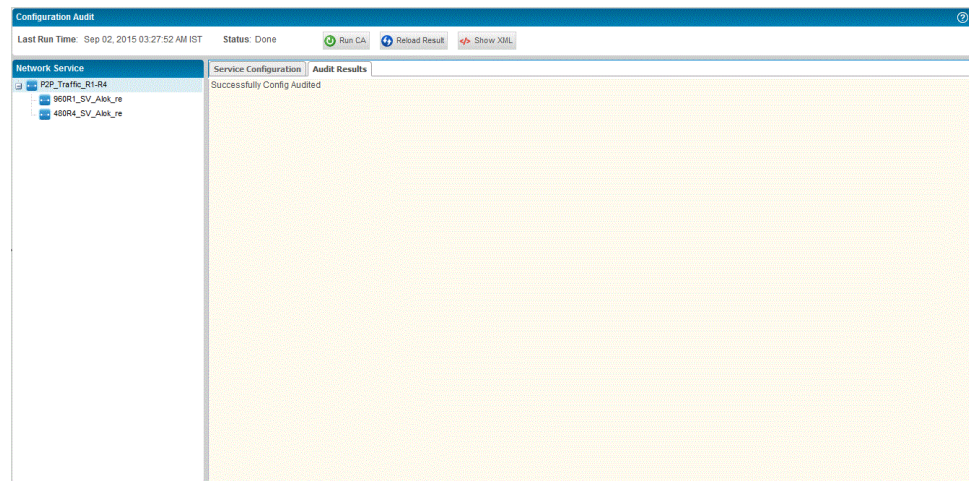
Field	Description
Job ID	The unique ID assigned to the job
Name	The name of the job
Percent	The percentage of completion of the job
State	The status of the job: <ul style="list-style-type: none"> • Success—Job completed successfully • Failure—Job failed and was terminated • Job Scheduled—Job is scheduled but has not yet started • In progress—Job is has started, but not completed • Cancelled—Job is cancelled
Job Type	The type of the job
Summary	Summary of the job scheduled and executed with status
Scheduled Start Time	The time when the job is scheduled to start
Actual Start Time	The actual time when the job started
End Time	The time when the job was completed
User	The login ID of the user that initiated the task
Recurrence	The recurrent time when the job will be restarted.

Related Documentation

- [Managing Service Configuration Deployment Jobs on page 1003](#)
- [Deploying Services Configuration to Devices on page 1005](#)

Performing a Configuration Audit for Recovered Services

A configuration audit can help you determine whether the service configuration on the device has been changed out of band. To this end, you can compare the results of a configuration audit with the service configuration in the Junos Space database. The following example shows a sample comparison.



To perform a configuration audit:

1. From the View selector, select **Service View**.
The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in Service View of the Connectivity Services Director banner.
The functionalities that you can configure in Build mode are displayed on the Tasks pane.
3. In the View pane, select the **Network Services > Connectivity** node without expanding the tree and selecting a type of service.
The tasks that are applicable for the different connectivity services are displayed on the Tasks pane.
4. In the **Network Services > Connectivity** task pane, select **Service Recovery > View Recovered Services**.
The Service Recovery page is displayed with a list of recovered services with the Recovered Services tab selected.
5. Select a recovered service, and click the **Audit** button at the top of the table of listed services and select **Configuration Audit > Run Configuration Audit**.

The image shows a 'Confirmation' dialog box with a blue header bar containing the title 'Confirmation' and a close button (X). The main content area has a label 'Confirm Schedule Configuration Audit of' followed by a text field containing 'P2P_Traffic_R1-R4'. Below this is a section titled 'Deployment Options:' containing two radio buttons: 'Audit Now' (which is selected) and 'Audit Later'. Under 'Audit Later', there is a 'Date and Time:' label followed by a date input field showing '31 Aug, 2015' and a time input field showing 'IST'. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

6. In the **Schedule Configuration Audit** window, either:
 - Select **Audit Now**, then click **OK**.
An informational dialog appears, stating that the configuration audit job is successfully triggered with the job ID, and an **OK** button.
 - Select **Audit Later**, enter a date and time, then click **OK**.
7. To monitor the progress of an audit after selecting **Audit Now**, click the Job ID in the **Audit Information** window. The **Job Management** page shows information about the configuration audit job.



NOTE: Alternatively, to display the Job Management page, click the **System** icon on the Connectivity Services Director banner, and select **Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

The **State** field indicates whether the service passed or failed the audit. If the service failed the audit, then the **Summary** field provides information about the failure.

To monitor the progress of an audit after selecting **Audit Later**, after the scheduled time of the audit:

- a. On the Junos Space Network Management Platform user interface, select **Jobs**.
- b. In the **Job Types** chart, select the **Configuration Audit** segment of the pie chart.

- c. Select the configuration audit of interest from the list on the **Job Management** page.
Summary information about the audit appears in the quick look panel.

- d. In the filter bar, select the table view icon to see additional information about the job. If the service failed the audit, information about the failure appears in the **Summary** field.

8. In the **Audit Information** window, click the job ID of the configuration audit.

The **Job Management** window appears and shows a filtered view of the job inventory, showing only the configuration audit job.



NOTE: If a resynchronization between a device and the Junos Space database is ongoing when the configuration audit job starts, the configuration audit job suspends until the resynchronization job finishes. If the resynchronization job fails to complete, the audit could be suspended indefinitely. To allow the audit to proceed, go to the **Job Management** workspace and cancel the resynchronization job, as described in *Canceling a Job*.

9. In the **Status** column, check the status of the audit to determine whether it succeeded or failed.

Check the **Summary** column, which contains useful service information such as the VC ID and endpoint information. For some failed deployments, this column also contains information about why the deployment failed.



NOTE: When a configuration audit is performed, the XPATH attributes that are present in the service configuration are used. Only the addition, modification, or deletion of the XPATH attributes is detected, and the creation of a new attribute (child XPATH) on a device is not determined. The audit operation disregards such attributes and does not identify them. This behavior is expected and occurs because Junos Space Platform software audits only the settings present a user template. If the template has a container, Junos Space Platform only audits to determine whether the device is configured with this container. If a user wants to audit any container child, the user needs add it into the template. This scenario is similar to an out-of-band configuration change on the device, which Junos Space Platform can determine only if the system of record (SOR) mode is set for the Junos Space Network Management Platform application.

**Related
Documentation**

- [Performing a Functional Audit on page 1067](#)
- [Troubleshooting N-PE Devices Before Provisioning a Service on page 1080](#)

- [Modifying the Application Settings of Connectivity Services Director on page 1082](#)
- [Troubleshooting the Endpoints of Services on page 1088](#)
- [Viewing Configuration Audit Results on page 1098](#)
- [Viewing Functional Audit Results on page 1102](#)
- [Viewing Functional Audit Results for an Inverse Multiplexing for ATM Service on page 1106](#)

Viewing Configuration Audit Results of Recovered Services

After performing a configuration audit of a recovered service, check the detailed results of the audit:

1. From the View selector, select **Service View**.

The workspaces that are applicable to routing and tunnel services are displayed.

2. Click the **Build** icon in Service View of the Connectivity Services Director banner.

The functionalities that you can configure in Build mode are displayed on the Tasks pane.

3. In the View pane, select the **Network Services > Connectivity** node without expanding the tree and selecting a type of service.

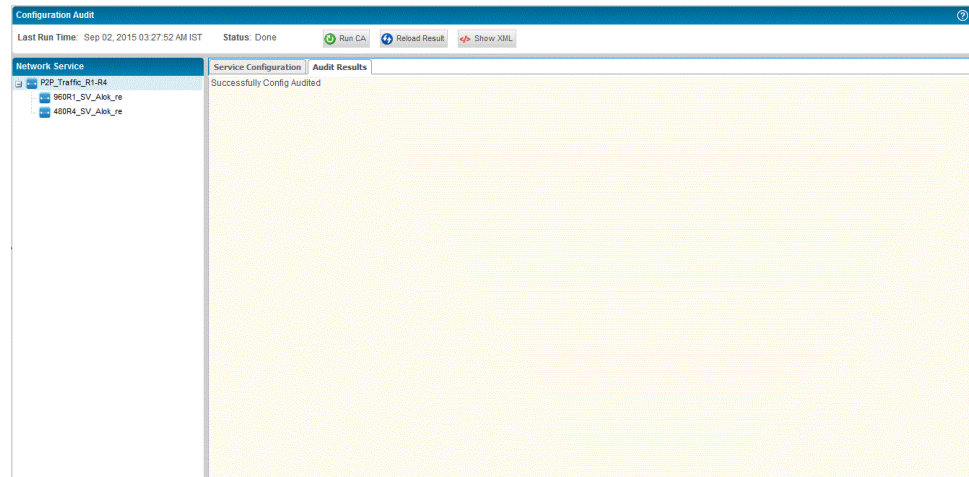
The tasks that are applicable for the different connectivity services are displayed on the Tasks pane.

4. In the **Network Services > Connectivity** task pane, select **Service Recovery > View Recovered Services**.

The Service Recovery page is displayed with a list of recovered services with the Recovered Services tab selected.

5. Select a recovered service, and click the **Audit** button at the top of the table of listed services and select **Configuration Audit > View Audit Results**.

The configuration audit results are displayed if an audit operation was previously performed on the selected service.



Examine the audit results for missing configuration information, and keep the window open for later comparison with the service configuration in the Junos Space database.

You can validate policies for the hub and spoke (1 interface).



NOTE: In the Service Configuration tab of the Configuration Audit dialog box, you can observe several lines with the **delete** statement in the service settings. These **delete** statements indicate the policy attributes that are deleted from the corresponding service on a device. Whenever a service is created or modified, the policy options are always deleted from the device to prevent the previously existing policies from interfering with the service. The presence of the **delete** statements is an expected behavior and does not indicate any incorrect service configuration.

6. To view the service configuration in the Junos Space database, in Deploy mode, from the **Network Services > Connectivity** task pane, select **Service Provisioning > Deploy Services**. The Manage Service Deployment page is displayed on the bottom part of the right pane. Select a service from the **Manage Service Deployment** page, then in the **Actions** menu, select **View Service Configuration**.

A new window opens and shows the service configuration.

If a CFM is configured in P2P service or VPLS service, the configuration audit result displays the CFM configuration details.

7. Compare the contents of the Service Configuration with those of the **Configuration Audit Results** window for each device in turn. If you see discrepancies, then it is likely that the service configuration was modified out-of-band. If so, you might need to synchronize the device with the Junos Space database.

For step-by-step instructions about synchronizing devices, see *Resynchronizing Managed Devices with the Network* for details.

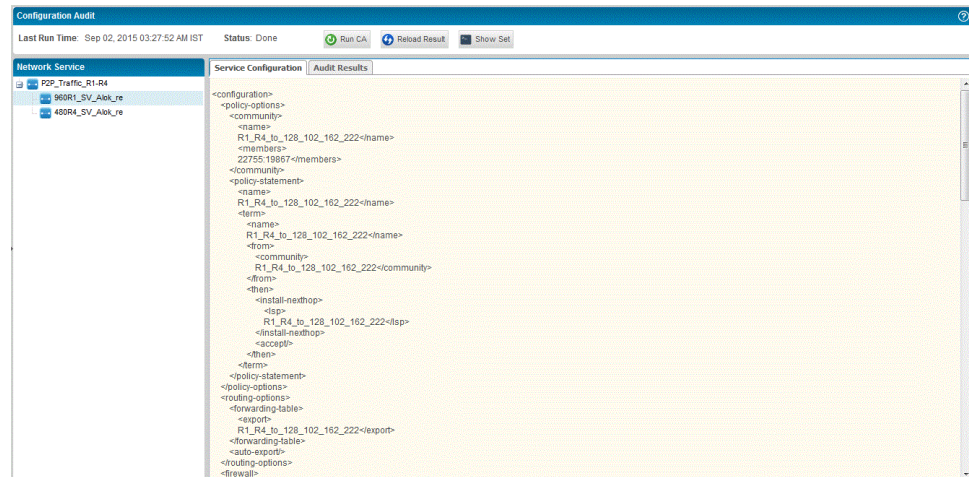
After the audit job is completed, you can view the output of the operation in the Configuration Audit Results window that is displayed on the right pane. The left pane displays a tree of devices associated with the specified service. You can select a **Service-name > Interface-name Device-name** in the left pane of the window. The attribute definitions and parameters defined in the service are displayed in the right pane. The right pane contains three tabs— Service Configuration, Template Configuration, and Audit Results. The Service Configuration tab displays the settings specified for the service on the device in CLI format. This tab displays the elements or components specified for a service template in the form of configuration stanzas and hierarchy levels. This display is similar to the **show** command that you can use at a certain **[edit]** hierarchy level to view the defined settings. The Template Configuration tab displays the service attributes and options defined in the service template, if any, that is associated with the service. The Audit Results tab displays the status of the audit job that was run, such as whether the job succeeded or failed. You can also view the service definition and associated template details under the Service Config and Template Config tabs in Junos OS XML API format, instead of the CLI format.

Click the **Show XML Config** button at the top-right corner of the window to view the audit results in XML API format. Alternatively, click the **Show Set** button to view the audit results in the manner in which they are displayed in the Junos OS CLI interface. The **Show XML/Set** button is a toggle button.

The screenshot shows the Configuration Audit window. At the top, it displays 'Last Run Time: Sep 02, 2015 03:27:52 AM IST' and 'Status: Done'. Below this are buttons for 'Run CA', 'Reload Result', and 'Show XML'. The main area is divided into two panes. The left pane, titled 'Network Service', shows a tree structure with 'P2P_Traffic_R1-R4' expanded, showing '960R1_SV_Ask_Re' and '450R4_SV_Ask_Re'. The right pane, titled 'Service Configuration', shows the configuration for the selected service in CLI format. The configuration includes policy options, firewall policies, routing options, and interface settings for ge-0/0/2.

```

set policy-options community R1_R4_to_128_102_162_222 members 22755:19867
set policy-options policy-statement R1_R4_to_128_102_162_222 term R1_R4_to_128_102_162_222 from community R1_R4_to_128_102_162_222
set policy-options policy-statement R1_R4_to_128_102_162_222 term R1_R4_to_128_102_162_222 then install-neighbor-lap R1_R4_to_128_102_162_222
set policy-options policy-statement R1_R4_to_128_102_162_222 term R1_R4_to_128_102_162_222 then accept
set routing-options forwarding-table export R1_R4_to_128_102_162_222
set routing-options auto-export
set firewall policer policer_in_ge-0/0/2_1 if-exceeding bandwidth-limit 10000000
set firewall policer policer_in_ge-0/0/2_1 if-exceeding burst-size-limit 15220
set firewall policer policer_in_ge-0/0/2_1 then discard
set firewall family ccc filter filter_in_ge-0/0/2_1 interface-specific
set firewall family ccc filter filter_in_ge-0/0/2_1 term 1 then policer policer_in_ge-0/0/2_1
set firewall family ccc filter filter_in_ge-0/0/2_1 term 1 then accept
set interfaces ge-0/0/2 flexible-vlan-tagging
set interfaces ge-0/0/2 mtu 1522
set interfaces ge-0/0/2 encapsulation flexible-ethernet-services
set interfaces ge-0/0/2 unit 1 description
set interfaces ge-0/0/2 unit 1 encapsulation vlan-ccc
set interfaces ge-0/0/2 unit 1 vlan-id 1
set interfaces ge-0/0/2 unit 1 family ccc filter input-filter_in_ge-0/0/2_1
set protocols l2circuit neighbor 128.102.162.222 interface ge-0/0/2.1 virtual-circuit-id 2147467275
set protocols l2circuit neighbor 128.102.162.222 interface ge-0/0/2.1 no-control-word
set protocols l2circuit neighbor 128.102.162.222 interface ge-0/0/2.1 community R1_R4_to_128_102_162_222
set protocols l2circuit neighbor 128.102.162.222 interface ge-0/0/2.1 ignore-encapsulation-mismatch
set protocols l2circuit neighbor 128.102.162.222 interface ge-0/0/2.1 mtu 1522
  
```

The Junos OS command-line interface (CLI) and the Junos OS infrastructure communicate using XML. When you issue an operational mode command in the CLI, the CLI converts the command into XML format for processing. After processing, Junos OS returns the output in the form of an XML document, which the CLI converts back into a readable format for display. Remote client applications also use XML-based data encoding for operational and configuration requests on devices running Junos OS. The Junos XML API is an XML representation of Junos configuration statements and operational mode commands. It defines an XML equivalent for all statements in the Junos configuration hierarchy and many of the commands that you issue in CLI operational mode. Each operational mode command with a Junos XML counterpart maps to a request tag element and, if necessary, a response tag element.

Click **Reload Result** at the top-right corner of the window to refresh and display the results of the audit. When you click this button, only the output of the audit operation is displayed afresh and the audit job is not run again. You can refresh the results only for completed audit instances. When you select **Service-name** in the left pane of the window, service status information is displayed in the right pane. Click **Run Configuration Audit** after selecting the services you need to run the audit job again.

Configuration audit can be run for multiple services from Build mode of Service View of the Connectivity Services Director GUI. From the Manage Network Services page, select the check boxes beside multiple services, click the **Audit** button at the top of the table of configured services, and select **Run Configuration Audit** from the drop-down menu.

We recommend that you configure a script as a local script for effective and optimal debugging and analysis of the configuration settings contained in the script. The main advantage of a local script is that you need not download the script to a device (because a connection is established with the device by the GUI application and the script is run) and you need not remove the script from a device after you decommission a service.

Related Documentation

- [Viewing Functional Audit Results on page 1102](#)
- [Performing a Functional Audit on page 1067](#)
- [Performing a Configuration Audit on page 1077](#)

Recovering Modifications and Deletions Performed for Existing Endpoints

Until Connectivity Services Director Release 1.0R2, the service recovery operation did not support the recovery of updated configurations made on existing endpoints associated with services. The only supported operations were recovery of new services and new endpoints for existing services, and recovery of connectivity fault management (CFM) profiles.

Starting with Release 2.0R1, the following recovery operations are supported in addition:

- Recovering modifications to existing endpoints
- Recovering endpoint deletions for a service

Also, recovery of the swap of hubs and spokes for hub-and-spoke Layer 3 VPN and VPLS services are supported. In addition, recovery of changes in configuration of backup endpoints for point-to-point A and Z endpoints is supported.

Recovery of templates, recovery for devices with different Junos OS versions running on them, and recovery of class of service (CoS) profiles are not supported.

Recovering Parameters for Point-to-Point Services

Table 62 on page 441 describes the fields or parameters that are supported for recovery during a service recovery operation and the corresponding XPath notifications for those configuration parameters. This table also denotes the service operation that is supported, such as creation, edit, or deletion of a service

Table 62: Mapping of Parameters, XPaths, and Supported Operations for Point-to-Point Services

Field	XPath	Supported Operation
Interface MTU	configuration/interfaces/interface/mtu	Modify service
Interface bandwidth	/configuration/firewall/policer/if-exceeding/bandwidth-limit	Modify service
Starting C-VLAN ID in a range	/configuration/interfaces/unit/vlan-tags/inner-range	Modify service
Ending C-VLAN ID in a range	/configuration/interfaces/unit/vlan-tags/inner-range	Modify service
C-VLAN ID	/configuration/interfaces/unit/vlan-tags/inner (Q-in-Q)	Modify service
V-LAN ID	/configuration/interfaces/unit/vlan-tags/outer (Q-in-Q) /configuration/interfaces/unit/vlan-id (Dot1Q)	Modify service
Outer TPID	/configuration/interfaces/interface/unit/input-vlan-map/tag-protocol-id /configuration/interfaces/interface/unit/output-vlan-map/tag-protocol-id	Create, modify, or delete service

Table 62: Mapping of Parameters, XPath, and Supported Operations for Point-to-Point Services (contin

Field	XPath	Supported Operation
Inner TPID	/configuration/interfaces/interface/unit/input-vlan-map/inner-tag-protocol-id /configuration/interfaces/interface/unit/output-vlan-map/inner-tag-protocol-id	Create, modify, and delete service
Endpoint LSP association	/configuration/protocols/l2circuit/neighbor/interface/community /configuration/policy-options/policy-statement/term/then/install-nexthop/lsp	Create, modify, and delete service
Interface description	/configuration/interfaces/interface/unit/description	Create, modify, and delete service
Changing, disabling, and enabling CFM profile	Not supported	Not applicable

Recovering Parameters for Layer 3 VPN Services

Table 63 on page 442 describes the fields or parameters that are supported for recovery during a service recovery operation and the corresponding XPath notifications for those configuration parameters. This table also denotes the service operation that is supported, such as creation, edit, or deletion of a service

Table 63: Mapping of Parameters, XPath, and Supported Operations for Layer 3 VPN Services

Field	XPath	Supported Operation
Interface MTU	configuration/interfaces/interface/mtu	Modify service
Interface bandwidth	/configuration/firewall/policer/if-exceeding/bandwidth-limit	Modify service
Starting C-VLAN ID in a range	/configuration/interfaces/unit/vlan-tags/inner-range	Modify service
Ending C-VLAN ID in a range	/configuration/interfaces/unit/vlan-tags/inner-range	Modify service
C-VLAN ID	/configuration/interfaces/unit/vlan-tags/inner (Q-in-Q)	Modify service
V-LAN ID	/configuration/interfaces/unit/vlan-tags/outer (Q-in-Q) /configuration/interfaces/unit/vlan-id (dot1Q)	Modify service
Outer TPID	Gets prefixed to VLAN tags, for example: <vlan-tags> <outer>0x88a8.51</outer> <inner-range>0x9100.56-65</inner-range> </vlan-tags>	Create, modify, and delete service

Table 63: Mapping of Parameters, XPath, and Supported Operations for Layer 3 VPN Services (continue)

Field	XPath	Supported Operation
Inner TPID	<pre><vlan-tags> <outer>0x88a8.51</outer> <inner-range>0x9100.56-65</inner-range> </vlan-tags></pre>	Create, modify, and delete
MAC table size	Not supported	Not applicable
Interface MAC limit	Not supported	Not applicable
Mesh group name change	Not supported	Not applicable
Interface description	/configuration/interfaces/interface/unit/description	Create, modify, and delete
PW extension (BGP and LDP)	<p>Addition of point-to-point spoke and update of neighbor in hub are supported</p> <pre>/configuration/instances/instance/instance/protocols/vpls/mesh-group/vpls-id /configuration/instances/instance/instance/protocols/vpls/mesh-group/neighbor</pre>	Create and delete service
PW resiliency (LDP)	<p>Addition of a backup hub and update of neighbor details in point-to-point spoke and VPLS LDP spoke are supported</p> <p>Update of neighbor to primary hub is not supported</p> <pre>/configuration/instances/instance/instance/protocols/vpls/neighbor/backup-neighbor-name for LDP spoke</pre> <pre>/configuration/protocols/ldp/circuit/neighbor/interface/backup-neighbor-name for point-to-point spoke</pre>	Create and delete service
Changing, disabling, and enabling CFM profile	Not supported	Not applicable

Recovering Parameters for VPLS Services

Table 64 on page 443 describes the fields or parameters that are supported for recovery during a service recovery operation and the corresponding XPath notifications for those configuration parameters. This table also denotes the service operation that is supported, such as creation, edit, or deletion of a service

Table 64: Mapping of Parameters, XPath, and Supported Operations for VPLS Services

Field	XPath	Supported Operation
Interface MTU	configuration/interfaces/interface/mtu	Modify service
Interface bandwidth	/configuration/protocols/lsp/forwarding/bandwidth-limit	Modify service

Table 64: Mapping of Parameters, XPath, and Supported Operations for VPLS Services (continued)

Field	XPath	Supported Operation
Tagging	Not supported	Not applicable
Starting C-VLAN ID in a range	/configuration/interfaces/unit/vlan-tags/inner-range	Modify service
Ending C-VLAN ID in a range	/configuration/interfaces/unit/vlan-tags/inner-range	Modify service
C-VLAN ID	/configuration/interfaces/unit/vlan-tags/inner (Q-in-Q)	Modify service
V-LAN ID	/configuration/interfaces/unit/vlan-tags/outer (Q-in-Q) /configuration/interfaces/unit/vlan-id (dot1Q)	Modify service
IP address	/configuration/interfaces/unit/vlan-id/ip-address	Modify service
Neighbor IP address	/configuration/interfaces/unit/vlan-id/neighbor-ip-address	Modify service
Peer AS	/configuration/interfaces/unit/vlan-id/peer-as	Create and modify service
AS override	/configuration/interfaces/unit/vlan-id/as-override	Create, modify, and delete service
Interface description	/configuration/interfaces/interface/unit/description	Create, modify, and delete service
Static routes (destination prefix, next hop)	Not supported	Not applicable
Enable or disable of MVPN and MC-LAG (addition of MVPN capability to an existing L3VPN)	Not supported	Not applicable
PE-CE Settings, OSPF Domain ID, version	Not supported	Not applicable
Stitching into a point-to-point service	Both services must be recovered individually according to the current behavior	Not applicable
Route distinguisher (full-mesh OSPF_	Not supported	Not applicable

Recovering Endpoint Deletions from a Service

The following scenarios are supported when recovering endpoint deletion from a service:

- Recovery of a deleted endpoint for multipoint-to-multipoint VPLS and full-mesh Layer 3 VPN services
- Recovery of a deleted spoke for point-to-multipoint VPLS and hub-and-spoke Layer 3 VPN services

Related Documentation • [Creating and Handling a Service Recovery Request on page 406](#)

REST API Changes in Connectivity Services Director for Service Recovery

The previous implementation of Service Recovery in Services Activation Director contained three different REST APIs to create a service request report. The three REST APIs were as follows:

```
PUT method
@Path("/deviceList")
@Consumes({ "application/json" })
public void putDeviceList(List<DeviceBean> deviceList);

PUT method
@Path("/sdList")
@Consumes({ "application/json" })
public void putServiceDefinitionList(List<ServiceDefinitionBean> sdList);

POST method
@Path("/start")
@Consumes({ "application/x-www-form-urlencoded", "application/json" })
public Response startServiceRecovery(ServiceRecoveryProfileBean svcRecProfileBean,
    @Context HttpServletRequest request);
```

In Connectivity Services Director, all these three REST APIs for creating a service request report are being merged into one REST API as follows:

```
POST method
@Path("/startServiceRecovery")
@Consumes({ "application/x-www-form-urlencoded", "application/json" })
public Response startServiceRecovery_V2(ServiceRecoveryProfileBean
    svcRecProfileBean, List<DeviceBean> deviceList, (List<ServiceDefinitionBean>
    sdList, @Context
    HttpServletRequest request);
```

Related Documentation • [Creating and Handling a Service Recovery Request on page 406](#)

Sample XPath Notifications Received on Devices for Deleted Endpoints

For endpoints that are removed from a service, such as a VPLS service, the changed XPath list contains the following values for removed endpoint, which includes the routing instance along with its logical unit of the interface, firewall, and policy, that are deleted from the device.

The following are the changed XPath attributes:

```
/configuration/routing-instances/instance/protocols/vpls/mac-table-size/limit,
/configuration/firewall/family/vpls/filter/term/name,
/configuration/firewall/policer/if-exceeding/bandwidth-limit,
/configuration/firewall/policer/if-exceeding/burst-size-limit
/configuration/interfaces/interface/unit/name
/configuration/routing-instances/instance/interface/name
/configuration/routing-instances/instance/instance-type
/configuration/firewall/policer/name
/configuration/routing-instances/instance/protocols/vpls/site/interface/name
/configuration/routing-instances/instance/protocols/vpls/site/site-preference
/configuration/interfaces/interface/unit/vlan-id
/configuration/interfaces/interface/unit/family/vpls/filter/input/filter-name
/configuration/routing-instances/instance/route-distinguisher/rd-type
/configuration/routing-instances/instance/name
/configuration/interfaces/interface/unit/encapsulation
/configuration/routing-instances/instance/vrf-export
/configuration/routing-instances/instance/protocols/vpls/no-mac-learning
/configuration/firewall/policer/then/discard
/configuration/routing-instances/instance/protocols/vpls/site/site-identifier
/configuration/routing-instances/instance/protocols/vpls/interface-mac-limit/limit

/configuration/firewall/family/vpls/filter/name
/configuration/routing-instances/instance/protocols/vpls/no-tunnel-services
/configuration/firewall/family/vpls/filter/interface-specific
/configuration/firewall/family/vpls/filter/term/then/policer
/configuration/firewall/family/vpls/filter/term/then/accept
/configuration/routing-instances/instance/protocols/vpls/site/name
/configuration/routing-instances/instance/vrf-import
```

The following is the differential configuration set for the XPath attributes:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply op="U">
  <configuration op="U">
    <interfaces op="U">
      <interface op="U">
        <name>ge-0/1/7</name>
        <flexible-vlan-tagging/>
        <mtu>1522</mtu>
        <encapsulation>flexible-ethernet-services</encapsulation>
        <unit op="D">
          <name op="D">29</name>
          <encapsulation op="D">vlan-vpls</encapsulation>
          <vlan-id op="D">34</vlan-id>
          <family op="D">
```

```

        <vp1s op="D">
          <filter op="D">
            <input op="D">
              <filter-name op="D">filter_in_ge-0/1/7_29</filter-name>
            </input>
          </filter>
        </vp1s>
      </family>
    </unit>
  </interface>
</interfaces>
<firewall op="U">
  <family op="U">
    <vp1s op="U">
      <filter op="D">
        <name op="D">filter_in_ge-0/1/7_29</name>
        <interface-specific op="D"/>
        <term op="D">
          <name op="D">1</name>
          <then op="D">
            <policer op="D">policer_in_ge-0/1/7_29</policer>
            <accept op="D"/>
          </then>
        </term>
      </filter>
      <filter op="D">
        <name op="D">filter_in_ge-0/1/8_102</name>
        <interface-specific op="D"/>
        <term op="D">
          <name op="D">1</name>
          <then op="D">
            <policer op="D">policer_in_ge-0/1/8_102</policer>
            <accept op="D"/>
          </then>
        </term>
      </filter>
    </vp1s>
  </family>
  <policer op="D">
    <name op="D">policer_in_ge-0/1/7_29</name>
    <if-exceeding op="D">
      <bandwidth-limit op="D">10m</bandwidth-limit>
      <burst-size-limit op="D">15220</burst-size-limit>
    </if-exceeding>
    <then op="D">
      <discard op="D"/>
    </then>
  </policer>
  <policer op="D">
    <name op="D">policer_in_ge-0/1/8_102</name>
    <if-exceeding op="D">
      <bandwidth-limit op="D">10m</bandwidth-limit>
      <burst-size-limit op="D">15220</burst-size-limit>
    </if-exceeding>
    <then op="D">
      <discard op="D"/>
    </then>
  </policer>
</firewall>
<routing-instances op="U">

```

```
<instance op="D">
  <name op="D">VplsBgpPW</name>
  <instance-type op="D">vpls</instance-type>
  <interface op="D">
    <name op="D">ge-0/1/7.29</name>
  </interface>
  <route-distinguisher op="D">
    <rd-type op="D">36000:23</rd-type>
  </route-distinguisher>
  <vrf-import op="D">VplsBgpPW-import</vrf-import>
  <vrf-export op="D">VplsBgpPW-export</vrf-export>
  <protocols op="D">
    <vpls op="D">
      <mac-table-size op="D">
        <limit op="D">5120</limit>
      </mac-table-size>
      <interface-mac-limit op="D">
        <limit op="D">1024</limit>
      </interface-mac-limit>
      <no-mac-learning op="D"/>
      <no-tunnel-services op="D"/>
      <site op="D">
        <name op="D">Site_2</name>
        <site-identifier op="D">2</site-identifier>
        <site-preference op="D">primary</site-preference>
        <interface op="D">
          <name op="D">ge-0/1/7.29</name>
        </interface>
      </site>
    </vpls>
  </protocols>
</instance>
</routing-instances>
</configuration>
</rpc-reply>
```

Related Documentation

- [Creating and Handling a Service Recovery Request on page 406](#)

Sample XPath Notifications Received on Devices for a Modified VPLS Service

While developing configlets, XPath and Regular Expressions would be used intensively. It would be desirable to let the user define frequently used XPath and Regular expressions in such a way that they can be referred when required. User can define these templates from the XPath and Regex task group in the CLI Configlets workspace of the Junos Space Platform GUI. For a VPLS service that is modified using the Connectivity Services Director application, the XPath attributes corresponding to the modified configuration settings and parameters are sent to the associated devices of the service for the revised configuration elements to be applied on the devices. This topic illustrates the differential configuration, which is the delta or the change-set of the configuration that you are about to deploy on the devices, and the XPath attributes associated with the delta configuration for a modified VPLS service:

The following is the changed XPath attribute for a routing instance of a modified VPLS service:

```
/configuration/routing-instances/instance/route-distinguisher/rd-type
```

The following is the differential configuration set for the XPath attribute for a routing instance of a modified VPLS service:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply op="U">
<configuration op="U">
<routing-instances op="U">
  <instance op="U">
    <name>VplsBasicS0</name>
    <instance-type>vpls</instance-type>
    <interface>
      <name>ge-0/1/4.69</name>
    </interface>
    <route-distinguisher op="U">
      <rd-type op="U">36001:7</rd-type>
    </route-distinguisher>
    <vrf-target>
      <community>target:36000:6</community>
    </vrf-target>
    <protocols>
      <vpls>
        <mac-table-size>
          <limit>5120</limit>
        </mac-table-size>
        <interface-mac-limit>
          <limit>1024</limit>
        </interface-mac-limit>
        <no-tunnel-services/>
        <site>
          <name>Site_1</name>
          <site-identifier>1</site-identifier>
          <site-preference>primary</site-preference>
          <interface>
            <name>ge-0/1/4.69</name>
```

```

        </interface>
      </site>
    </vpls>
  </protocols>
</instance>
</routing-instances>
</configuration>
</rpc-reply>

```

For the **policy-statement** statement at the **[edit policy-options]** hierarchy level, the correct XPath Notification is not received if changes happen only to the policy-statement. The notification does not contain the changed XPath and configuration difference. Therefore, it is not possible to determine the instance of service impacted due to the change (when only localized to **policy-options->policy-statement**). Full service recovery is recommended in such cases.

The following is the changed XPath attribute for physical interfaces:

```
/configuration/interfaces/interface
```

The following is the configuration difference for the XPath attribute of physical interfaces:

```

<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply op="U">
  <configuration op="U">
    <system>
      <services/>
    </system>
    <chassis/>
    <interfaces op="U">
      <interface op="U">
        <name>ge-0/0/5</name>
        <flexible-vlan-tagging/>
        <mtu op="U">1520</mtu>
        <encapsulation>flexible-ethernet-services</encapsulation>
        <unit>
          <name>29</name>
          <encapsulation>vlan-vpls</encapsulation>
          <vlan-tags>
            <outer>34</outer>
          </vlan-tags>
          <family>
            <vpls>
              <filter>
                <input>
                  <filter-name>filter_in_ge-0/0/5_29</filter-name>
                </input>
              </filter>
            </vpls>
          </family>
        </unit>
      </interface>
    </interfaces>
  </configuration>
</rpc-reply>

```

The following is the changed XPath attribute for the logical unit of an interface:

```
/configuration/interfaces/interface/unit/vlan-tags/outer
```

The following is the configuration difference for the XPath attribute of logical unit of an interface:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply op="U">
  <configuration op="U">
    <system>
      <services/>
    </system>
    <chassis/>
    <interfaces op="U">
      <interface op="U">
        <name>ge-0/0/5</name>
        <flexible-vlan-tagging/>
        <mtu>1522</mtu>
        <encapsulation>flexible-ethernet-services</encapsulation>
        <unit op="U">
          <name>29</name>
          <encapsulation>vlan-vpls</encapsulation>
          <vlan-tags op="U">
            <outer op="U">34</outer>
          </vlan-tags>
          <family>
            <vpls>
              <filter>
                <input>
                  <filter-name>filter_in_ge-0/0/5_29</filter-name>
                </input>
              </filter>
            </vpls>
          </family>
        </unit>
      </interface>
    </interfaces>
  </configuration>
</rpc-reply>
```

The following are the changed XPath attributes for a firewall filter at the **[edit firewall family vpls]** hierarchy level:

```
/configuration/firewall/family/vpls/filter/term/then/discard,
/configuration/firewall/family/vpls/filter/term/name
```

The following is the configuration difference for the XPath attribute of a firewall filter in a VPLS family:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply op="U">
```

```

<configuration op="U">
  <system>
    <services/>
  </system>
  <chassis/>
  <interfaces op="U">
    <interface op="U">
      <name>ge-0/0/5</name>
      <flexible-vlan-tagging/>
      <mtu op="U">1520</mtu>
      <encapsulation>flexible-ethernet-services</encapsulation>
      <unit>
        <name>29</name>
        <encapsulation>vlan-vpls</encapsulation>
        <vlan-tags>
          <outer>34</outer>
        </vlan-tags>
        <family>
          <vpls>
            <filter>
              <input>
                <filter-name>filter_in_ge-0/0/5_29</filter-name>
              </input>
            </filter>
          </vpls>
        </family>
      </unit>
    </interface>
  </interfaces>
</configuration>
</rpc-reply>

```

The following are the changed XPath attributes for the **policer** statement at the **[edit firewall]** hierarchy level:

```

/configuration/firewall/policer/if-exceeding/bandwidth-percent
/configuration/firewall/policer/if-exceeding/bandwidth-limit

```

The following is the configuration difference for the XPath attribute of a firewall policer:

```

<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply op="U">
  <configuration op="U">
    <system>
      <services/>
    </system>
    <chassis/>
    <interfaces op="U">
      <interface op="U">
        <name>ge-0/0/5</name>
        <flexible-vlan-tagging/>
        <mtu op="U">1520</mtu>
        <encapsulation>flexible-ethernet-services</encapsulation>
        <unit>
          <name>29</name>

```

```

    <encapsulation>vlan-vpls</encapsulation>
    <vlan-tags>
      <outer>34</outer>
    </vlan-tags>
    <family>
      <vpls>
        <filter>
          <input>
            <filter-name>filter_in_ge-0/0/5_29</filter-name>
          </input>
        </filter>
      </vpls>
    </family>
  </unit>
</interface>
</interfaces>
</configuration>
</rpc-reply>

```

The service instance cannot be determined if the changes to policer occur and in such cases, you need to determine the type of service and also identify whether the change is to existing service or a new service. You can select a service instance and the operation type (such as create or modify) to recover service for that endpoint. Using changed XPath and applying the differential configuration to the changed XPath, you can determine the type of change and the name of the changed configuration parameter.

Related Documentation

- [Creating and Handling a Service Recovery Request on page 406](#)

Sample XPath Notifications Received on Devices for a Created VPLS Service

This topic illustrates the differential configuration, which is the delta or the change-set of the configuration that you are about to deploy on the devices, and the XPath attributes associated with the delta configuration for a newly created VPLS service:

The following are the configuration stanzas and device settings for a newly created VPLS service at the different hierarchy levels of the CLI interface:

```

[edit interfaces ge-0/1/7]
unit 29 {
  encapsulation vlan-vpls;
  vlan-id 34;
  family vpls {
    filter {
      input filter_in_ge-0/1/7_29;
    }
  }
}

```

```

[edit firewall family vpls]
filter filter_in_ge-0/1/8_102 { ... }

```

```
filter filter_in_ge-0/1/7_29 {
  interface-specific;
  term 1 {
    then {
      policer policer_in_ge-0/1/7_29;
      accept;
    }
  }
}
```

```
[edit firewall]
policer policer_in_ge-0/1/8_102 { ... }
policer policer_in_ge-0/1/7_29 {
  if-exceeding {
    bandwidth-limit 10m;
    burst-size-limit 1g;
  }
  then discard;
}
```

```
[edit routing-instances]
VplsBgpPW {
  instance-type vpls;
  interface ge-0/1/7.29;
  route-distinguisher 36000:23;
  vrf-import VplsBgpPW-import;
  vrf-export VplsBgpPW-export;
  protocols {
    vpls {
      mac-table-size {
        5120;
      }
      interface-mac-limit {
        1024;
      }
      no-mac-learning;
      no-tunnel-services;
      site Site_2 {
        site-identifier 2;
        site-preference primary;
        interface ge-0/1/7.29;
      }
    }
  }
}
```

The following are the changed XPath attributes for a newly created VPLS service:

```
/configuration/routing-instances/instance/protocols/vpls/mac-table-size/limit
/configuration/firewall/family/vpls/filter/term/name
/configuration/firewall/policer/if-exceeding/burst-size-limit
/configuration/interfaces/interface/unit/name
/configuration/routing-instances/instance/interface/name
/configuration/routing-instances/instance/instance-type
```

```

/configuration/firewall/policer/name
/configuration/routing-instances/instance/protocols/vpls/site/interface/name
/configuration/routing-instances/instance/protocols/vpls/site/site-preference
/configuration/interfaces/interface/unit/vlan-id
/configuration/interfaces/interface/unit/family/vpls/filter/input/filter-name
/configuration/routing-instances/instance/route-distinguisher/rd-type
/configuration/routing-instances/instance/name
/configuration/interfaces/interface/unit/encapsulation
/configuration/routing-instances/instance/vrf-export
/configuration/routing-instances/instance/protocols/vpls/no-mac-learning
/configuration/firewall/policer/then/discard
/configuration/routing-instances/instance/protocols/vpls/site/site-identifier
/configuration/routing-instances/instance/protocols/vpls/interface-mac-limit/limit
/configuration/firewall/family/vpls/filter/name
/configuration/routing-instances/instance/protocols/vpls/no-tunnel-services
/configuration/firewall/family/vpls/filter/interface-specific
/configuration/firewall/family/vpls/filter/term/then/policer
/configuration/firewall/family/vpls/filter/term/then/accept
/configuration/routing-instances/instance/protocols/vpls/site/name
/configuration/routing-instances/instance/vrf-import

```

The following is the differential configuration set for the XPath attributes of a newly created VPLS service:

```

<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply op="U">
  <configuration op="U">
    <interfaces op="U">
      <interface op="U">
        <name>ge-0/1/7</name>
        <flexible-vlan-tagging/>
        <mtu>1522</mtu>
        <encapsulation>flexible-ethernet-services</encapsulation>
        <unit op="C">
          <name op="C">29</name>
          <encapsulation op="C">vlan-vpls</encapsulation>
          <vlan-id op="C">34</vlan-id>
          <family op="C">
            <vpls op="C">
              <filter op="C">
                <input op="C">
                  <filter-name op="C">filter_in_ge-0/1/7_29</filter-name>
                </input>
              </filter>
            </vpls>
          </family>
        </unit>
      </interface>
    </interfaces>
    <firewall op="U">
      <family op="U">
        <vpls op="U">
          <filter op="C">
            <name op="C">filter_in_ge-0/1/7_29</name>
            <interface-specific op="C"/>
            <term op="C">
              <name op="C">1</name>

```

```

        <then op="C">
            <policer op="C">policer_in_ge-0/1/7_29</policer>
            <accept op="C"/>
        </then>
    </term>
</filter>
</vpls>
</family>
<policer op="C">
    <name op="C">policer_in_ge-0/1/7_29</name>
    <if-exceeding op="C">
        <bandwidth-limit op="C">10m</bandwidth-limit>
        <burst-size-limit op="C">1g</burst-size-limit>
    </if-exceeding>
    <then op="C">
        <discard op="C"/>
    </then>
</policer>
</firewall>
<routing-instances op="U">
    <instance op="C">
        <name op="C">VplsBgpPW</name>
        <instance-type op="C">vpls</instance-type>
        <interface op="C">
            <name op="C">ge-0/1/7.29</name>
        </interface>
        <route-distinguisher op="C">
            <rd-type op="C">36000:23</rd-type>
        </route-distinguisher>
        <vrf-import op="C">VplsBgpPW-import</vrf-import>
        <vrf-export op="C">VplsBgpPW-export</vrf-export>
        <protocols op="C">
            <vpls op="C">
                <mac-table-size op="C">
                    <limit op="C">5120</limit>
                </mac-table-size>
                <interface-mac-limit op="C">
                    <limit op="C">1024</limit>
                </interface-mac-limit>
                <no-mac-learning op="C"/>
                <no-tunnel-services op="C"/>
                <site op="C">
                    <name op="C">Site_2</name>
                    <site-identifier op="C">2</site-identifier>
                    <site-preference op="C">primary</site-preference>
                    <interface op="C">
                        <name op="C">ge-0/1/7.29</name>
                    </interface>
                </site>
            </vpls>
        </protocols>
    </instance>
</routing-instances>
</configuration>
</rpc-reply>

```

Related Documentation • [Creating and Handling a Service Recovery Request on page 406](#)

Sample XPath Notifications Received on Devices for a Created Layer 3 VPN Service

This topic illustrates the differential configuration, which is the delta or the change-set of the configuration that you are about to deploy on the devices, and the XPath attributes associated with the delta configuration for a newly created Layer 3 VPN service:

The following is the changed XPath attribute for routing instances of a newly created Layer 3 VPN service:

```
/configuration/routing-instances/instance/route-distinguisher/rd-type
```

For the **policy-statement** statement at the **[edit policy-options]** hierarchy level, the correct XPath Notification is not received if changes happen only to the policy-statement. The notification does not contain the changed XPath and configuration difference. Therefore, it is not possible to determine the instance of service impacted due to the change (when only localized to **policy-options->policy-statement**). Full service recovery is recommended in such cases.

The following is the changed XPath attribute for physical interfaces:

```
/configuration/interfaces/interface/mtu
```

The following is the changed XPath attribute for the logical unit of interfaces:

```
/configuration/interfaces/interface/unit/description
```

The following are the changed XPath attributes for the **policer** statement at the **[edit firewall]** hierarchy level:

```
/configuration/firewall/policer/if-exceeding/bandwidth-percent  
/configuration/firewall/policer/if-exceeding/bandwidth-limit
```

The service instance cannot be determined if the changes to policer occur and in such cases, you need to determine the type of service and also identify whether the change is to existing service or a new service. You can select a service instance and the operation type (such as create or modify) to recover service for that endpoint. Using changed XPath and applying the differential configuration to the changed XPath, you can determine the type of change and the name of the changed configuration parameter.

Related Documentation

- [Creating and Handling a Service Recovery Request on page 406](#)

Sample XPath Notifications Received on Devices for a Created Point-to-Point Service

This topic illustrates the differential configuration, which is the delta or the change-set of the configuration that you are about to deploy on the devices, and the XPath attributes associated with the delta configuration for a newly created point-to-point service. The following two scenarios need to be handled for P2P services. Accordingly, the mechanism to identify impacted services is implemented.

- A or Z endpoint of the existing service
- A pseudowire extension for VPLS or L3VPN services

The following is the changed XPath attribute for Layer 2 circuit of a newly created point-to-point service:

```
/configuration/protocols/l2circuit/neighbor/interface/description
```

The following is the configuration difference corresponding to the XPath attribute for Layer 2 circuit:

```
<protocols op="U">
  <l2circuit op="U">
    <neighbor op="U">
      <name>128.220.3.158</name>
      <interface>
        <name>ge-0/1/5.560</name>
        <virtual-circuit-id>1</virtual-circuit-id>
        <mtu>1522</mtu>
      </interface>
      <interface>
        <name>ge-0/1/5.512</name>
        <virtual-circuit-id>2</virtual-circuit-id>
        <mtu>1522</mtu>
      </interface>
      <interface op="U">
        <name>ge-0/0/3.0</name>
        <virtual-circuit-id>221</virtual-circuit-id>
        <description op="U">TestP2P2</description>
        <community>R2-to-R1</community>
        <mtu>1522</mtu>
      </interface>
    </neighbor>
  </l2circuit>
</protocols>
```

For the **policy-statement** statement at the **[edit policy-options]** hierarchy level, the correct XPath Notification is not received if changes happen only to the policy-statement. The notification does not contain the changed XPath and configuration difference. Therefore, it is not possible to determine the instance of service impacted due to the change (when only localized to **policy-options->policy-statement**). Full service recovery is recommended in such cases.

The following is the changed XPath attribute for physical interfaces:

```
/configuration/interfaces/interface/mtu
```

The following is the changed XPath attribute for the logical unit of interfaces:

```
/configuration/interfaces/interface/unit/description
```

The following are the changed XPath attributes for the **policer** statement at the **[edit firewall]** hierarchy level:

```
/configuration/firewall/policer/if-exceeding/bandwidth-percent  
/configuration/firewall/policer/if-exceeding/bandwidth-limit
```

The following are the changed XPath attributes for the **filter** statement at the **[edit firewall family family-name filter filter-name term term-name]** hierarchy level

```
/configuration/firewall/filter
```

The service instance cannot be determined if the changes to policer occur and in such cases, you need to determine the type of service and also identify whether the change is to existing service or a new service. You can select a service instance and the operation type (such as create or modify) to recover service for that endpoint. Using changed XPath and applying the differential configuration to the changed XPath, you can determine the type of change and the name of the changed configuration parameter.

Related Documentation

- [Creating and Handling a Service Recovery Request on page 406](#)

Sample XPath Notifications Received on Devices for CFM Profiles Associated with a P2P Service

This topic illustrates the differential configuration, which is the delta or the change-set of the configuration that you are about to deploy on the devices, and the XPath attributes associated with the delta configuration for CFM profiles associated with a point-to-point service:

The following is the changed XPath attribute for CFM profiles of a point-to-point service:

```
/configuration/protocols/oam/ethernet/connectivity-fault-management/maintenance-domain/  
maintenance-association/continuity-check/loss-threshold
```

The following is the configuration difference corresponding to the XPath attribute for CFM profiles associated with a point-to-point service:

```
<protocols op="U">
  <oam op="U">
    <ethernet op="U">
      <connectivity-fault-management op="U">
        <maintenance-domain op="U">
          <name>Default-Domain</name>
          <level>1</level>
          <maintenance-association>
            <name>PW_1001_P2P-CFM992015-12-30-05</name>
            <continuity-check>
              <interval>1s</interval>
              <loss-threshold>3</loss-threshold>
              <hold-interval>10</hold-interval>
            </continuity-check>
            <mep>
              <name>1</name>
              <interface>
                <interface-name>ge-0/0/5.1</interface-name>
              </interface>
              <direction>up</direction>
              <auto-discovery/>
              <lowest-priority-defect>all-defects</lowest-priority-defect>
            </mep>
          </maintenance-association>
          <maintenance-association>
            <name>PW_101_P2P-Asym-CFM2015-12-30-</name>
            <continuity-check>
              <interval>1s</interval>
              <loss-threshold>3</loss-threshold>
              <hold-interval>10</hold-interval>
            </continuity-check>
            <mep>
              <name>3</name>
              <interface>
                <interface-name>ge-0/0/4.0</interface-name>
              </interface>
              <direction>up</direction>
              <auto-discovery/>
              <lowest-priority-defect>all-defects</lowest-priority-defect>
            </mep>
          </maintenance-association>
          <maintenance-association op="U">
            <name>PW_221_P2PService1</name>
            <continuity-check op="U">
              <interval>1s</interval>
              <loss-threshold op="U">5</loss-threshold>
              <hold-interval>10</hold-interval>
            </continuity-check>
            <mep>
              <name>1</name>
              <interface>
                <interface-name>ge-0/0/2.0</interface-name>
              </interface>
              <direction>up</direction>
              <auto-discovery/>
              <lowest-priority-defect>all-defects</lowest-priority-defect>
            </mep>
          </maintenance-association>
        </maintenance-domain>
      </connectivity-fault-management>
    </ethernet>
  </oam>
</protocols>
```

```

        </maintenance-association>
      </maintenance-domain>
    </connectivity-fault-management>
  </ethernet>
</oam>
</protocols>

```

**Related
Documentation**

- [Creating and Handling a Service Recovery Request on page 406](#)

Sample XPath Notifications Received on Devices for CoS Profiles Associated with a P2P Service

This topic illustrates the differential configuration, which is the delta or the change-set of the configuration that you are about to deploy on the devices, and the XPath attributes associated with the delta configuration for CoS profiles associated with a point-to-point service:

The following is the changed XPath attribute for CoS profiles of a point-to-point service:

```
/configuration/class-of-service/interfaces/interface/shaping-rate/rate
```

The following is the configuration difference corresponding to the XPath attribute for CoS profiles associated with a point-to-point service:

```

<class-of-service op="U">
  <interfaces op="U">
    <interface op="U">
      <name>ge-0/0/3</name>
      <scheduler-map>nd_schedulerMap</scheduler-map>
      <unit>
        <name>513</name>
        <classifiers>
          <dscp>
            <name>dscp_nd_classifier</name>
          </dscp>
        </classifiers>
      </unit>
      <shaping-rate op="C">
        <rate op="C">160001</rate>
      </shaping-rate>
    </interface>
  </interfaces>
</class-of-service>

```

**Related
Documentation**

- [Creating and Handling a Service Recovery Request on page 406](#)

PART 7

Service Design: Working with Service Definitions

- [Service Design: Predefined Service Definitions on page 465](#)
- [Service Design: Managing Point-to-Point Service Definitions on page 593](#)
- [Service Design: Managing VPLS Service Definitions on page 653](#)
- [Service Design: Managing Layer 3 VPN Service Definitions on page 709](#)

Service Design: Predefined Service Definitions

- [Predefined Service Definitions on page 465](#)
- [Predefined Point-to-Point Service Definitions on page 517](#)
- [Predefined Multipoint-to-Multipoint Ethernet Service Definitions on page 551](#)
- [Predefined Point-to-Multipoint Ethernet Service Definitions on page 576](#)
- [Predefined Full Mesh Layer 3 VPN Service Definitions on page 589](#)
- [Predefined Hub-and-Spoke Layer 3 VPN Service Definitions on page 590](#)

Predefined Service Definitions

Connectivity Services Director provides predefined service definitions that a service provisioner can use when creating a service order.

If none of the predefined service definitions is appropriate for your needs, you can create a service definition as described in [“Creating a Point-to-Point Ethernet Service Definition” on page 625](#), [“Creating a Point-to-Multipoint VPLS Service Definition” on page 678](#), or [“Creating a Service Definition for VPLS Access into Layer 3 Networks” on page 705](#).

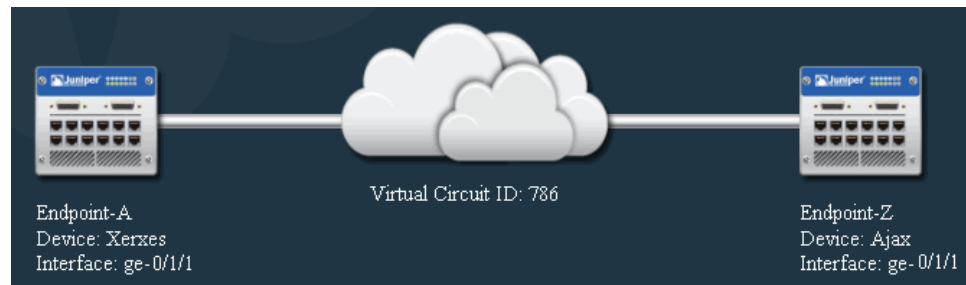
The Junos Space Connectivity Services Director product provides predefined service definitions for Ethernet point-to-point services and for VPLS services. The following sections describe these service definitions:

- [Ethernet Point-to-Point Predefined Service Definitions on page 465](#)
- [Multipoint-to-Multipoint Predefined Service Definitions on page 489](#)
- [Point-to-Multipoint Service Definitions on page 515](#)

Ethernet Point-to-Point Predefined Service Definitions

The Ethernet Activator software provides predefined service definitions for Ethernet point-to-point services that use LDP switching in the network core. These services are sometimes known as E-Line Martini services. [Figure 31 on page 466](#) shows an example of such a service.

Figure 31: Point-to-Point Service



Information specific to each service instance, such as the device name, endpoint name, and customer VLAN ID, is provided in the service order. Attributes that can apply across many service instances are typically defined in the service definition. These attributes include:

- Ethernet option (dot1q, port-port, qinq)
- Traffic type (single VLAN, multiple VLAN, all traffic)
- Physical interface encapsulation
- Logical interface encapsulation
- Rate limit range

[Table 65 on page 466](#) lists each of the standard Ethernet point-to-point service definitions. Each standard service definition is then described in detail in the sections that follow.

Table 65: Standard Service Definitions

Standard Service Definition Name	Service Attributes
"ELine-Dot1q-SingleVLAN" on page 468	<ul style="list-style-type: none"> • Point-to-point service for M Series and MX Series devices • Gigabit Ethernet interfaces • 802.1Q endpoint interface types • Customer traffic is single VLAN • Flexible-ethernet-services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELine-Dot1q-SingleVLAN-CCC" on page 470	<ul style="list-style-type: none"> • Point-to-point service for J Series, M Series, and MX Series devices • Gigabit Ethernet interfaces • 802.1Q endpoint interface types • Customer traffic is single VLAN • Vlan-ccc physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment

Table 65: Standard Service Definitions (continued)

Standard Service Definition Name	Service Attributes
"ELine-Dot1q-SingleVLAN-Ext-CCC" on page 472	<ul style="list-style-type: none"> Point-to-point service for J Series, M Series, and MX Series devices Gigabit Ethernet interfaces 802.1Q endpoint interface types Customer traffic is single VLAN Extended-vlan-ccc physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELine-PortBased" on page 474	<ul style="list-style-type: none"> Point-to-point service for J Series, M Series, and MX Series devices Gigabit Ethernet interfaces Port-based UNI Ethernet-ccc physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELine-QinQ-AllVLAN" on page 476	<ul style="list-style-type: none"> Point-to-point service for M Series and MX Series devices Gigabit Ethernet interfaces Q-in-Q endpoint interface types All customer traffic Flexible-ethernet-services physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELine-QinQ-AllVLAN-CCC" on page 479	<ul style="list-style-type: none"> Point-to-point service for J series, M Series, and MX Series devices Gigabit Ethernet interfaces Q-in-Q endpoint interface types All customer traffic Vlan-ccc physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELine-QinQ-AllVLAN-Ext-CCC" on page 481	<ul style="list-style-type: none"> Point-to-point service for J Series, M Series, and MX Series devices Gigabit Ethernet interfaces Q-in-Q endpoint interface types All customer traffic Extended-vlan-ccc physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment

Table 65: Standard Service Definitions (continued)

Standard Service Definition Name	Service Attributes
"ELine-QinQ-VLANRange" on page 483	<ul style="list-style-type: none"> Point-to-point service for MX Series devices only Gigabit Ethernet interfaces Q-in-Q endpoint interface types Customer traffic is range of VLANs Flexible-ethernet-services physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELine-QinQ-VLANRange-CCC" on page 485	<ul style="list-style-type: none"> Point-to-point service for MX Series devices only Gigabit Ethernet interfaces Q-in-Q endpoint interface types Customer traffic is range of VLANs Vlan-ccc physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELine-QinQ-VLANRange-Ext-CCC" on page 487	<ul style="list-style-type: none"> Point-to-point service for MX Series devices only Gigabit Ethernet interfaces Q-in-Q endpoint interface types Customer traffic is range of VLANs Extended-vlan-ccc physical encapsulation Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment

ELine-Dot1q-SingleVLAN

This service definition provides a base for creating point-to-point services that transport a single VLAN across an LDP network core using 802.1Q endpoint interface types and flexible-ethernet-services as the physical encapsulation type. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- [Configuration on Endpoint A on page 468](#)
- [Configuration on Endpoint Z on page 469](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```
ge-0/1/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation flexible-ethernet-services;
    unit 1 {
```

```

        description "Dot1q Eline Martini ";
        encapsulation vlan-ccc;
        vlan-id 1;
        family ccc {
            filter {
                input filter_in_ge-0/1/1_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/1_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
}

family ccc {
    filter filter_in_ge-0/1/1_1 {
        interface-specific;
        term 1 {
            then {
                policer policer_in_ge-0/1/1_1;
                accept;
            }
        }
    }
}

protocols {
    l2circuit {
        neighbor 192.168.1.40
        interface ge-0/1/1.1 {
            virtual-circuit-id 786;
            no-control-word;
            mtu 1522;
        }
    }
}
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z:

```

ge-0/1/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation flexible-ethernet-services;
    unit 1 {
        description "Dot1q Eline Martini ";
        encapsulation vlan-ccc;
        vlan-id 1;
        family ccc {
            filter {
                input filter_in_ge-0/1/1_1;
            }
        }
    }
}

```

```

    }
}

firewall {
  policer policer_in_ge-0/1/1_1 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
    then discard;
  }
}

family ccc {
  filter filter_in_ge-0/1/1_1 {
    interface-specific;
    term 1 {
      then {
        policer policer_in_ge-0/1/1_1;
        accept;
      }
    }
  }
}

protocols {
  l2circuit {
    neighbor 192.168.1.30 {
      interface ge-0/1/1.1 {
        virtual-circuit-id 786;
        no-control-word;
        mtu 1522;
      }
    }
  }
}

```

ELine-Dot1q-SingleVLAN-CCC

This service definition provides a base for creating point-to-point services that transport a single VLAN across an LDP network core using 802.1Q endpoint interface types and vlan-ccc as the physical encapsulation type. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- [Configuration on Endpoint A on page 470](#)
- [Configuration on Endpoint Z on page 471](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```

ge-0/1/1 {
  flexible-vlan-tagging;
  mtu 1522;
  encapsulation vlan-ccc;
}

```

```

    unit 513 {
        description VLANCCC-SR;
        encapsulation vlan-ccc;
        vlan-id 513;
        family ccc {
            filter {
                input filter_in_ge-0/1/1_513;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/1_513 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family ccc {
        filter filter_in_ge-0/1/1_513 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/1/1_513;
                    accept;
                }
            }
        }
    }
}

protocols {
    l2circuit {
        neighbor 192.168.1.40 {
            interface ge-0/1/1.513 {
                virtual-circuit-id 786;
                no-control-word;
                mtu 1522;
            }
        }
    }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z:

```

ge-0/1/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation vlan-ccc;
    unit 513 {
        description VLANCCC-SR;
        encapsulation vlan-ccc;
    }
}

```

```

        vlan-id 513;
        family ccc {
            filter {
                input filter_in_ge-0/1/1_513;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/1_513 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family ccc {
        filter filter_in_ge-0/1/1_513 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/1/1_513;
                    accept;
                }
            }
        }
    }
}

protocols {
    l2circuit {
        neighbor 192.168.1.30 {
            interface ge-0/1/1.513 {
                virtual-circuit-id 786;
                no-control-word;
                mtu 1522;
            }
        }
    }
}

```

ELine-Dot1q-SingleVLAN-Ext-CCC

This service definition provides a base for creating point-to-point services that transport a single VLAN across an LDP network core using 802.1Q endpoint interface types and extended-vlan-ccc as the physical encapsulation type. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- [Configuration on Endpoint A on page 473](#)
- [Configuration on Endpoint Z on page 474](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```

ge-0/1/1 {
  flexible-vlan-tagging;
  mtu 1522;
  encapsulation extended-vlan-ccc;
  unit 1 {
    description Extended-SR;
    vlan-id 1;
    family ccc {
      filter {
        input filter_in_ge-0/1/1_1;
      }
    }
  }
}

firewall {
  policer policer_in_ge-0/1/1_1 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
    then discard;
  }
  family ccc {
    filter filter_in_ge-0/1/1_1 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/1/1_1;
          accept;
        }
      }
    }
  }
}

protocols {
  l2circuit {
    neighbor 192.168.1.40 {
      interface ge-0/1/1.1 {
        virtual-circuit-id 786;
        no-control-word;
        mtu 1522;
      }
    }
  }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z:

```

ge-0/1/1 {
  flexible-vlan-tagging;
  mtu 1522;
  encapsulation extended-vlan-ccc;
  unit 1 {
    description Extended-SR;
    vlan-id 1;
    family ccc {
      filter {
        input filter_in_ge-0/1/1_1;
      }
    }
  }
}

firewall {
  policer policer_in_ge-0/1/1_1 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
    then discard;
  }
  family ccc {
    filter filter_in_ge-0/1/1_1 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/1/1_1;
          accept;
        }
      }
    }
  }
}

protocols {
  l2circuit {
    neighbor 192.168.1.30 {
      interface ge-0/1/1.1 {
        virtual-circuit-id 786;
        no-control-word;
        mtu 1522;
      }
    }
  }
}

```

ELine-PortBased

This service definition provides a base for creating point-to-point services that transport all traffic across an LDP network core using an entire port at each endpoint using ethernet-ccc as the physical encapsulation type. Service provisioners can limit the

bandwidth of services built from this service definition to specific values from 10 Mbps to 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- [Configuration on Endpoint A on page 475](#)
- [Configuration on Endpoint Z on page 476](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```
ge-0/1/1 {
  encapsulation ethernet-ccc;
  unit 0 {
    family ccc {
      filter {
        input filter_in_ge-0/1/1;
      }
    }
  }
}

firewall {
  policer policer_in_ge-0/1/1 {
    if-exceeding {
      bandwidth-limit 10m;
      burst-size-limit 6250000;
    }
    then discard;
  }
  family ccc {
    filter filter_in_ge-0/1/1 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/1/1;
          accept;
        }
      }
    }
  }
}

protocols {
  l2circuit {
    neighbor 192.168.1.40 {
      interface ge-0/1/1.0 {
        virtual-circuit-id 786;
        no-control-word;
        mtu 1522;
      }
    }
  }
}
```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z:

```

ge-0/1/1 {
    encapsulation ethernet-ccc;
    unit 0 {
        family ccc {
            filter {
                input filter_in_ge-0/1/1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/1 {
        if-exceeding {
            bandwidth-limit 10m;
            burst-size-limit 6250000;
        }
        then discard;
    }
    family ccc {
        filter filter_in_ge-0/1/1 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/1/1;
                    accept;
                }
            }
        }
    }
}

protocols {
    l2circuit {
        neighbor 192.168.1.30 {
            interface ge-0/1/1.0 {
                virtual-circuit-id 786;
                no-control-word;
                mtu 1522;
            }
        }
    }
}

```

ELine-QinQ-AllVLAN

This service definition provides a base for creating point-to-point services that transport all customer traffic across an LDP network core using Q-in-Q endpoint interface types and flexible-ethernet-services as the physical encapsulation type. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- [Configuration on Endpoint A on page 477](#)
- [Configuration on Endpoint Z on page 478](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```
ge-0/1/1 {
  flexible-vlan-tagging;
  mtu 1522;
  encapsulation flexible-ethernet-services;
  unit 1 {
    description "AllVlanTransport";
    encapsulation vlan-ccc;
    vlan-tags outer 1;
    family ccc {
      filter {
        input filter_in_ge-0/1/1_1;
      }
    }
  }
}

protocols {
  l2circuit {
    neighbor 192.168.1.40 {
      interface ge-0/1/1.1 {
        virtual-circuit-id 786;
        no-control-word;
        mtu 1522;
      }
    }
  }
}

firewall {
  policer policer_in_ge-0/1/1_1 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
    then discard;
  }
  family ccc {
    filter filter_in_ge-0/1/1_1 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/1/1_1;
          accept;
        }
      }
    }
  }
}
```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z:

```
ge-0/1/1 {
  flexible-vlan-tagging;
  mtu 1522;
  encapsulation flexible-ethernet-services;
  unit 1 {
    description "AllVlanTransport";
    encapsulation vlan-ccc;
    vlan-tags outer 1;
    family ccc {
      filter {
        input filter_in_ge-0/1/1_1;
      }
    }
  }
}

firewall {
  policer policer_in_ge-0/1/1_1 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
    then discard;
  }
  family ccc {
    filter filter_in_ge-0/1/1_1 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/1/1_1;
          accept;
        }
      }
    }
  }
}

protocols {
  l2circuit {
    neighbor 192.168.1.30 {
      interface ge-0/1/1.1 {
        virtual-circuit-id 786;
        no-control-word;
        mtu 1522;
      }
    }
  }
}
```

ELine-QinQ-AllVLAN-CCC

This service definition provides a base for creating point-to-point services that transport all customer traffic across an LDP network core using Q-in-Q endpoint interface types and vlan-ccc as the physical encapsulation type. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- [Configuration on Endpoint A on page 479](#)
- [Configuration on Endpoint Z on page 480](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```
ge-0/1/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation vlan-ccc;
    unit 515 {
        description QinQ-ALLVLAN;
        encapsulation vlan-ccc;
        vlan-tags outer 515;
        family ccc {
            filter {
                input filter_in_ge-0/1/1_515;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/1_515 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }

    family ccc {
        filter filter_in_ge-0/1/1_515 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/1/1_515;
                    accept;
                }
            }
        }
    }
}
```

```

protocols {
  l2circuit {
    neighbor 192.168.1.40 {
      interface ge-0/1/1.515 {
        virtual-circuit-id 786;
        no-control-word;
        mtu 1522;
      }
    }
  }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z:

```

ge-0/1/1 {
  flexible-vlan-tagging;
  mtu 1522;
  encapsulation vlan-ccc;
  unit 515 {
    description QinQ-ALLVLAN;
    encapsulation vlan-ccc;
    vlan-tags outer 515;
    family ccc {
      filter {
        input filter_in_ge-0/1/1_515;
      }
    }
  }
}

firewall {
  policer policer_in_ge-0/1/1_515 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
    then discard;
  }
  family ccc {
    filter filter_in_ge-0/1/1_515 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/1/1_515;
          accept;
        }
      }
    }
  }
}

protocols {
  l2circuit {
    neighbor 192.168.1.30 {
      interface ge-0/1/1.515 {

```



```

        virtual-circuit-id 786;
        no-control-word;
        mtu 1522;
    }
}
}

```

ELine-QinQ-AllVLAN-Ext-CCC

This service definition provides a base for creating point-to-point services that transport all customer traffic across an LDP network core using Q-in-Q endpoint interface types and extended-vlan-ccc as the physical encapsulation type. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- [Configuration on Endpoint A on page 481](#)
- [Configuration on Endpoint Z on page 482](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```

ge-0/1/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation extended-vlan-ccc;
    unit 1 {
        description Ext-AllVLAN;
        vlan-tags outer 1;
        family ccc {
            filter {
                input filter_in_ge-0/1/1_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/1_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family ccc {
        filter filter_in_ge-0/1/1_1 {
            interface-specific;
            term 1 {

```

```

        then {
            policer policer_in_ge-0/1/1_1;
            accept;
        }
    }
}

protocols {
    l2circuit {
        neighbor 192.168.1.40 {
            interface ge-0/1/1.1 {
                virtual-circuit-id 786;
                no-control-word;
                mtu 1522;
            }
        }
    }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z:

```

ge-0/1/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation extended-vlan-ccc;
    unit 1 {
        description Ext-AllVLAN;
        vlan-tags outer 1;
        family ccc {
            filter {
                input filter_in_ge-0/1/1_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/1_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family ccc {
        filter filter_in_ge-0/1/1_1 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/1/1_1;
                }
            }
        }
    }
}

```

```

    accept;
  }
}
}
}

protocols {
  l2circuit {
    neighbor 192.168.1.30 {
      interface ge-0/1/1.1 {
        virtual-circuit-id 786;
        no-control-word;
        mtu 1522;
      }
    }
  }
}

```

ELine-QinQ-VLANRange

This service definition provides a base for creating point-to-point services that transport a range of VLANs across an LDP network core using Q-in-Q endpoint interface types and flexible-ethernet-services as the physical encapsulation type. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- [Configuration on Endpoint A on page 483](#)
- [Configuration on Endpoint Z on page 484](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```

ge-0/1/1 {
  flexible-vlan-tagging;
  mtu 1522;
  encapsulation flexible-ethernet-services;
  unit 2 {
    description "QinQ Eline Martini";
    encapsulation vlan-ccc;
    vlan-tags outer 2 inner-range 100-110;
    family ccc {
      filter {
        input filter_in_ge-0/1/1_2;
      }
    }
  }
}

```

```

firewall {
  policer policer_in_ge-0/1/1_2 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
  }

  family ccc {
    filter filter_in_ge-0/1/1_2 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/1/1_2;
          accept;
        }
      }
    }
  }

  protocols {
    l2circuit {
      neighbor 192.168.1.40 {
        interface ge-0/1/1.2 {
          virtual-circuit-id 786;
          no-control-word;
          mtu 1522;
        }
      }
    }
  }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z:

```

ge-0/1/1 {
  flexible-vlan-tagging;
  mtu 1522;
  encapsulation flexible-ethernet-services;
  unit 2 {
    description "QinQ Eline Martini";
    encapsulation vlan-ccc;
    vlan-tags outer 2 inner-range 100-110;
    family ccc {
      filter {
        input filter_in_ge-0/1/1_2;
      }
    }
  }
}

firewall {
  policer policer_in_ge-0/1/1_2 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
  }
}

```

```

        then discard;
    }

    family ccc {
        filter filter_in_ge-0/1/1_2 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/1/1_2;
                    accept;
                }
            }
        }
    }
}

protocols {
    l2circuit {
        interface ge-0/1/1.2 {
            virtual-circuit-id 786;
            no-control-word;
            mtu 1522;
        }
    }
}
}

```

ELine-QinQ-VLANRange-CCC

This service definition provides a base for creating point-to-point services that transport a range of VLANs across an LDP network core using Q-in-Q endpoint interface types and vlan-ccc as the physical encapsulation type. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- [Configuration on Endpoint A on page 485](#)
- [Configuration on Endpoint Z on page 486](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```

ge-0/1/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation vlan-ccc;
    unit 514 {
        description VLANRANGE-SR;
        encapsulation vlan-ccc;
        vlan-tags outer 514 inner-range 600-610;
        family ccc {

```

```

        filter {
            input filter_in_ge-0/1/1_514;
        }
    }
}

firewall {
    policer policer_in_ge-0/1/1_514 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family ccc {
        filter filter_in_ge-0/1/1_514 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/1/1_514;
                    accept;
                }
            }
        }
    }
}

protocols {
    l2circuit {
        neighbor 192.168.1.40 {
            interface ge-0/1/1.514 {
                virtual-circuit-id 786;
                no-control-word;
                mtu 1522;
            }
        }
    }
}
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z:

```

ge-0/1/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation vlan-ccc;
    unit 514 {
        description VLANRANGE-SR;
        encapsulation vlan-ccc;
        vlan-tags outer 514 inner-range 600-610;
        family ccc {
            filter {
                input filter_in_ge-0/1/1_514;
            }
        }
    }
}

```

```

    }
  }
}

firewall {
  policer policer_in_ge-0/1/1_514 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
    then discard;
  }
  family ccc {
    filter filter_in_ge-0/1/1_514 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/1/1_514;
          accept;
        }
      }
    }
  }
}

protocols {
  l2circuit {
    neighbor 192.168.1.30 {
      interface ge-0/1/1.514 {
        virtual-circuit-id 786;
        no-control-word;
        mtu 1522;
      }
    }
  }
}

```

ELine-QinQ-VLANRange-Ext-CCC

This service definition provides a base for creating point-to-point services that transport a range of VLANs across an LDP network core using Q-in-Q endpoint interface types and extended-vlan-ccc as the physical encapsulation type. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- [Configuration on Endpoint A on page 488](#)
- [Configuration on Endpoint Z on page 489](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```
ge-0/1/1 {
  flexible-vlan-tagging;
  mtu 1522;
  encapsulation extended-vlan-ccc;
  unit 2 {
    description Ext-VLANRange;
    vlan-tags outer 2 inner-range 100-110;
    family ccc {
      filter {
        input filter_in_ge-0/1/1_2;
      }
    }
  }
}

firewall {
  policer policer_in_ge-0/1/1_2 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
    then discard;
  }
  family ccc {
    filter filter_in_ge-0/1/1_2 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/1/1_2;
          accept;
        }
      }
    }
  }
}

protocols {
  l2circuit {
    neighbor 192.168.1.30 {
      interface ge-0/1/1.2 {
        virtual-circuit-id 786;
        no-control-word;
        mtu 1522;
      }
    }
  }
}
```


Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z:

```

ge-0/1/1 {
  flexible-vlan-tagging;
  mtu 1522;
  encapsulation extended-vlan-ccc;
  unit 2 {
    description Ext-VLANRange;
    vlan-tags outer 2 inner-range 100-110;
    family ccc {
      filter {
        input filter_in_ge-0/1/1_2;
      }
    }
  }
}

firewall {
  policer policer_in_ge-0/1/1_2 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
    then discard;
  }
  family ccc {
    filter filter_in_ge-0/1/1_2 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/1/1_2;
          accept;
        }
      }
    }
  }
}

protocols {
  l2circuit {
    neighbor 192.168.1.30 {
      interface ge-0/1/1.2 {
        virtual-circuit-id 786;
        no-control-word;
        mtu 1522;
      }
    }
  }
}

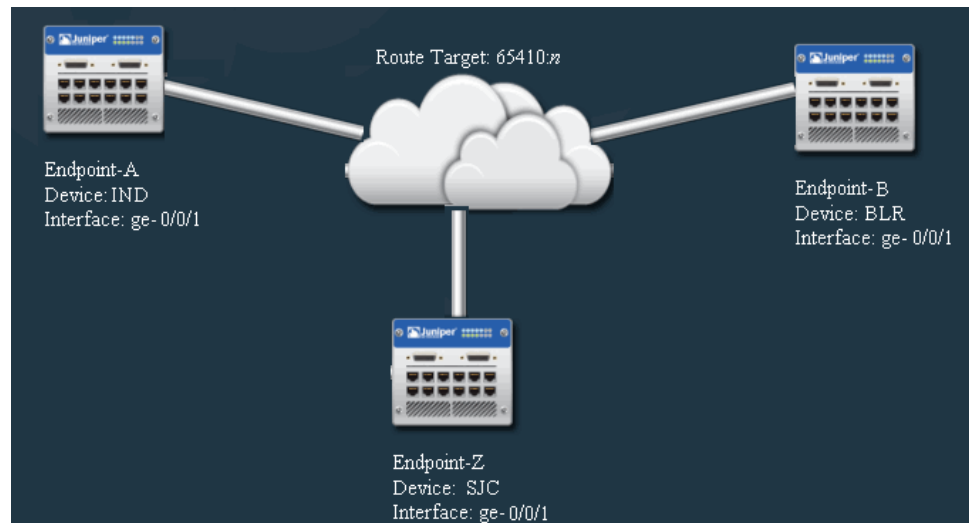
```

Multipoint-to-Multipoint Predefined Service Definitions

The Ethernet Activator software provides predefined service definitions for VPLS services that use BGP switching in the network core. These services are sometimes known as

E-LAN services. This section covers multipoint-to-multipoint (or full mesh) service definitions. [Figure 32 on page 490](#) shows an example of such a service.

Figure 32: Multipoint—to—Multipoint Service



Information specific to each service instance, such as the device name, endpoint name, and customer VLAN ID, is provided in the service order. Attributes that can apply across many service instances are typically defined in the service definition. These attributes include:

- Ethernet option (dot1.q, port-port, qinq)
- Traffic type (single VLAN, VLAN range, all traffic)
- VLAN normalization
- Physical interface encapsulation
- Logical interface encapsulation
- Rate limit range

[Table 66 on page 491](#) lists each of the standard VPLS service definitions. Each standard service definition is then described in detail in the sections that follow.

Table 66: Standard Service Definitions

Standard Service Definition Name	Service Attributes
"ELAN-BGP-Dot1q-Normalized-VLAN-None" on page 492	<ul style="list-style-type: none"> • Multipoint Ethernet service for M Series and MX Series devices • Gigabit Ethernet interfaces • Customer VLAN IDs are not preserved • 802.1Q endpoint interface types • Customer traffic is single VLAN • Flexible-ethernet-services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELAN-BGP-Dot1Q-SingleVLAN" on page 496	<ul style="list-style-type: none"> • Multipoint Ethernet service for M Series or MX Series devices • Gigabit Ethernet interfaces • 802.1Q endpoint interface types • Customer traffic is single VLAN • Flexible-ethernet-services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELAN-BGP-PortBased" on page 499	<ul style="list-style-type: none"> • Multipoint Ethernet service for M series and MX Series devices • Gigabit Ethernet interfaces • Port-based UNIs • Transports all customer traffic • Ethernet VPLS as physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELAN-BGP-QinQ-AllVLAN" on page 502	<ul style="list-style-type: none"> • Multipoint Ethernet service for M Series and MX Series devices • Gigabit Ethernet interfaces • Q-in-Q endpoint interface types • All customer traffic • Flexible-ethernet-services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment

Table 66: Standard Service Definitions (continued)

Standard Service Definition Name	Service Attributes
"ELAN-BGP-QinQ-AllVLAN-Normalized-All" on page 506	<ul style="list-style-type: none"> • Multipoint Ethernet service for M Series and MX Series devices • Gigabit Ethernet interfaces • Customer VLAN IDs preserved • Q-in-Q endpoint interface types • All customer traffic • Flexible-ethernet-services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELAN-BGP-QinQ-AllVLAN-Normalized-None" on page 509	<ul style="list-style-type: none"> • Multipoint Ethernet service for M Series and MX Series devices • Gigabit Ethernet interfaces • Q-in-Q endpoint interface types • VLAN IDs not preserved • All customer traffic • Flexible-ethernet-services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELAN-BGP-QinQ-Range-Normalized-VLAN" on page 512	<ul style="list-style-type: none"> • Multipoint Ethernet service for MX Series devices only • Gigabit Ethernet interfaces • Customer VLAN IDs preserved • Q-in-Q endpoint interface types • Transports specified VLAN range • Flexible Ethernet services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment

ELAN-BGP-Dot1q-Normalized-VLAN-None

This service definition provides a base for creating multipoint-to-multipoint Ethernet services that transport traffic from a single VLAN on an endpoint across a BGP network core using 802.1Q endpoint interface types and flexible-ethernet-services as the physical encapsulation type. VLAN IDs are not preserved across the network—traffic passes from the single VLAN on an endpoint to any VLANs in the broadcast domain. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 32 on page 490](#):

- [Configuration on Endpoint A on page 493](#)
- [Configuration on Endpoint B on page 494](#)
- [Configuration on Endpoint Z on page 495](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A (device IND):

```
ge-0/0/1 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-id 1;
        family vpls {
            filter {
                input filter_in_ge-0/0/1_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/0/1_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family vpls {
        filter filter_in_ge-0/0/1_1 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/0/1_1;
                    accept;
                }
            }
        }
    }
}

routing-instances {
    BestCustomer_ELAN-BGP-Dot1q-Normalized-VLAN-SR {
        instance-type vpls;
        interface ge-0/0/1.1;
        route-distinguisher 65410:1;
        vrf-target target:65410:0;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_2 {
                    site-identifier 2;
                    site-preference primary;
                }
            }
        }
    }
}
```

```

        interface ge-0/0/1.1;
    }
}

```

Configuration on Endpoint B

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint B (device BLR):

```

ge-0/0/1 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-id 1;
        family vpls {
            filter {
                input filter_in_ge-0/0/1_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/0/1_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family vpls {
        filter filter_in_ge-0/0/1_1 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/0/1_1;
                    accept;
                }
            }
        }
    }
}

routing-instances {
    BestCustomer_ELAN-BGP-Dot1q-Normalized-VLAN-SR {
        instance-type vpls;
        interface ge-0/0/1.1;
        route-distinguisher 65410:0;
        vrf-target target:65410:0;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_1 {
                    site-identifier 1;
                    site-preference primary;
                    interface ge-0/0/1.1;
                }
            }
        }
    }
}

```

```

    }
  }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z (device SJC):

SJC:

```

ge-0/0/1 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 1 {
    encapsulation vlan-vpls;
    vlan-id 1;
    family vpls {
      filter {
        input filter_in_ge-0/0/1_1;
      }
    }
  }
}

firewall {
  policer policer_in_ge-0/0/1_1 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
    then discard;
  }
  family vpls {
    filter filter_in_ge-0/0/1_1 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/0/1_1;
          accept;
        }
      }
    }
  }
}

routing-instances {
  BestCustomer_ELAN-BGP-Dot1q-Normalized-VLAN-SR {
    instance-type vpls;
    interface ge-0/0/1.1;
    vlan-id none;
    route-distinguisher 65410:2;
    vrf-target target:65410:0;
    protocols {
      vpls {
        no-tunnel-services;
        site Site_3 {
          site-identifier 3;

```

```

        site-preference primary;
        interface ge-0/0/1.1;
    }
}
}

```

ELAN-BGP-Dot1Q-SingleVLAN

This service definition provides a base for creating multipoint-to-multipoint Ethernet services that transport traffic on a single VLAN across a BGP network core using 802.1Q endpoint interface types and flexible-ethernet-services as the physical encapsulation type. No VLAN mapping is performed—the VLAN ID must be the same on all endpoints. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 32 on page 490](#):

- [Configuration on Endpoint A on page 496](#)
- [Configuration on Endpoint B on page 497](#)
- [Configuration on Endpoint Z on page 498](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A (device IND):

```

ge-0/0/2 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-id 1;
        family vpls {
            filter {
                input filter_in_ge-0/0/2_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/0/2_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }

    filter filter_in_ge-0/0/2_1 {
        interface-specific;
        term 1 {
            then {

```


Configuration on Endpoint B

```

ge-0/0/2 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-id 1;
        family vpls {
            filter {
                input filter_in_ge-0/0/2_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/0/2_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }

    filter filter_in_ge-0/0/2_1 {
        interface-specific;
        term 1 {
            then {
                policer policer_in_ge-0/0/2_1;
                accept;
            }
        }
    }
}

```

```

    }
  }
}

routing-instances {
  BestCustomer_ELAN-BGP-Dot1Q-SingleVLAN-SR {
    instance-type vpls;
    interface ge-0/0/2.1;
    route-distinguisher 65410:3;
    vrf-target target:65410:1;
    protocols {
      vpls {
        no-tunnel-services;
        site Site_1 {
          site-identifier 1;
          site-preference primary;
          interface ge-0/0/2.1;
        }
      }
    }
  }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z (device SJC):

```

ge-0/0/2 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 1 {
    encapsulation vlan-vpls;
    vlan-id 1;
    family vpls {
      filter {
        input filter_in_ge-0/0/2_1;
      }
    }
  }
}

firewall {
  policer policer_in_ge-0/0/2_1 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
    then discard;
  }
  family vpls {
    filter filter_in_ge-0/0/2_1 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/0/2_1;
          accept;
        }
      }
    }
  }
}

```

```

    }
  }
}
routing-instances {
  BestCustomer_ELAN-BGP-Dot1Q-SingleVLAN-SR {
    instance-type vpls;
    interface ge-0/0/2.1;
    route-distinguisher 65410:5;
    vrf-target target:65410:1;
    protocols {
      vpls {
        no-tunnel-services;
        site Site_3 {
          site-identifier 3;
          site-preference primary;
          interface ge-0/0/2.1;
        }
      }
    }
  }
}

```

ELAN-BGP-PortBased

This service definition provides a base for creating multipoint-to-multipoint Ethernet services that transport all traffic on an entire port across a BGP network core using ethernet-vpls as the physical encapsulation type. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 32 on page 490](#):

- [Configuration on Endpoint A on page 499](#)
- [Configuration on Endpoint B on page 500](#)
- [Configuration on Endpoint Z on page 501](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A (device IND):

```

ge-0/1/3 {
  mtu 1522;
  encapsulation ethernet-vpls;
  unit 0 {
    family vpls {
      filter {
        input filter_in_ge-0/1/3;
      }
    }
  }
}

firewall {

```

```

    policer policer_in_ge-0/1/3 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 15220;
        }
        then discard;
    }
    family vpls {
        filter filter_in_ge-0/1/3 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/1/3;
                    accept;
                }
            }
        }
    }
}
routing-instances {
    ELAN_BGP_PortBased_10_100M {
        instance-type vpls;
        interface ge-0/1/3.0;
        route-distinguisher 65410:3;
        vrf-target target:65410:1;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_2 {
                    site-identifier 2;
                    site-preference primary;
                    interface ge-0/1/3.0;
                }
            }
        }
    }
}
}

```

Configuration on Endpoint B

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint B (device BLR):

```

ge-0/1/3 {
    mtu 1522;
    encapsulation ethernet-vpls;
    unit 0 {
        family vpls {
            filter {
                input filter_in_ge-0/1/3;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/3 {

```

```

        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 15220;
        }
        then discard;
    }
    family vpls {
        filter filter_in_ge-0/1/3 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/1/3;
                    accept;
                }
            }
        }
    }
}
routing-instances {
    ELAN_BGP_PortBased_10_100M {
        instance-type vpls;
        interface ge-0/1/3.0;
        route-distinguisher 65410:2;
        vrf-target target:65410:1;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_1 {
                    site-identifier 1;
                    site-preference primary;
                    interface ge-0/1/3.0;
                }
            }
        }
    }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z (device SJC):

```

ge-0/2/2 {
    mtu 1522;
    encapsulation ethernet-vpls;
    unit 0 {
        family vpls {
            filter {
                input filter_in_ge-0/2/2;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/2/2 {
        if-exceeding {

```

```

        bandwidth-limit 100m;
        burst-size-limit 15220;
    }
    then discard;
}
family vpls {
    filter filter_in_ge-0/2/2 {
        interface-specific;
        term 1 {
            then {
                policer policer_in_ge-0/2/2;
                accept;
            }
        }
    }
}
}

routing-instances {
    ELAN_BGP_PortBased_10_100M {
        instance-type vpls;
        interface ge-0/2/2.0;
        route-distinguisher 65410:4;
        vrf-target target:65410:1;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_3 {
                    site-identifier 3;
                    site-preference primary;
                    interface ge-0/2/2.0;
                }
            }
        }
    }
}

```

ELAN-BGP-QinQ-AllVLAN

This service definition provides a base for creating multipoint-to-multipoint Ethernet services that transport all traffic across a BGP network core using Q-in-Q endpoint interface types and flexible-ethernet-services as the physical encapsulation type. No VLAN mapping is performed—customer VLAN IDs and service provider VLAN IDs must match on each endpoint that is to send or receive traffic. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 32 on page 490](#):

- [Configuration on Endpoint A on page 503](#)
- [Configuration on Endpoint B on page 504](#)
- [Configuration on Endpoint Z on page 505](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A (device IND):

```

ge-0/1/1 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-tags outer 1;
        family vpls {
            filter {
                input filter_in_ge-0/1/1_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/1_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family vpls {
        filter filter_in_ge-0/1/1_1 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/1/1_1;
                    accept;
                }
            }
        }
    }
}

routing-instances {
    BestCustomer_ELAN-BGP-QinQ-AllVLAN-SR {
        instance-type vpls;
        interface ge-0/1/1.1;
        route-distinguisher 65410:13;
        vrf-target target:65410:4;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_2 {
                    site-identifier 2;
                    site-preference primary;
                    interface ge-0/1/1.1;
                }
            }
        }
    }
}

```

Configuration on Endpoint B

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint B (device BLR):

```

ge-0/1/1 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-tags outer 1;
        family vpls {
            filter {
                input filter_in_ge-0/1/1_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/1_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family vpls {
        filter filter_in_ge-0/1/1_1 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/1/1_1;
                    accept;
                }
            }
        }
    }
}

routing-instances {
    BestCustomer_ELAN-BGP-QinQ-AllVLAN-SR {
        instance-type vpls;
        interface ge-0/1/1.1;
        route-distinguisher 65410:12;
        vrf-target target:65410:4;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_1 {
                    site-identifier 1;
                    site-preference primary;
                    interface ge-0/1/1.1;
                }
            }
        }
    }
}

```


Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z (device SJC):

```

ge-0/0/5 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-tags outer 1;
        family vpls {
            filter {
                input filter_in_ge-0/0/5_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/0/5_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family vpls {
        filter filter_in_ge-0/0/5_1 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/0/5_1;
                    accept;
                }
            }
        }
    }
}

routing-instances {
    BestCustomer_ELAN-BGP-QinQ-AllVLAN-SR {
        instance-type vpls;
        interface ge-0/0/5.1;
        route-distinguisher 65410:14;
        vrf-target target:65410:4;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_3 {
                    site-identifier 3;
                    site-preference primary;
                    interface ge-0/0/5.1;
                }
            }
        }
    }
}

```

ELAN-BGP-QinQ-AllVLAN-Normalized-All

This service definition provides a base for creating multipoint-to-multipoint Ethernet services that transport all traffic across a BGP network core using Q-in-Q endpoint interface types and flexible-ethernet-services as the physical encapsulation type. Customer VLAN IDs are preserved across the network—traffic passes only among matching customer VLAN IDs. However, traffic can pass among any service provider VLAN ID in the broadcast domain. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 32 on page 490](#):

- [Configuration on Endpoint A on page 506](#)
- [Configuration on Endpoint B on page 507](#)
- [Configuration on Endpoint Z on page 508](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A (device IND):

```
ge-0/1/0 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-tags outer 1;
        family vpls {
            filter {
                input filter_in_ge-0/1/0_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/0_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family vpls {
        filter filter_in_ge-0/1/0_1 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/1/0_1;
                    accept;
                }
            }
        }
    }
}
```

```

routing-instances {
  BestCustomer_ELAN-BGP-QinQ-AllVLAN-Normalized-All-SR {
    instance-type vpls;
    interface ge-0/1/0.1;
    route-distinguisher 65410:10;
    vrf-target target:65410:3;
    protocols {
      vpls {
        no-tunnel-services;
        site Site_2 {
          site-identifier 2;
          site-preference primary;
          interface ge-0/1/0.1;
        }
      }
    }
  }
}

```

Configuration on Endpoint B

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint B (device BLR):

```

ge-0/1/0 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 1 {
    encapsulation vlan-vpls;
    vlan-tags outer 1;
    family vpls {
      filter {
        input filter_in_ge-0/1/0_1;
      }
    }
  }
}

firewall {
  policer policer_in_ge-0/1/0_1 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
    then discard;
  }
  family vpls {
    filter filter_in_ge-0/1/0_1 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/1/0_1;
          accept;
        }
      }
    }
  }
}

routing-instances {

```

```

BestCustomer_ELAN-BGP-QinQ-AllVLAN-Normalized-All-SR {
  instance-type vpls;
  interface ge-0/1/0.1;
  route-distinguisher 65410:9;
  vrf-target target:65410:3;
  protocols {
    vpls {
      no-tunnel-services;
      site Site_1 {
        site-identifier 1;
        site-preference primary;
        interface ge-0/1/0.1;
      }
    }
  }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z (device SJC):

```

ge-0/0/4 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 1 {
    encapsulation vlan-vpls;
    vlan-tags outer 1;
    family vpls {
      filter {
        input filter_in_ge-0/0/4_1;
      }
    }
  }
}
firewall {
  policer policer_in_ge-0/0/4_1 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
    then discard;
  }
  family vpls {
    filter filter_in_ge-0/0/4_1 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/0/4_1;
          accept;
        }
      }
    }
  }
}
routing-instances {
  BestCustomer_ELAN-BGP-QinQ-AllVLAN-Normalized-All-SR {
    instance-type vpls;
  }
}

```

```

interface ge-0/0/4.1;
vlan-id all;
route-distinguisher 65410:11;
vrf-target target:65410:3;
protocols {
  vpls {
    no-tunnel-services;
    site Site_3 {
      site-identifier 3;
      site-preference primary;
      interface ge-0/0/4.1;
    }
  }
}

```

ELAN-BGP-QinQ-AllVLAN-Normalized-None

This service definition provides a base for creating multipoint-to-multipoint Ethernet services that transport all traffic across a BGP network core using Q-in-Q endpoint interface types and flexible-ethernet-services as the physical encapsulation type. VLAN IDs are not preserved across the network—traffic passes between any customer VLAN or service provider VLAN in the broadcast domain. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 32 on page 490](#):

- [Configuration on Endpoint A on page 509](#)
- [Configuration on Endpoint B on page 510](#)
- [Configuration on Endpoint Z on page 511](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A (device IND):

```

ge-0/0/3 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 1 {
    encapsulation vlan-vpls;
    vlan-tags outer 1;
    family vpls {
      filter {
        input filter_in_ge-0/0/3_1;
      }
    }
  }
}

firewall {
  policer policer_in_ge-0/0/3_1 {
    if-exceeding {

```

```

        bandwidth-limit 100m;
        burst-size-limit 62500000;
    }
    then discard;
}
family vpls {
    filter filter_in_ge-0/0/3_1 {
        interface-specific;
        term 1 {
            then {
                policer policer_in_ge-0/0/3_1;
                accept;
            }
        }
    }
}
}
}
routing-instances {
    BestCustomer_ELAN-BGP-QinQ-AllVLAN-Normalized-SR {
        instance-type vpls;
        interface ge-0/0/3.1;
        route-distinguisher 65410:7;
        vrf-target target:65410:2;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_2 {
                    site-identifier 2;
                    site-preference primary;
                    interface ge-0/0/3.1;
                }
            }
        }
    }
}
}
}

```

Configuration on Endpoint B

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint B (device BLR):

```

ge-0/0/3 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-tags outer 1;
        family vpls {
            filter {
                input filter_in_ge-0/0/3_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/0/3_1 {
        if-exceeding {

```

```

        bandwidth-limit 100m;
        burst-size-limit 62500000;
    }
    then discard;
}
family vpls {
    filter filter_in_ge-0/0/3_1 {
        interface-specific;
        term 1 {
            then {
                policer policer_in_ge-0/0/3_1;
                accept;
            }
        }
    }
}
}
}
routing-instances {
    BestCustomer_ELAN-BGP-QinQ-AllVLAN-Normalized-SR {
        instance-type vpls;
        interface ge-0/0/3.1;
        route-distinguisher 65410:6;
        vrf-target target:65410:2;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_1 {
                    site-identifier 1;
                    site-preference primary;
                    interface ge-0/0/3.1;
                }
            }
        }
    }
}
}
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z (device SJC):

```

ge-0/0/3 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-tags outer 1;
        family vpls {
            filter {
                input filter_in_ge-0/0/3_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/0/3_1 {
        if-exceeding {

```

```

        bandwidth-limit 100m;
        burst-size-limit 62500000;
    }
    then discard;
}
family vpls {
    filter filter_in_ge-0/0/3_1 {
        interface-specific;
        term 1 {
            then {
                policer policer_in_ge-0/0/3_1;
                accept;
            }
        }
    }
}
}
routing-instances {
    BestCustomer_ELAN-BGP-QinQ-AllVLAN-Normalized-SR {
        instance-type vpls;
        interface ge-0/0/3.1;
        vlan-id none;
        route-distinguisher 65410:8;
        vrf-target target:65410:2;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_3 {
                    site-identifier 3;
                    site-preference primary;
                    interface ge-0/0/3.1;
                }
            }
        }
    }
}
}

```

ELAN-BGP-QinQ-Range-Normalized-VLAN

This service definition provides a base for creating multipoint-to-multipoint Ethernet services that transport traffic from a range of VLANs on an endpoint across a BGP network core using Q-in-Q endpoint interface types and flexible-ethernet-services as the physical encapsulation type. Services built from this service definition must use MX Series devices on the provider edge. Customer VLAN IDs are preserved across the network—traffic passes among like customer VLAN IDs on any service provider VLAN in the broadcast domain. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data for a service with only two endpoints, SJC and SFO.

- [Configuration on Endpoint A on page 513](#)
- [Configuration on Endpoint Z on page 514](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A (device SJC):

```

ge-0/0/6 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation flexible-ethernet-services;
    unit 2 {
        encapsulation vlan-vpls;
        vlan-tags outer 2 inner-range 1500-2000;
        family vpls {
            filter {
                input filter_in_ge-0/0/6_2;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/0/6_2 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family vpls {
        filter filter_in_ge-0/0/6_2 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/0/6_2;
                    accept;
                }
            }
        }
    }
}

routing-instances {
    BestCustomer_ELAN-BGP-QinQ-Range-Normalized-VLAN-SR1 {
        instance-type vpls;
        vlan-id all;
        interface ge-0/0/6.2;
        vlan-id all;
        route-distinguisher 65410:19;
        vrf-target target:65410:6;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_2 {
                    site-identifier 2;
                    site-preference primary;
                    interface ge-0/0/6.2;
                }
            }
        }
    }
}

```

```

    }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z (device SFO):

```

ge-0/0/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-tags outer 1 inner-range 1500-2000;
        family vpls {
            filter {
                input filter_in_ge-0/0/1_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/0/1_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family vpls {
        filter filter_in_ge-0/0/1_1 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/0/1_1;
                    accept;
                }
            }
        }
    }
}

routing-instances {
    BestCustomer_ELAN-BGP-QinQ-Range-Normalized-VLAN-SR1 {
        instance-type vpls;
        vlan-id all;
        interface ge-0/0/1.1;
        route-distinguisher 65410:18;
        vrf-target target:65410:6;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_1 {
                    site-identifier 1;
                    site-preference primary;
                    interface ge-0/0/1.1;
                }
            }
        }
    }
}

```

```

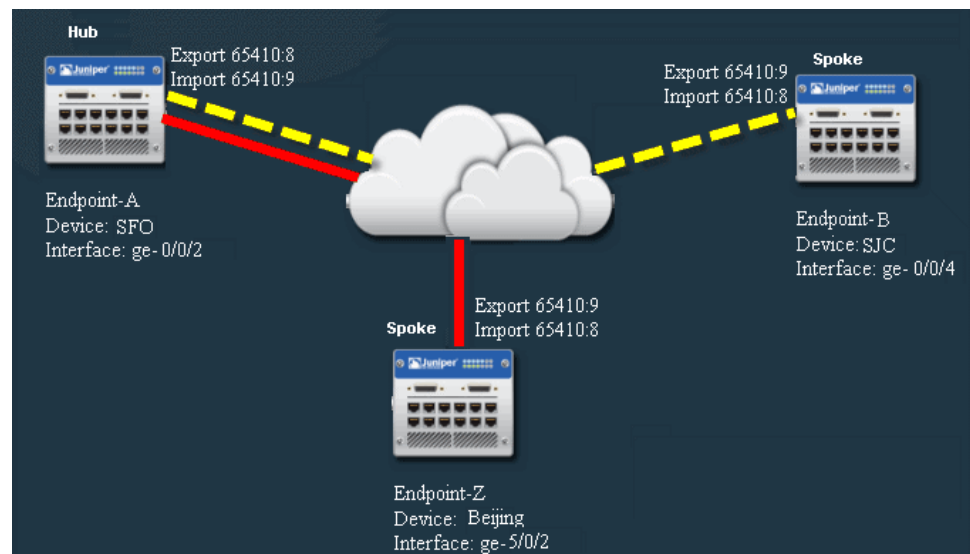
    }
  }
}

```

Point-to-Multipoint Service Definitions

The Ethernet Activator software provides predefined service definitions for VPLS services that use BGP switching in the network core. These services are sometimes known as E-LAN services. This section covers point-to-multipoint (or hub and spoke) service definitions. [Figure 33 on page 515](#) shows an example of such a service.

Figure 33: Point-to-Multipoint Service



Information specific to each service instance, such as the device name, endpoint name, customer VLAN ID, and whether a specific endpoint is a hub or a spoke is provided in the service order. Attributes that can apply across many service instances are typically defined in the service definition. These attributes include:

- Ethernet option (dot1.q, port-port, qinq)
- Traffic type (single VLAN, VLAN range, all traffic)
- VLAN normalization
- Physical interface encapsulation
- Logical interface encapsulation
- Rate limit range

[Table 67 on page 516](#) lists each of the standard VPLS service definitions. Each standard service definition is then described in detail in the sections that follow.

Table 67: Standard Service Definitions

Standard Service Definition Name	Service Attributes
"ELAN-Hub-Spoke-QinQ-AllVLAN" on page 516	<ul style="list-style-type: none"> • Multipoint Ethernet service for M Series and MX Series devices • Gigabit Ethernet interfaces • Customer VLAN IDs are not preserved • Q-in-Q endpoint interface types • All customer traffic • Flexible-ethernet-services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELAN-Hub-Spoke-QinQ-AllVLAN-No" on page 517	<ul style="list-style-type: none"> • Multipoint Ethernet service for M Series or MX Series devices • Gigabit Ethernet interfaces • Customer VLAN IDs are preserved • Q-in-Q endpoint interface types • All customer traffic • Flexible-ethernet-services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment

ELAN-Hub-Spoke-QinQ-AllVLAN

This service definition provides a base for creating point-to-multipoint Ethernet services that transport all traffic on an endpoint across a BGP network core using Q-in-Q endpoint interface types and flexible-ethernet-services as the physical encapsulation type. Customer VLAN IDs are preserved across the network—traffic passes among like customer VLAN IDs on any service provider VLAN in the broadcast domain. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 33 on page 515](#):

- [Configuration on Endpoint A on page 516](#)
- [Configuration on Endpoint B on page 516](#)
- [Configuration on Endpoint Z on page 517](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A (device IND):

Configuration on Endpoint B

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint B (device BLR):

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z (device SJC):

ELAN-Hub-Spoke-QinQ-AllVLAN-No

This service definition provides a base for creating point-to-multipoint Ethernet services that transport all traffic on an endpoint across a BGP network core using Q-in-Q endpoint interface types and flexible-ethernet-services as the physical encapsulation type. VLAN IDs are not preserved across the network—traffic passes from the single VLAN on an endpoint to any VLANs in the broadcast domain. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 33 on page 515](#):

- [Configuration on Endpoint A on page 517](#)
- [Configuration on Endpoint B on page 517](#)
- [Configuration on Endpoint Z on page 517](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A (device IND):

Configuration on Endpoint B

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint B (device BLR):

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z (device SJC):

Related Documentation

- [Creating a Point-to-Point Ethernet Service Definition on page 625](#)
- [Creating a Multipoint-to-Multipoint VPLS Service Definition on page 653](#)

Predefined Point-to-Point Service Definitions

The Connectivity Services Director application provides predefined service definitions that a service provisioner can choose from when creating a service order. This section provides information about predefined service definitions used for creating Ethernet point-to-point services. For information about predefined service definitions used to create other types of service, see the following topics:

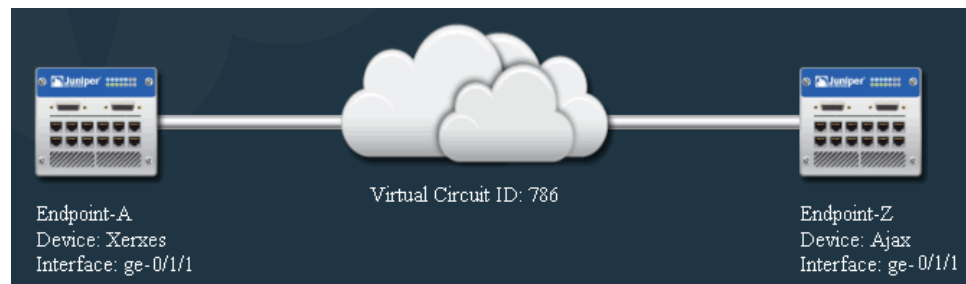
- [Predefined Multipoint-to-Multipoint Ethernet Service Definitions on page 551](#)
- [Predefined Point-to-Multipoint Ethernet Service Definitions on page 576](#)

- [Predefined Full Mesh Layer 3 VPN Service Definitions on page 589](#)
- [Predefined Hub-and-Spoke Layer 3 VPN Service Definitions on page 590](#)

If none of the point-to-point predefined service definitions described here is appropriate for your needs, you can create a service definition as described in [“Creating a Point-to-Point Ethernet Service Definition” on page 625](#),

The Connectivity Services Director application provides predefined service definitions for Ethernet point-to-point services that use LDP switching or BGP in the network core. The LDP based services are sometimes known as E-Line Martini services, and the BGP based services are sometimes known as E-Line Kompella services. [Figure 31 on page 466](#) shows an example of such a service.

Figure 34: Point-to-Point Service



Information specific to each service instance, such as the device name, endpoint name, and customer VLAN ID, is provided in the service order. Attributes that can apply across many service instances are typically defined in the service definition. These attributes include:

- Ethernet option (dot1.q, port-port, qinq)
- Traffic type (single VLAN, multiple VLAN, all traffic)
- Physical interface encapsulation
- Logical interface encapsulation
- Rate limit range

[Table 65 on page 466](#) lists each of the standard point-to-point service definitions. Each standard service definition is then described in detail in the sections that follow.

Table 68: Standard Ethernet Point-to-Point Ethernet Service Definitions

Standard Service Definition Name	Service Attributes
"ELine-Dot1q-SingleVLAN" on page 468	<ul style="list-style-type: none"> Point-to-point service for M Series and MX Series routers Gigabit Ethernet interfaces 802.1Q endpoint interface types Customer traffic is single VLAN Flexible-ethernet-services physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELine-Dot1q-SingleVLAN-CCC" on page 470	<ul style="list-style-type: none"> Point-to-point service for M Series and MX Series routers Gigabit Ethernet interfaces 802.1Q endpoint interface types Customer traffic is single VLAN Vlan-ccc physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELine-Dot1q-SingleVLAN-Ext-CCC" on page 472	<ul style="list-style-type: none"> Point-to-point service for M Series and MX Series routers Gigabit Ethernet interfaces 802.1Q endpoint interface types Customer traffic is single VLAN Extended-vlan-ccc physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELine-PortBased" on page 474	<ul style="list-style-type: none"> Point-to-point service for M Series and MX Series routers Gigabit Ethernet interfaces Port-based UNI Ethernet-ccc physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELine-QinQ-AllVLAN" on page 476	<ul style="list-style-type: none"> Point-to-point service for M Series and MX Series routers Gigabit Ethernet interfaces Q-in-Q endpoint interface types All customer traffic Flexible-ethernet-services physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment

Table 68: Standard Ethernet Point-to-Point Ethernet Service Definitions (continued)

Standard Service Definition Name	Service Attributes
"ELine-QinQ-AllVLAN-CCC" on page 479	<ul style="list-style-type: none"> Point-to-point service for M Series and MX Series routers Gigabit Ethernet interfaces Q-in-Q endpoint interface types All customer traffic Vlan-ccc physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELine-QinQ-AllVLAN-Ext-CCC" on page 481	<ul style="list-style-type: none"> Point-to-point service for M Series and MX Series routers Gigabit Ethernet interfaces Q-in-Q endpoint interface types All customer traffic Extended-vlan-ccc physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELine-QinQ-VLANRange" on page 483	<ul style="list-style-type: none"> Point-to-point service for MX Series routers only Gigabit Ethernet interfaces Q-in-Q endpoint interface types Customer traffic is range of VLANs Flexible-ethernet-services physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELine-QinQ-VLANRange-CCC" on page 485	<ul style="list-style-type: none"> Point-to-point service for MX Series routers only Gigabit Ethernet interfaces Q-in-Q endpoint interface types Customer traffic is range of VLANs Vlan-ccc physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELine-QinQ-VLANRange-Ext-CCC" on page 487	<ul style="list-style-type: none"> Point-to-point service for MX Series routers only Gigabit Ethernet interfaces Q-in-Q endpoint interface types Customer traffic is range of VLANs Extended-vlan-ccc physical encapsulation Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
TDM Interface	<ul style="list-style-type: none"> Point-to-point service for MX Series routers only T1 interfaces satop physical encapsulation

Table 68: Standard Ethernet Point-to-Point Ethernet Service Definitions (continued)

Standard Service Definition Name	Service Attributes
Static TDM pseudowire	<ul style="list-style-type: none"> Point-to-point service for MX Series routers only T1 interfaces satop physical encapsulation Static pseudowire
ATM pseudowire	<ul style="list-style-type: none"> Point-to-point service for MX Series routers only ATM/T1 interfaces atm-ccc-cell-relay physical encapsulation
ATM-AAL5 pseudowire	<ul style="list-style-type: none"> Point-to-point service for MX Series routers only ATM/T1 interfaces atm-ccc-vc-mux/aal5 physical encapsulation
Static ATM pseudowire	<ul style="list-style-type: none"> Point-to-point service for MX Series routers only ATM/T1 interfaces atm-ccc-cell-relay/atm physical encapsulation Static pseudowire
Static ATM-AAL5 pseudowire	<ul style="list-style-type: none"> Point-to-point service for MX Series routers only ATM/T1 interfaces atm-ccc-vc-mux / aal5 physical encapsulation Static pseudowire
"Eline-BGP-QinQ-AllVLAN" on page 548	<ul style="list-style-type: none"> Ethernet service for M Series, MX Series, and ACX Series routers Gigabit Ethernet interface Q-in-Q endpoint interface type Transport all traffic Flexible-ethernet-services physical encapsulation type Rate limit from 10 Mbps to 100 Mbps with 10 Mbps increment
"Eline-BGP-Dot1q-SingleVLAN" on page 546	<ul style="list-style-type: none"> Ethernet service for M Series, MX Series, and ACX Series routers Gigabit Ethernet interface 802.1Q endpoint interface types Single VLAN traffic Flexible-ethernet-services physical encapsulation type Rate limit from 10 Mbps to 100 Mbps with 10 Mbps increment

Table 68: Standard Ethernet Point-to-Point Ethernet Service Definitions (continued)

Standard Service Definition Name	Service Attributes
"ELine-BGP-Port-Based" on page 543	<ul style="list-style-type: none"> Ethernet service for M Series, MX Series, and ACX routers Gigabit Ethernet interface Port-based UNIs Ethernet-ccc physical encapsulation type Rate limit from 10 Mbps to 100 Mbps with 10 Mbps increment

ELine-Dot1q-SingleVLAN Service Definition

This service definition provides a base for creating point-to-point services that transport a single VLAN across an LDP or BGP network core using 802.1Q endpoint interface types and flexible-ethernet-services as the physical encapsulation type. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- [Configuration on Endpoint A on page 522](#)
- [Configuration on Endpoint Z on page 523](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```

ge-0/1/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation flexible-ethernet-services;
    unit 1 {
        description "Dot1q Eline Martini ";
        encapsulation vlan-ccc;
        vlan-id 1;
        family ccc {
            filter {
                input filter_in_ge-0/1/1_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/1_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
}

```

```

family ccc {
  filter filter_in_ge-0/1/1_1 {
    interface-specific;
    term 1 {
      then {
        policer policer_in_ge-0/1/1_1;
        accept;
      }
    }
  }
}

protocols {
  l2circuit {
    neighbor 192.168.1.40
    interface ge-0/1/1.1 {
      virtual-circuit-id 786;
      no-control-word;
      mtu 1522;
    }
  }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z:

```

ge-0/1/1 {
  flexible-vlan-tagging;
  mtu 1522;
  encapsulation flexible-ethernet-services;
  unit 1 {
    description "Dot1q Eline Martini ";
    encapsulation vlan-ccc;
    vlan-id 1;
    family ccc {
      filter {
        input filter_in_ge-0/1/1_1;
      }
    }
  }
}

firewall {
  policer policer_in_ge-0/1/1_1 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
    then discard;
  }
}

family ccc {
  filter filter_in_ge-0/1/1_1 {
    interface-specific;
    term 1 {
      then {
        policer policer_in_ge-0/1/1_1;

```

```

        accept;
    }

    protocols {
        l2circuit {
            neighbor 192.168.1.30 {
                interface ge-0/1/1.1 {
                    virtual-circuit-id 786;
                    no-control-word;
                    mtu 1522;
                }
            }
        }
    }
}

```

ELine-Dot1q-SingleVLAN-CCC Service Definition

This service definition provides a base for creating point-to-point services that transport a single VLAN across an LDP or BGP network core using 802.1Q endpoint interface types and vlan-ccc as the physical encapsulation type. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- [Configuration on Endpoint A on page 524](#)
- [Configuration on Endpoint Z on page 525](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```

ge-0/1/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation vlan-ccc;
    unit 513 {
        description VLANCCC-SR;
        encapsulation vlan-ccc;
        vlan-id 513;
        family ccc {
            filter {
                input filter_in_ge-0/1/1_513;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/1_513 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
}

```

```

    }
    family ccc {
        filter filter_in_ge-0/1/1_513 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/1/1_513;
                    accept;
                }
            }
        }
    }
}

protocols {
    l2circuit {
        neighbor 192.168.1.40 {
            interface ge-0/1/1.513 {
                virtual-circuit-id 786;
                no-control-word;
                mtu 1522;
            }
        }
    }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z:

```

ge-0/1/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation vlan-ccc;
    unit 513 {
        description VLANCCC-SR;
        encapsulation vlan-ccc;
        vlan-id 513;
        family ccc {
            filter {
                input filter_in_ge-0/1/1_513;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/1_513 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family ccc {
        filter filter_in_ge-0/1/1_513 {

```

```

        interface-specific;
        term 1 {
            then {
                policer policer_in_ge-0/1/1_513;
                accept;
            }
        }
    }
}

protocols {
    l2circuit {
        neighbor 192.168.1.30 {
            interface ge-0/1/1.513 {
                virtual-circuit-id 786;
                no-control-word;
                mtu 1522;
            }
        }
    }
}

```

ELine-Dot1q-SingleVLAN-Ext-CCC Service Definition

This service definition provides a base for creating point-to-point services that transport a single VLAN across an LDP or BGP network core using 802.1Q endpoint interface types and extended-vlan-ccc as the physical encapsulation type. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- [Configuration on Endpoint A on page 526](#)
- [Configuration on Endpoint Z on page 527](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```

ge-0/1/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation extended-vlan-ccc;
    unit 1 {
        description Extended-SR;
        vlan-id 1;
        family ccc {
            filter {
                input filter_in_ge-0/1/1_1;
            }
        }
    }
}

```

```

firewall {
  policer policer_in_ge-0/1/1_1 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
    then discard;
  }
  family ccc {
    filter filter_in_ge-0/1/1_1 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/1/1_1;
          accept;
        }
      }
    }
  }
}

protocols {
  l2circuit {
    neighbor 192.168.1.40 {
      interface ge-0/1/1.1 {
        virtual-circuit-id 786;
        no-control-word;
        mtu 1522;
      }
    }
  }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z:

```

ge-0/1/1 {
  flexible-vlan-tagging;
  mtu 1522;
  encapsulation extended-vlan-ccc;
  unit 1 {
    description Extended-SR;
    vlan-id 1;
    family ccc {
      filter {
        input filter_in_ge-0/1/1_1;
      }
    }
  }
}

firewall {
  policer policer_in_ge-0/1/1_1 {
    if-exceeding {

```

```

        bandwidth-limit 100m;
        burst-size-limit 62500000;
    }
    then discard;
}
family ccc {
    filter filter_in_ge-0/1/1_1 {
        interface-specific;
        term 1 {
            then {
                policer policer_in_ge-0/1/1_1;
                accept;
            }
        }
    }
}
}

protocols {
    l2circuit {
        neighbor 192.168.1.30 {
            interface ge-0/1/1.1 {
                virtual-circuit-id 786;
                no-control-word;
                mtu 1522;
            }
        }
    }
}
}

```

ELine-PortBased Service Definition

This service definition provides a base for creating point-to-point services that transport all traffic across an LDP or BGP network core using an entire port at each endpoint using ethernet-ccc as the physical encapsulation type. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps to 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- [Configuration on Endpoint A on page 528](#)
- [Configuration on Endpoint Z on page 529](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```

ge-0/1/1 {
    encapsulation ethernet-ccc;
    unit 0 {
        family ccc {
            filter {
                input filter_in_ge-0/1/1;
            }
        }
    }
}

```



```

    }
  }
}

firewall {
  policer policer_in_ge-0/1/1 {
    if-exceeding {
      bandwidth-limit 10m;
      burst-size-limit 6250000;
    }
    then discard;
  }
  family ccc {
    filter filter_in_ge-0/1/1 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/1/1;
          accept;
        }
      }
    }
  }
}

protocols {
  l2circuit {
    neighbor 192.168.1.40 {
      interface ge-0/1/1.0 {
        virtual-circuit-id 786;
        no-control-word;
        mtu 1522;
      }
    }
  }
}
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z:

```

ge-0/1/1 {
  encapsulation ethernet-ccc;
  unit 0 {
    family ccc {
      filter {
        input filter_in_ge-0/1/1;
      }
    }
  }
}

firewall {
  policer policer_in_ge-0/1/1 {
    if-exceeding {
      bandwidth-limit 10m;

```

```

        burst-size-limit 6250000;
    }
    then discard;
}
family ccc {
    filter filter_in_ge-0/1/1 {
        interface-specific;
        term 1 {
            then {
                policer policer_in_ge-0/1/1;
                accept;
            }
        }
    }
}
}

protocols {
    l2circuit {
        neighbor 192.168.1.30 {
            interface ge-0/1/1.0 {
                virtual-circuit-id 786;
                no-control-word;
                mtu 1522;
            }
        }
    }
}
}

```

ELine-QinQ-AllVLAN Service Definition

This service definition provides a base for creating point-to-point services that transport all customer traffic across an LDP or BGP network core using Q-in-Q endpoint interface types and flexible-ethernet-services as the physical encapsulation type. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- [Configuration on Endpoint A on page 530](#)
- [Configuration on Endpoint Z on page 531](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```

ge-0/1/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation flexible-ethernet-services;
    unit 1 {
        description "AllVlanTransport";
        encapsulation vlan-ccc;
        vlan-tags outer 1;
    }
}

```

```

        family ccc {
            filter {
                input filter_in_ge-0/1/1_1;
            }
        }
    }

protocols {
    l2circuit {
        neighbor 192.168.1.40 {
            interface ge-0/1/1.1 {
                virtual-circuit-id 786;
                no-control-word;
                mtu 1522;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/1_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family ccc {
        filter filter_in_ge-0/1/1_1 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/1/1_1;
                    accept;
                }
            }
        }
    }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z:

```

ge-0/1/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation flexible-ethernet-services;
    unit 1 {
        description "AllVlanTransport";
        encapsulation vlan-ccc;
        vlan-tags outer 1;
        family ccc {
            filter {
                input filter_in_ge-0/1/1_1;
            }
        }
    }
}

```

```

}

firewall {
  policer policer_in_ge-0/1/1_1 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
    then discard;
  }
  family ccc {
    filter filter_in_ge-0/1/1_1 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/1/1_1;
          accept;
        }
      }
    }
  }
}

protocols {
  l2circuit {
    neighbor 192.168.1.30 {
      interface ge-0/1/1.1 {
        virtual-circuit-id 786;
        no-control-word;
        mtu 1522;
      }
    }
  }
}

```

ELine-QinQ-AllVLAN-CCC Service Definition

This service definition provides a base for creating point-to-point services that transport all customer traffic across an LDP or BGP network core using Q-in-Q endpoint interface types and vlan-ccc as the physical encapsulation type. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- [Configuration on Endpoint A on page 533](#)
- [Configuration on Endpoint Z on page 534](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```

ge-0/1/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation vlan-ccc;
    unit 515 {
        description QinQ-ALLVLAN;
        encapsulation vlan-ccc;
        vlan-tags outer 515;
        family ccc {
            filter {
                input filter_in_ge-0/1/1_515;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/1_515 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }

    family ccc {
        filter filter_in_ge-0/1/1_515 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/1/1_515;
                    accept;
                }
            }
        }
    }
}

protocols {
    l2circuit {
        neighbor 192.168.1.40 {
            interface ge-0/1/1.515 {
                virtual-circuit-id 786;
                no-control-word;
                mtu 1522;
            }
        }
    }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z:

```

ge-0/1/1 {
  flexible-vlan-tagging;
  mtu 1522;
  encapsulation vlan-ccc;
  unit 515 {
    description QinQ-ALLVLAN;
    encapsulation vlan-ccc;
    vlan-tags outer 515;
    family ccc {
      filter {
        input filter_in_ge-0/1/1_515;
      }
    }
  }
}

firewall {
  policer policer_in_ge-0/1/1_515 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
    then discard;
  }
  family ccc {
    filter filter_in_ge-0/1/1_515 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/1/1_515;
          accept;
        }
      }
    }
  }
}

protocols {
  l2circuit {
    neighbor 192.168.1.30 {
      interface ge-0/1/1.515 {
        virtual-circuit-id 786;
        no-control-word;
        mtu 1522;
      }
    }
  }
}

```

ELine-QinQ-AllVLAN-Ext-CCC Service Definition

This service definition provides a base for creating point-to-point services that transport all customer traffic across an LDP or BGP network core using Q-in-Q endpoint interface types and extended-vlan-ccc as the physical encapsulation type. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- [Configuration on Endpoint A on page 535](#)
- [Configuration on Endpoint Z on page 536](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```
ge-0/1/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation extended-vlan-ccc;
    unit 1 {
        description Ext-AllVLAN;
        vlan-tags outer 1;
        family ccc {
            filter {
                input filter_in_ge-0/1/1_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/1_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family ccc {
        filter filter_in_ge-0/1/1_1 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/1/1_1;
                    accept;
                }
            }
        }
    }
}
```

```

protocols {
  l2circuit {
    neighbor 192.168.1.40 {
      interface ge-0/1/1.1 {
        virtual-circuit-id 786;
        no-control-word;
        mtu 1522;
      }
    }
  }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z:

```

ge-0/1/1 {
  flexible-vlan-tagging;
  mtu 1522;
  encapsulation extended-vlan-ccc;
  unit 1 {
    description Ext-AllVLAN;
    vlan-tags outer 1;
    family ccc {
      filter {
        input filter_in_ge-0/1/1_1;
      }
    }
  }
}

firewall {
  policer policer_in_ge-0/1/1_1 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
    then discard;
  }
  family ccc {
    filter filter_in_ge-0/1/1_1 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/1/1_1;
          accept;
        }
      }
    }
  }
}

protocols {

```



```

12circuit {
  neighbor 192.168.1.30 {
    interface ge-0/1/1.1 {
      virtual-circuit-id 786;
      no-control-word;
      mtu 1522;
    }
  }
}

```

ELine-QinQ-VLANRange Service Definition

This service definition provides a base for creating point-to-point services that transport a range of VLANs across an LDP or BGP network core using Q-in-Q endpoint interface types and flexible-ethernet-services as the physical encapsulation type. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- [Configuration on Endpoint A on page 537](#)
- [Configuration on Endpoint Z on page 538](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```

ge-0/1/1 {
  flexible-vlan-tagging;
  mtu 1522;
  encapsulation flexible-ethernet-services;
  unit 2 {
    description "QinQ Eline Martini";
    encapsulation vlan-ccc;
    vlan-tags outer 2 inner-range 100-110;
    family ccc {
      filter {
        input filter_in_ge-0/1/1_2;
      }
    }
  }
}

firewall {
  policer policer_in_ge-0/1/1_2 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
  }
}

family ccc {
  filter filter_in_ge-0/1/1_2 {

```

```

        interface-specific;
        term 1 {
            then {
                policer policer_in_ge-0/1/1_2;
                accept;
            }
        }
    protocols {
        l2circuit {
            neighbor 192.168.1.40 {
                interface ge-0/1/1.2 {
                    virtual-circuit-id 786;
                    no-control-word;
                    mtu 1522;
                }
            }
        }
    }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z:

```

ge-0/1/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation flexible-ethernet-services;
    unit 2 {
        description "QinQ Eline Martini";
        encapsulation vlan-ccc;
        vlan-tags outer 2 inner-range 100-110;
        family ccc {
            filter {
                input filter_in_ge-0/1/1_2;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/1_2 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }

    family ccc {
        filter filter_in_ge-0/1/1_2 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/1/1_2;
                }
            }
        }
    }
}

```

```
    accept;
  }
}

protocols {
  l2circuit {
    interface ge-0/1/1.2 {
      virtual-circuit-id 786;
      no-control-word;
      mtu 1522;
    }
  }
}
```

ELine-QinQ-VLANRange-CCC Service Definition

This service definition provides a base for creating point-to-point services that transport a range of VLANs across an LDP or BGP network core using Q-in-Q endpoint interface types and vlan-ccc as the physical encapsulation type. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- Configuration on Endpoint A on page 539
- Configuration on Endpoint Z on page 540

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```

ge-0/1/1 {
  flexible-vlan-tagging;
  mtu 1522;
  encapsulation vlan-ccc;
  unit 514 {
    description VLANRANGE-SR;
    encapsulation vlan-ccc;
    vlan-tags outer 514 inner-range 600-610;
    family ccc {
      filter {
        input filter_in_ge-0/1/1_514;
      }
    }
  }
}

firewall {
  policer policer_in_ge-0/1/1_514 {

```

```

        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family ccc {
        filter filter_in_ge-0/1/1_514 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/1/1_514;
                    accept;
                }
            }
        }
    }
}

protocols {
    l2circuit {
        neighbor 192.168.1.40 {
            interface ge-0/1/1.514 {
                virtual-circuit-id 786;
                no-control-word;
                mtu 1522;
            }
        }
    }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z:

```

ge-0/1/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation vlan-ccc;
    unit 514 {
        description VLANRANGE-SR;
        encapsulation vlan-ccc;
        vlan-tags outer 514 inner-range 600-610;
        family ccc {
            filter {
                input filter_in_ge-0/1/1_514;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/1_514 {
        if-exceeding {
            bandwidth-limit 100m;

```

```

        burst-size-limit 62500000;
    }
    then discard;
}
family ccc {
    filter filter_in_ge-0/1/1_514 {
        interface-specific;
        term 1 {
            then {
                policer policer_in_ge-0/1/1_514;
                accept;
            }
        }
    }
}

protocols {
    l2circuit {
        neighbor 192.168.1.30 {
            interface ge-0/1/1.514 {
                virtual-circuit-id 786;
                no-control-word;
                mtu 1522;
            }
        }
    }
}

```

ELine-QinQ-VLANRange-Ext-CCC Service Definition

This service definition provides a base for creating point-to-point services that transport a range of VLANs across an LDP or BGP network core using Q-in-Q endpoint interface types and extended-vlan-ccc as the physical encapsulation type. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- [Configuration on Endpoint A on page 541](#)
- [Configuration on Endpoint Z on page 542](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```

ge-0/1/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation extended-vlan-ccc;
    unit 2 {
        description Ext-VLANRange;
        vlan-tags outer 2 inner-range 100-110;
    }
}

```

```

        family ccc {
            filter {
                input filter_in_ge-0/1/1_2;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/1_2 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family ccc {
        filter filter_in_ge-0/1/1_2 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/1/1_2;
                    accept;
                }
            }
        }
    }
}

protocols {
    l2circuit {
        neighbor 192.168.1.30 {
            interface ge-0/1/1.2 {
                virtual-circuit-id 786;
                no-control-word;
                mtu 1522;
            }
        }
    }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z:

```

ge-0/1/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation extended-vlan-ccc;
    unit 2 {
        description Ext-VLANRange;
        vlan-tags outer 2 inner-range 100-110;
        family ccc {
            filter {
                input filter_in_ge-0/1/1_2;
            }
        }
    }
}

```

```

    }
  }
}

firewall {
  policer policer_in_ge-0/1/1_2 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
    then discard;
  }
  family ccc {
    filter filter_in_ge-0/1/1_2 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/1/1_2;
          accept;
        }
      }
    }
  }
}

protocols {
  l2circuit {
    neighbor 192.168.1.30 {
      interface ge-0/1/1.2 {
        virtual-circuit-id 786;
        no-control-word;
        mtu 1522;
      }
    }
  }
}

```

ELine-BGP-Port-Based

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- [Configuration on Endpoint A on page 543](#)
- [Configuration on Endpoint Z on page 544](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```

routing-instances{
  instance-type l2vpn;
  interface ge-1/0/7.0;
  route-distinguisher 69:27;
  vrf-target target:69:49165;
  protocols {

```

```

l2vpn {
    encapsulation-type ethernet-vlan;
    no-control-word;
    site L2VPN_Site_1 {
        site-identifier 1;
        mtu 1522;
        interface ge-1/0/7.0 {
            remote-site-id 2;
            description P2P-BGP-PortBased;
        }
    }
}

ge-1/0/7 {
    mtu 1522;
    encapsulation ethernet-ccc;
    unit 0 {
        family ccc {
            filter {
                input filter_in_ge-1/0/7;
            }
        }
    }
}

firewall{
    family ccc {
        filter filter_in_ge-1/0/7 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-1/0/7;
                    accept;
                }
            }
        }
        policer policer_in_ge-1/0/7 {
            if-exceeding {
                bandwidth-limit 10m;
                burst-size-limit 15220;
            }
            then discard;
        }
    }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z:

```

routing-instances{
    instance-type l2vpn;
    interface ge-1/0/8.0;
}

```



```

route-distinguisher 69:27;
vrf-target target:69:49165;
protocols {
  l2vpn {
    encapsulation-type ethernet-vlan;
    no-control-word;
    site L2VPN_Site_2 {
      site-identifier 2;
      mtu 1522;
      interface ge-1/0/8.0 {
        remote-site-id 1;
        description P2P-BGP-PortBased;
      }
    }
  }
}

ge-1/0/8 {
  mtu 1522;
  encapsulation ethernet-ccc;
  unit 0 {
    family ccc {
      filter {
        input filter_in_ge-1/0/8;
      }
    }
  }
}

firewall{
  family ccc {
    filter filter_in_ge-1/0/8 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-1/0/8;
          accept;
        }
      }
    }
    policer policer_in_ge-1/0/8 {
      if-exceeding {
        bandwidth-limit 10m;
        burst-size-limit 15220;
      }
      then discard;
    }
  }
}

```

ELine-BGP-Dot1q-SingleVLAN

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- [Configuration on Endpoint A on page 546](#)
- [Configuration on Endpoint Z on page 547](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```

routing-instances {
  instance-type l2vpn;
  interface ge-0/0/2.823;
  route-distinguisher 69:26;
  vrf-target target:69:49164;
  protocols {
    l2vpn {
      encapsulation-type ethernet-vlan;
      no-control-word;
      site L2VPN_Site_1 {
        site-identifier 1;
        interface ge-0/0/2.823 {
          remote-site-id 2;
        }
      }
    }
  }
}

ge-0/0/2 {
  enable;
  flexible-vlan-tagging;
  mtu 1522;
  encapsulation flexible-ethernet-services;
  unit 823 {
    description "ELine-BGP-Dot1Q";
    encapsulation vlan-ccc;
    vlan-id 823;
    family ccc {
      filter {
        input filter_in_ge-0/0/2_823;
      }
    }
  }
}

firewall{
  family ccc {
    filter filter_in_ge-0/0/2_823 {
      interface-specific;
      term 1 {
        then {

```

```

    policer policer_in_ge-0/0/2_823;
    accept;
}
}
}
}
policer policer_in_ge-0/0/2_823 {
    if-exceeding {
        bandwidth-limit 10m;
        burst-size-limit 15220;
    }
then discard;
}
}
```

```

routing-instances {
  instance-type l2vpn;
  interface ge-0/0/3.823;
  route-distinguisher 69:26;
  vrf-target target:69:49164;
  protocols {
    l2vpn {
      encapsulation-type ethernet-vlan;
      no-control-word;
      site L2VPN_Site_2 {
        site-identifier 2;
        interface ge-0/0/3.823 {
          remote-site-id 1;
        }
      }
    }
  }
}

ge-0/0/3 {
  enable;
  flexible-vlan-tagging;
  mtu 1522;
  encapsulation flexible-ethernet-services;
  unit 823 {
    description "ELine-BGP-Dot1Q";
    encapsulation vlan-ccc;
    vlan-id 823;
    family ccc {
      filter {
        input filter_in_ge-0/0/3_823;
      }
    }
  }
}

firewall{

```

```

family ccc {
    filter filter_in_ge-0/0/3_823 {
        interface-specific;
        term 1 {
            then {
                policer policer_in_ge-0/0/3_823;
                accept;
            }
        }
    }
    policer policer_in_ge-0/0/3_823 {
        if-exceeding {
            bandwidth-limit 10m;
            burst-size-limit 15220;
        }
        then discard;
    }
}

```

Eline-BGP-QinQ-AllVLAN

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 31 on page 466](#):

- [Configuration on Endpoint A on page 548](#)
- [Configuration on Endpoint Z on page 549](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A:

```

routing-instances {
    instance-type l2vpn;
    interface ge-0/0/1.981;
    route-distinguisher 69:15;
    vrf-target target:69:49160;
    protocols {
        l2vpn {
            encapsulation-type ethernet-vlan;
            no-control-word;
            site L2VPN_Site_1 {
                site-identifier 1;
                mtu 1522;
                interface ge-0/0/1.981 {
                    remote-site-id 2;
                    description P2P-BGP-QnQA11Vlan;
                }
            }
        }
    }
}

ge-0/0/3 {

```

```

flexible-vlan-tagging;
mtu 1522;
encapsulation flexible-ethernet-services;
unit 981 {
    description "No description available for selected UNI interface.";
    encapsulation vlan-ccc;
    vlan-tags outer 981;
    family ccc {
        filter {
            input filter_in_ge-0/0/3_981;
        }
    }
}

firewall{

    family ccc {

        filter filter_in_ge-0/0/3_981;{
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/0/3_981;
                    accept;
                }
            }
        }
    }
    policer policer_in_ge-0/0/3_981;{
        if-exceeding {
            bandwidth-limit 10m;
            burst-size-limit 15220;
        }
        then discard;
    }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z:

```

routing-instances {
    instance-type l2vpn;
    interface ge-0/0/5.981;
    route-distinguisher 69:15;
    vrf-target target:69:49160;
    protocols {
        l2vpn {
            encapsulation-type ethernet-vlan;
            no-control-word;
            site L2VPN_Site_2 {
                site-identifier 2;
                mtu 1522;
                interface ge-0/0/5.981 {
                    remote-site-id 1;
                    description P2P-BGP-QnQA11VLan;
                }
            }
        }
    }
}

```

```

    }
  }
}

ge-0/0/5 {
  flexible-vlan-tagging;
  mtu 1522;
  encapsulation flexible-ethernet-services;
  unit 981 {
    description "No description available for selected UNI interface.";
    encapsulation vlan-ccc;
    vlan-tags outer 981;
    family ccc {
      filter {
        input filter_in_ge-0/0/5.981
      }
    }
  }
}

firewall{
  family ccc {
    filter filter_in_ge-0/0/5.981 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/0/5.981
          accept;
        }
      }
    }
  }
  policer policer_in_ge-0/0/5.981 {
    if-exceeding {
      bandwidth-limit 10m;
      burst-size-limit 15220;
    }
    then discard;
  }
}

```

Related Documentation

- [Choosing a Predefined Service Definition or Creating a New Service Definition on page 593](#)
- [Creating a Point-to-Point Ethernet Service Definition on page 625](#)
- [Predefined Multipoint-to-Multipoint Ethernet Service Definitions on page 551](#)
- [Predefined Point-to-Multipoint Ethernet Service Definitions on page 576](#)
- [Predefined Full Mesh Layer 3 VPN Service Definitions on page 589](#)
- [Predefined Hub-and-Spoke Layer 3 VPN Service Definitions on page 590](#)

Predefined Multipoint-to-Multipoint Ethernet Service Definitions

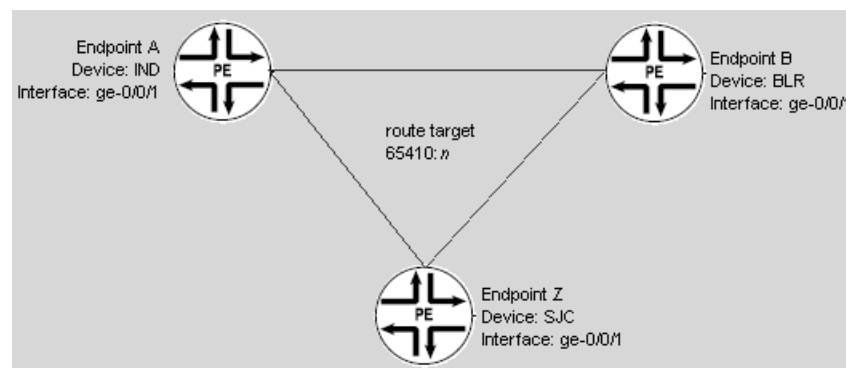
The Connectivity Services Director application provides predefined service definitions that a service provisioner can choose from when creating a service order. This section provides information about predefined service definitions used for creating multipoint-to-multipoint Ethernet services. For information about predefined service definitions used to create point-to-point service definitions or point-to-multipoint service definitions, see the following topics:

- [Predefined Point-to-Point Service Definitions on page 517](#)
- [Predefined Point-to-Multipoint Ethernet Service Definitions on page 576](#)

If none of the multipoint-to-multipoint predefined service definitions described here is appropriate for your needs, you can create a service definition as described in [“Creating a Multipoint-to-Multipoint VPLS Service Definition” on page 653](#).

The Connectivity Services Director application provides predefined service definitions for VPLS services that use BGP switching in the network core. These services are sometimes known as E-LAN services. This section covers multipoint-to-multipoint (or full mesh) service definitions. [Figure 32 on page 490](#) shows an example of such a service.

Figure 35: Multipoint-to-Multipoint Service



Information specific to each service instance, such as the device name, endpoint name, and customer VLAN ID, is provided in the service order. Attributes that can apply across many service instances are typically defined in the service definition. These attributes include:

- Ethernet option (dot1.q, port-port, qinq)
- Traffic type (single VLAN, VLAN range, all traffic)
- VLAN normalization
- Physical interface encapsulation
- Logical interface encapsulation
- Rate limit range

Table 66 on page 491 lists each of the standard VPLS service definitions. Each standard service definition is then described in detail in the sections that follow.

Table 69: Standard Multipoint-to-Multipoint Service Definitions

Standard Service Definition Name	Service Attributes
"ELAN-BGP-Dot1q-Normalized-VLAN-None" on page 492	<ul style="list-style-type: none"> • Multipoint Ethernet service for M Series and MX Series devices • Gigabit Ethernet interfaces • Customer VLAN IDs are not preserved • 802.1Q endpoint interface types • Customer traffic is single VLAN • Flexible-ethernet-services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELAN-BGP-Dot1Q-SingleVLAN" on page 496	<ul style="list-style-type: none"> • Multipoint Ethernet service for M Series or MX Series devices • Gigabit Ethernet interfaces • 802.1Q endpoint interface types • Customer traffic is single VLAN • Flexible-ethernet-services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELAN-BGP-PortBased" on page 499	<ul style="list-style-type: none"> • Multipoint Ethernet service for M series and MX Series devices • Gigabit Ethernet interfaces • Port-based UNIs • Transports all customer traffic • Ethernet VPLS as physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELAN-BGP-QinQ-AllVLAN" on page 502	<ul style="list-style-type: none"> • Multipoint Ethernet service for M Series and MX Series devices • Gigabit Ethernet interfaces • Q-in-Q endpoint interface types • All customer traffic • Flexible-ethernet-services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment

Table 69: Standard Multipoint-to-Multipoint Service Definitions (continued)

Standard Service Definition Name	Service Attributes
"ELAN-BGP-QinQ-AllVLAN-Normalized-All" on page 506	<ul style="list-style-type: none"> • Multipoint Ethernet service for M Series and MX Series devices • Gigabit Ethernet interfaces • Customer VLAN IDs preserved • Q-in-Q endpoint interface types • All customer traffic • Flexible-ethernet-services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELAN-BGP-QinQ-AllVLAN-Normalized-None" on page 509	<ul style="list-style-type: none"> • Multipoint Ethernet service for M Series and MX Series devices • Gigabit Ethernet interfaces • Q-in-Q endpoint interface types • VLAN IDs not preserved • All customer traffic • Flexible-ethernet-services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELAN-BGP-QinQ-Range-Normalized-VLAN" on page 512	<ul style="list-style-type: none"> • Multipoint Ethernet service for MX Series devices only • Gigabit Ethernet interfaces • Customer VLAN IDs preserved • Q-in-Q endpoint interface types • Transports specified VLAN range • Flexible Ethernet services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment

ELAN-BGP-Dot1q-Normalized-VLAN-None Service Definition

This service definition provides a base for creating multipoint-to-multipoint Ethernet services that transport traffic from a single VLAN on an endpoint across a BGP network core using 802.1Q endpoint interface types and flexible-ethernet-services as the physical encapsulation type. VLAN IDs are not preserved across the network—traffic passes from the single VLAN on an endpoint to any VLANs in the broadcast domain. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 32 on page 490](#):

- [Configuration on Endpoint A on page 554](#)
- [Configuration on Endpoint B on page 555](#)
- [Configuration on Endpoint Z on page 556](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A (device IND):

```
ge-0/0/1 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-id 1;
        family vpls {
            filter {
                input filter_in_ge-0/0/1_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/0/1_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family vpls {
        filter filter_in_ge-0/0/1_1 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/0/1_1;
                    accept;
                }
            }
        }
    }
}

routing-instances {
    BestCustomer_ELAN-BGP-Dot1q-Normalized-VLAN-SR {
        instance-type vpls;
        vlan-id none;
        interface ge-0/0/1.1;
        route-distinguisher 65410:1;
        vrf-target target:65410:0;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_2 {
                    site-identifier 2;
                }
            }
        }
    }
}
```

```

        site-preference primary;
        interface ge-0/0/1.1;
    }
}

```

Configuration on Endpoint B

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint B (device BLR):

```

ge-0/0/1 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-id 1;
        family vpls {
            filter {
                input filter_in_ge-0/0/1_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/0/1_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family vpls {
        filter filter_in_ge-0/0/1_1 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/0/1_1;
                    accept;
                }
            }
        }
    }
}

routing-instances {
    BestCustomer_ELAN-BGP-Dot1q-Normalized-VLAN-SR {
        instance-type vpls;
        vlan-id none;
        interface ge-0/0/1.1;
        route-distinguisher 65410:0;
        vrf-target target:65410:0;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_1 {
                    site-identifier 1;
                    site-preference primary;
                }
            }
        }
    }
}

```

```

        }
    }
}
interface ge-0/0/1.1;

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z (device SJC):

```

ge-0/0/1 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-id 1;
        family vpls {
            filter {
                input filter_in_ge-0/0/1_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/0/1_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family vpls {
        filter filter_in_ge-0/0/1_1 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/0/1_1;
                    accept;
                }
            }
        }
    }
}

routing-instances {
    BestCustomer_ELAN-BGP-Dot1q-Normalized-VLAN-SR {
        instance-type vpls;
        vlan-id none;
        interface ge-0/0/1.1;
        vlan-id none;
        route-distinguisher 65410:2;
        vrf-target target:65410:0;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_3 {

```

```

        site-identifier 3;
        site-preference primary;
        interface ge-0/0/1.1;
    }
}
}

```

ELAN-BGP-Dot1Q-SingleVLAN Service Definition

This service definition provides a base for creating multipoint-to-multipoint Ethernet services that transport traffic on a single VLAN across a BGP network core using 802.1Q endpoint interface types and flexible-ethernet-services as the physical encapsulation type. No VLAN mapping is performed—the VLAN ID must be the same on all endpoints. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 32 on page 490](#):

- [Configuration on Endpoint A on page 557](#)
- [Configuration on Endpoint B on page 558](#)
- [Configuration on Endpoint Z on page 559](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A (device IND):

```

ge-0/0/2 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-id 1;
        family vpls {
            filter {
                input filter_in_ge-0/0/2_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/0/2_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }

    filter filter_in_ge-0/0/2_1 {
        interface-specific;
        term 1 {

```

```

        then {
            policer policer_in_ge-0/0/2_1;
            accept;
        }
    }
}

routing-instances {
    BestCustomer_ELAN-BGP-Dot1Q-SingleVLAN-SR {
        instance-type vpls;
        interface ge-0/0/2.1;
        route-distinguisher 65410:4;
        vrf-target target:65410:1;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_2 {
                    site-identifier 2;
                    site-preference primary;
                    interface ge-0/0/2.1;
                }
            }
        }
    }
}

```

Configuration on Endpoint B

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint B (device BLR):

```

ge-0/0/2 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-id 1;
        family vpls {
            filter {
                input filter_in_ge-0/0/2_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/0/2_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }

    filter filter_in_ge-0/0/2_1 {
        interface-specific;
        term 1 {
            then {
                policer policer_in_ge-0/0/2_1;
            }
        }
    }
}

```

```

        accept;
    }
}
}
}
}

routing-instances {
    BestCustomer_ELAN-BGP-Dot1Q-SingleVLAN-SR {
        instance-type vpls;
        interface ge-0/0/2.1;
        route-distinguisher 65410:3;
        vrf-target target:65410:1;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_1 {
                    site-identifier 1;
                    site-preference primary;
                    interface ge-0/0/2.1;
                }
            }
        }
    }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z (device SJC):

```

ge-0/0/2 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-id 1;
        family vpls {
            filter {
                input filter_in_ge-0/0/2_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/0/2_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family vpls {
        filter filter_in_ge-0/0/2_1 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/0/2_1;
                }
            }
        }
    }
}

```

```

    }
    }
    }
}
routing-instances {
    BestCustomer_ELAN-BGP-Dot1Q-SingleVLAN-SR {
        instance-type vpls;
        interface ge-0/0/2.1;
        route-distinguisher 65410:5;
        vrf-target target:65410:1;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_3 {
                    site-identifier 3;
                    site-preference primary;
                    interface ge-0/0/2.1;
                }
            }
        }
    }
}

```

ELAN-BGP-PortBased Service Definition

This service definition provides a base for creating multipoint-to-multipoint Ethernet services that transport all traffic on an entire port across a BGP network core using ethernet-vpls as the physical encapsulation type. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 32 on page 490](#):

- Configuration on Endpoint A on page 560
- Configuration on Endpoint B on page 561
- Configuration on Endpoint Z on page 562

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A (device IND):

```
ge-0/1/3 {
    mtu 1522;
    encapsulation ethernet-vpls;
    unit 0 {
        family vpls {
            filter {
                input filter_in_ge-0/1/3;
            }
        }
    }
}
```



```

firewall {
  policer policer_in_ge-0/1/3 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 15220;
    }
    then discard;
  }
  family vpls {
    filter filter_in_ge-0/1/3 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/1/3;
          accept;
        }
      }
    }
  }
}
routing-instances {
  ELAN_BGP_PortBased_10_100M {
    instance-type vpls;
    interface ge-0/1/3.0;
    route-distinguisher 65410:3;
    vrf-target target:65410:1;
    protocols {
      vpls {
        no-tunnel-services;
        site Site_2 {
          site-identifier 2;
          site-preference primary;
          interface ge-0/1/3.0;
        }
      }
    }
  }
}

```

Configuration on Endpoint B

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint B (device BLR):

```

ge-0/1/3 {
  mtu 1522;
  encapsulation ethernet-vpls;
  unit 0 {
    family vpls {
      filter {
        input filter_in_ge-0/1/3;
      }
    }
  }
}

```

```

firewall {
  policer policer_in_ge-0/1/3 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 15220;
    }
    then discard;
  }
  family vpls {
    filter filter_in_ge-0/1/3 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/1/3;
          accept;
        }
      }
    }
  }
}
routing-instances {
  ELAN_BGP_PortBased_10_100M {
    instance-type vpls;
    interface ge-0/1/3.0;
    route-distinguisher 65410:2;
    vrf-target target:65410:1;
    protocols {
      vpls {
        no-tunnel-services;
        site Site_1 {
          site-identifier 1;
          site-preference primary;
          interface ge-0/1/3.0;
        }
      }
    }
  }
}
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z (device SJC):

```

ge-0/2/2 {
  mtu 1522;
  encapsulation ethernet-vpls;
  unit 0 {
    family vpls {
      filter {
        input filter_in_ge-0/2/2;
      }
    }
  }
}
}
firewall {

```

```

    policer policer_in_ge-0/2/2 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 15220;
        }
        then discard;
    }
    family vpls {
        filter filter_in_ge-0/2/2 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/2/2;
                    accept;
                }
            }
        }
    }
}

routing-instances {
    ELAN_BGP_PortBased_10_100M {
        instance-type vpls;
        interface ge-0/2/2.0;
        route-distinguisher 65410:4;
        vrf-target target:65410:1;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_3 {
                    site-identifier 3;
                    site-preference primary;
                    interface ge-0/2/2.0;
                }
            }
        }
    }
}

```

ELAN-BGP-QinQ-AllVLAN Service Definition

This service definition provides a base for creating multipoint-to-multipoint Ethernet services that transport all traffic across a BGP network core using Q-in-Q endpoint interface types and flexible-ethernet-services as the physical encapsulation type. No VLAN mapping is performed—customer VLAN IDs and service provider VLAN IDs must match on each endpoint that is to send or receive traffic. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 32 on page 490](#):

- [Configuration on Endpoint A on page 564](#)
- [Configuration on Endpoint B on page 565](#)
- [Configuration on Endpoint Z on page 566](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A (device IND):

```

ge-0/1/1 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-tags outer 1;
        family vpls {
            filter {
                input filter_in_ge-0/1/1_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/1_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family vpls {
        filter filter_in_ge-0/1/1_1 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/1/1_1;
                    accept;
                }
            }
        }
    }
}

routing-instances {
    BestCustomer_ELAN-BGP-QinQ-AllVLAN-SR {
        instance-type vpls;
        interface ge-0/1/1.1;
        route-distinguisher 65410:13;
        vrf-target target:65410:4;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_2 {
                    site-identifier 2;
                    site-preference primary;
                    interface ge-0/1/1.1;
                }
            }
        }
    }
}

```

Configuration on Endpoint B

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint B (device BLR):

```
ge-0/1/1 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-tags outer 1;
        family vpls {
            filter {
                input filter_in_ge-0/1/1_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/1_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family vpls {
        filter filter_in_ge-0/1/1_1 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/1/1_1;
                    accept;
                }
            }
        }
    }
}

routing-instances {
    BestCustomer_ELAN-BGP-QinQ-AllVLAN-SR {
        instance-type vpls;
        interface ge-0/1/1.1;
        route-distinguisher 65410:12;
        vrf-target target:65410:4;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_1 {
                    site-identifier 1;
                    site-preference primary;
                    interface ge-0/1/1.1;
                }
            }
        }
    }
}
```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z (device SJC):

```

ge-0/0/5 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-tags outer 1;
        family vpls {
            filter {
                input filter_in_ge-0/0/5_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/0/5_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family vpls {
        filter filter_in_ge-0/0/5_1 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/0/5_1;
                    accept;
                }
            }
        }
    }
}

routing-instances {
    BestCustomer_ELAN-BGP-QinQ-AllVLAN-SR {
        instance-type vpls;
        interface ge-0/0/5.1;
        route-distinguisher 65410:14;
        vrf-target target:65410:4;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_3 {
                    site-identifier 3;
                    site-preference primary;
                    interface ge-0/0/5.1;
                }
            }
        }
    }
}

```

ELAN-BGP-QinQ-AllVLAN-Normalized-All Service Definition

This service definition provides a base for creating multipoint-to-multipoint Ethernet services that transport all traffic across a BGP network core using Q-in-Q endpoint interface types and flexible-ethernet-services as the physical encapsulation type. Customer VLAN IDs are preserved across the network—traffic passes only among matching customer VLAN IDs. However, traffic can pass among any service provider VLAN ID in the broadcast domain. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 32 on page 490](#):

- [Configuration on Endpoint A on page 567](#)
- [Configuration on Endpoint B on page 568](#)
- [Configuration on Endpoint Z on page 569](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A (device IND):

```
ge-0/1/0 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-tags outer 1;
        family vpls {
            filter {
                input filter_in_ge-0/1/0_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/1/0_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family vpls {
        filter filter_in_ge-0/1/0_1 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/1/0_1;
                    accept;
                }
            }
        }
    }
}
```

```

}
routing-instances {
  BestCustomer_ELAN-BGP-QinQ-AllVLAN-Normalized-All-SR {
    instance-type vpls;
    vlan-id all;
    interface ge-0/1/0.1;
    route-distinguisher 65410:10;
    vrf-target target:65410:3;
    protocols {
      vpls {
        no-tunnel-services;
        site Site_2 {
          site-identifier 2;
          site-preference primary;
          interface ge-0/1/0.1;
        }
      }
    }
  }
}

```

Configuration on Endpoint B

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint B (device BLR):

```

ge-0/1/0 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 1 {
    encapsulation vlan-vpls;
    vlan-tags outer 1;
    family vpls {
      filter {
        input filter_in_ge-0/1/0_1;
      }
    }
  }
}

firewall {
  policer policer_in_ge-0/1/0_1 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
    then discard;
  }
  family vpls {
    filter filter_in_ge-0/1/0_1 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/1/0_1;
          accept;
        }
      }
    }
  }
}

```



```

}
routing-instances {
  BestCustomer_ELAN-BGP-QinQ-AllVLAN-Normalized-All-SR {
    instance-type vpls;
    vlan-id all;
    interface ge-0/1/0.1;
    route-distinguisher 65410:9;
    vrf-target target:65410:3;
    protocols {
      vpls {
        no-tunnel-services;
        site Site_1 {
          site-identifier 1;
          site-preference primary;
          interface ge-0/1/0.1;
        }
      }
    }
  }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z (device SJC):

```

ge-0/0/4 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 1 {
    encapsulation vlan-vpls;
    vlan-tags outer 1;
    family vpls {
      filter {
        input filter_in_ge-0/0/4_1;
      }
    }
  }
}
firewall {
  policer policer_in_ge-0/0/4_1 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
    then discard;
  }
  family vpls {
    filter filter_in_ge-0/0/4_1 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/0/4_1;
          accept;
        }
      }
    }
  }
}
}

```

```

routing-instances {
  BestCustomer_ELAN-BGP-QinQ-AllVLAN-Normalized-All-SR {
    instance-type vpls;
    vlan-id all;
    interface ge-0/0/4.1;
    vlan-id all;
    route-distinguisher 65410:11;
    vrf-target target:65410:3;
    protocols {
      vpls {
        no-tunnel-services;
        site Site_3 {
          site-identifier 3;
          site-preference primary;
          interface ge-0/0/4.1;
        }
      }
    }
  }
}

```

ELAN-BGP-QinQ-AllVLAN-Normalized-None Service Definition

This service definition provides a base for creating multipoint-to-multipoint Ethernet services that transport all traffic across a BGP network core using Q-in-Q endpoint interface types and flexible-ethernet-services as the physical encapsulation type. VLAN IDs are not preserved across the network—traffic passes between any customer VLAN or service provider VLAN in the broadcast domain. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 32 on page 490](#):

- [Configuration on Endpoint A on page 570](#)
- [Configuration on Endpoint B on page 571](#)
- [Configuration on Endpoint Z on page 572](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A (device IND):

```

ge-0/0/3 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 1 {
    encapsulation vlan-vpls;
    vlan-tags outer 1;
    family vpls {
      filter {
        input filter_in_ge-0/0/3_1;
      }
    }
  }
}

```

```

    }
firewall {
    policer policer_in_ge-0/0/3_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family vpls {
        filter filter_in_ge-0/0/3_1 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/0/3_1;
                    accept;
                }
            }
        }
    }
}
routing-instances {
    BestCustomer_ELAN-BGP-QinQ-AllVLAN-Normalized-SR {
        instance-type vpls;
        vlan-id none;
        interface ge-0/0/3.1;
        route-distinguisher 65410:7;
        vrf-target target:65410:2;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_2 {
                    site-identifier 2;
                    site-preference primary;
                    interface ge-0/0/3.1;
                }
            }
        }
    }
}
}

```

Configuration on Endpoint B

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint B (device BLR):

```

ge-0/0/3 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-tags outer 1;
        family vpls {
            filter {
                input filter_in_ge-0/0/3_1;
            }
        }
    }
}

```

```

    }
  }
  firewall {
    policer policer_in_ge-0/0/3_1 {
      if-exceeding {
        bandwidth-limit 100m;
        burst-size-limit 62500000;
      }
      then discard;
    }
    family vpls {
      filter filter_in_ge-0/0/3_1 {
        interface-specific;
        term 1 {
          then {
            policer policer_in_ge-0/0/3_1;
            accept;
          }
        }
      }
    }
  }
}
routing-instances {
  BestCustomer_ELAN-BGP-QinQ-AllVLAN-Normalized-SR {
    instance-type vpls;
    vlan-id none;
    interface ge-0/0/3.1;
    route-distinguisher 65410:6;
    vrf-target target:65410:2;
    protocols {
      vpls {
        no-tunnel-services;
        site Site_1 {
          site-identifier 1;
          site-preference primary;
          interface ge-0/0/3.1;
        }
      }
    }
  }
}
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z (device SJC):

```

ge-0/0/3 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 1 {
    encapsulation vlan-vpls;
    vlan-tags outer 1;
    family vpls {
      filter {
        input filter_in_ge-0/0/3_1;
      }
    }
  }
}

```

```

    }
  }
}

firewall {
  policer policer_in_ge-0/0/3_1 {
    if-exceeding {
      bandwidth-limit 100m;
      burst-size-limit 62500000;
    }
    then discard;
  }
  family vpls {
    filter filter_in_ge-0/0/3_1 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/0/3_1;
          accept;
        }
      }
    }
  }
}

routing-instances {
  BestCustomer_ELAN-BGP-QinQ-AllVLAN-Normalized-SR {
    instance-type vpls;
    vlan-id none;
    interface ge-0/0/3.1;
    vlan-id none;
    route-distinguisher 65410:8;
    vrf-target target:65410:2;
    protocols {
      vpls {
        no-tunnel-services;
        site Site_3 {
          site-identifier 3;
          site-preference primary;
          interface ge-0/0/3.1;
        }
      }
    }
  }
}
}

```

ELAN-BGP-QinQ-Range-Normalized-VLAN Service Definition

This service definition provides a base for creating multipoint-to-multipoint Ethernet services that transport traffic from a range of VLANs on an endpoint across a BGP network core using Q-in-Q endpoint interface types and flexible-ethernet-services as the physical encapsulation type. Services built from this service definition must use MX Series devices on the provider edge. Customer VLAN IDs are preserved across the network—traffic passes among like customer VLAN IDs on any service provider VLAN in the broadcast domain. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data for a service with only two endpoints, SJC and SFO.

- [Configuration on Endpoint A on page 574](#)
- [Configuration on Endpoint Z on page 575](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A (device SJC):

```
ge-0/0/6 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation flexible-ethernet-services;
    unit 2 {
        encapsulation vlan-vpls;
        vlan-tags outer 2 inner-range 1500-2000;
        family vpls {
            filter {
                input filter_in_ge-0/0/6_2;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/0/6_2 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family vpls {
        filter filter_in_ge-0/0/6_2 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/0/6_2;
                    accept;
                }
            }
        }
    }
}

routing-instances {
    BestCustomer_ELAN-BGP-QinQ-Range-Normalized-VLAN-SR1 {
        instance-type vpls;
        vlan-id all;
        interface ge-0/0/6.2;
        vlan-id all;
        route-distinguisher 65410:19;
        vrf-target target:65410:6;
        protocols {
            vpls {
                no-tunnel-services;
                site Site_2 {
```

```

        site-identifier 2;
        site-preference primary;
        interface ge-0/0/6.2;
    }
}
}
}
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z (device SFO):

```

ge-0/0/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-tags outer 1 inner-range 1500-2000;
        family vpls {
            filter {
                input filter_in_ge-0/0/1_1;
            }
        }
    }
}

firewall {
    policer policer_in_ge-0/0/1_1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 62500000;
        }
        then discard;
    }
    family vpls {
        filter filter_in_ge-0/0/1_1 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-0/0/1_1;
                    accept;
                }
            }
        }
    }
}

routing-instances {
    BestCustomer_ELAN-BGP-QinQ-Range-Normalized-VLAN-SR1 {
        instance-type vpls;
        vlan-id all;
        interface ge-0/0/1.1;
        route-distinguisher 65410:18;
        vrf-target target:65410:6;
        protocols {
            vpls {

```

```
no-tunnel-services;
site Site_1 {
    site-identifier 1;
    site-preference primary;
    interface ge-0/0/1.1;
}
}
```

**Related
Documentation**

- [Predefined Service Definitions on page 465](#)
- [Predefined Point-to-Point Service Definitions on page 517](#)
- [Predefined Point-to-Multipoint Ethernet Service Definitions on page 576](#)
- [Predefined Full Mesh Layer 3 VPN Service Definitions on page 589](#)
- [Predefined Hub-and Spoke Layer 3 VPN Service Definitions on page 590](#)

Predefined Point-to-Multipoint Ethernet Service Definitions

The Connectivity Services Director application provides predefined service definitions that a service provisioner can choose from when creating a service order. This section provides information about predefined service definitions used for creating point-to-multipoint services. For information about predefined service definitions used to create point-to-point service definitions or multipoint-to-multipoint service definitions, see the following topics:

- [Predefined Point-to-Point Service Definitions on page 517](#)
- [Predefined Multipoint-to-Multipoint Ethernet Service Definitions on page 551](#)

If none of the point-to-multipoint predefined service definitions described here is appropriate for your needs, you can create a service definition as described in "[Creating a Point-to-Multipoint VPLS Service Definition](#)" on page 678.

The Connectivity Services Director application provides predefined service definitions for VPLS services that use BGP switching in the network core. These services are sometimes known as E-LAN services. This section covers point-to-multipoint (or hub-and-spoke) service definitions.

Information specific to each service instance, such as the device name, endpoint name, customer VLAN ID, and whether a specific endpoint is a hub or a spoke is provided in the service order. Attributes that can apply across many service instances are typically defined in the service definition. These attributes include:

- Ethernet option (dot1.q, qinq)
- Traffic type (single VLAN, VLAN range, all traffic)
- VLAN normalization
- Physical interface encapsulation

- Logical interface encapsulation
- Rate limit range

Table 70 on page 577 lists each of the standard VPLS service definitions. Each standard service definition is then described in detail in the sections that follow.

Table 70: Standard Point-to-Multipoint Service Definitions

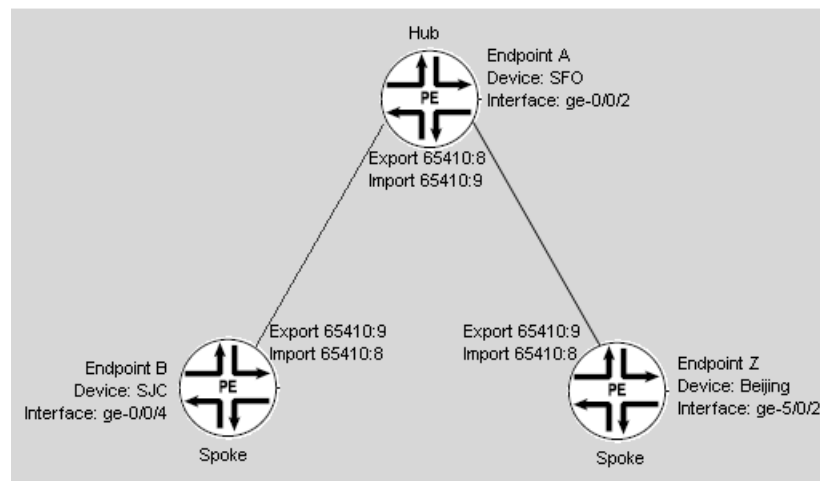
Standard Service Definition Name	Service Attributes
"ELAN-Hub-Spoke-QinQ-AllVLAN" on page 516	<ul style="list-style-type: none"> • Multipoint Ethernet service for M Series or MX Series devices • Gigabit Ethernet interfaces • Customer VLAN IDs are preserved • Q-in-Q endpoint interface types • All customer traffic • Flexible-ethernet-services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
"ELAN-Hub-Spoke-QinQ-AllVLAN-No" on page 517	<ul style="list-style-type: none"> • Multipoint Ethernet service for M Series and MX Series devices • Gigabit Ethernet interfaces • Customer VLAN IDs are not preserved • Q-in-Q endpoint interface types • All customer traffic • Flexible-ethernet-services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment

ELAN-Hub-Spoke-QinQ-AllVLAN-Normalized-All Service Definition

This service definition provides a base for creating point-to-multipoint Ethernet services that transport all traffic on an endpoint across a BGP network core using Q-in-Q endpoint interface types and flexible-ethernet-services as the physical encapsulation type. VLAN IDs are not preserved across the network—traffic passes from the single VLAN on an endpoint to any VLANs in the broadcast domain. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps.

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in Figure 33 on page 515—a point-to-multipoint service with one hub and two spokes.

Figure 36: Point-to-Multipoint Service with One Hub



- [Configuration on Endpoint A on page 578](#)
- [Configuration on Endpoint B on page 580](#)
- [Configuration on Endpoint Z on page 581](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A (device SFO). This device is configured as the service hub.

```
interfaces {
  ge-0/0/2 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation flexible-ethernet-services;
    unit 4 {
      encapsulation vlan-vpls;
      vlan-tags outer 4;
      family vpls {
        filter {
          input filter_in_ge-0/0/2_4;
        }
      }
    }
  }
}

policy-options {
  policy-statement ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-hm-export {
    term 1 {
      then {
        community add
        export-comm-hm-ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-65410:8;
        accept;
      }
    }
    term 2 {
      then reject;
    }
  }
}
```

```

}
policy-statement ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-hm-import {
  term 1 {
    from {
      protocol bgp;
      community [
import-comm-hm-ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-65410:9
import-comm-hm-ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-65410:8 ];
      }
    then accept;
  }
  term 2 {
    then reject;
  }
}
community export-comm-hm-ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-65410:8
members target:65410:8;
community import-comm-hm-ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-65410:8
members target:65410:8;
community import-comm-hm-ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-65410:9
members target:65410:9;
}
firewall {
  family vpls {
    filter filter_in_ge-0/0/2_4 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/0/2_4;
          accept;
        }
      }
    }
  }
  policer policer_in_ge-0/0/2_4 {
    if-exceeding {
      bandwidth-limit 10m;
      burst-size-limit 15220;
    }
    then discard;
  }
}
routing-instances {
  ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All {
    instance-type vpls;
    vlan-id all;
    interface ge-0/0/2.4;
    route-distinguisher 65410:15;
    vrf-import ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-hm-import;
    vrf-export ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-hm-export;
    protocols {
      vpls {
        mac-table-size {
          5120;
        }
        interface-mac-limit {
          1024;
        }
        no-tunnel-services;
        site Site_2 {

```

```

        site-identifier 2;
        site-preference primary;
        interface ge-0/0/2.4;
    }
}

```

Configuration on Endpoint B

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint B (device SJC). This device is a service spoke.

```

interfaces {
  ge-0/0/4 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation flexible-ethernet-services;
    unit 4 {
      encapsulation vlan-vpls;
      vlan-tags outer 4;
      family vpls {
        filter {
          input filter_in_ge-0/0/4_4;
        }
      }
    }
  }
}

policy-options {
  policy-statement ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-export {
    term 1 {
      then {
        community add
        export-comm-ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-65410:9;
        accept;
      }
    }
    term 2 {
      then reject;
    }
  }
  policy-statement ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-import {
    term 1 {
      from {
        protocol bgp;
        community
        import-comm-ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-65410:8;
      }
      then accept;
    }
    term 2 {
      then reject;
    }
  }
  community export-comm-ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-65410:9
  members target:65410:9;
  community import-comm-ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-65410:8
  members target:65410:8;
}

```

```

}

firewall {
  family vpls {
    filter filter_in_ge-0/0/4_4 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/0/4_4;
          accept;
        }
      }
    }
  }
  policer policer_in_ge-0/0/4_4 {
    if-exceeding {
      bandwidth-limit 10m;
      burst-size-limit 15220;
    }
    then discard;
  }
}

routing-instances {
  ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All {
    instance-type vpls;
    vlan-id all;
    interface ge-0/0/4.4;
    route-distinguisher 65410:16;
    vrf-import ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-import;
    vrf-export ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-export;
    protocols {
      vpls {
        mac-table-size {
          5120;
        }
        interface-mac-limit {
          1024;
        }
        no-tunnel-services;
        site Site_3 {
          site-identifier 3;
          site-preference primary;
          interface ge-0/0/4.4;
        }
      }
    }
  }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z (device Beijing). Thus device is a service spoke.

```

interfaces {
  ge-5/0/2 {
    unit 2 {
      encapsulation vlan-vpls;
      vlan-tags outer 2;
      family vpls {

```

```

        filter {
            input filter_in_ge-5/0/2_2;
        }
    }
}

policy-options {
    policy-statement ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-export {
        term 1 {
            then {
                community add
                export-comm-ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-65410:9;
                accept;
            }
        }
        term 2 {
            then reject;
        }
    }
    policy-statement ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-import {
        term 1 {
            from {
                protocol bgp;
                community
                import-comm-ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-65410:8;
            }
            then accept;
        }
        term 2 {
            then reject;
        }
    }
    community export-comm-ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-65410:9
    members target:65410:9;
    community import-comm-ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-65410:8
    members target:65410:8;
}

firewall {
    family vpls {
        filter filter_in_ge-5/0/2_2 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-5/0/2_2;
                    accept;
                }
            }
        }
    }
    policer policer_in_ge-5/0/2_2 {
        if-exceeding {
            bandwidth-limit 10m;
            burst-size-limit 15220;
        }
        then discard;
    }
}

ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All {
    instance-type vpls;
}

```

```

vlan-id all;
interface ge-5/0/2.2;
route-distinguisher 65410:14;
vrf-import ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-import;
vrf-export ELAN_Hub_Spoke_QinQ_AllVLAN_Normalized_All-export;
protocols {
  vpls {
    mac-table-size {
      5120;
    }
    interface-mac-limit {
      1024;
    }
    no-tunnel-services;
    site Site_1 {
      site-identifier 1;
      site-preference primary;
      interface ge-5/0/2.2;
    }
  }
}
}

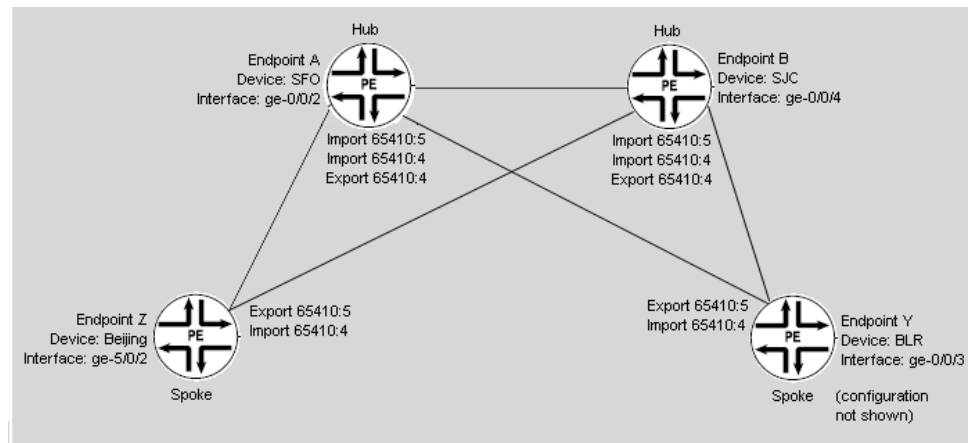
```

ELAN-Hub-Spoke-QinQ-AllVLAN Service Definition

This service definition provides a base for creating point-to-multipoint Ethernet services that transport all traffic on an endpoint across a BGP network core using Q-in-Q endpoint interface types and flexible-ethernet-services as the physical encapsulation type. Customer VLAN IDs are preserved across the network—traffic passes among like customer VLAN IDs on any service provider VLAN in the broadcast domain. Service provisioners can limit the bandwidth of services built from this service definition to specific values from 10 Mbps through 100 Mbps. [Figure 37 on page 584](#) shows a point-to-multipoint service with two hubs.

The following sections show the configuration data on endpoints A, B, and Z when you use this service definition to create the service shown in [Figure 37 on page 584](#)—a point-to-multipoint service with two service hubs and two spokes. The configuration for endpoint Y is not described.

Figure 37: Point-to-Multipoint Service with Two Hubs



- [Configuration on Endpoint A on page 584](#)
- [Configuration on Endpoint B on page 586](#)
- [Configuration on Endpoint Z on page 587](#)

Configuration on Endpoint A

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint A (device SFO). This device is configured as a service hub.

```

interfaces {
  ge-0/0/2 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation flexible-ethernet-services;
    unit 3 {
      encapsulation vlan-vpls;
      vlan-tags outer 3;
      family vpls {
        filter {
          input filter_in_ge-0/0/2_3;
        }
      }
    }
  }
}

policy-options {
  policy-statement ELAN_Hub_Spoke_QinQ_A11VLAN-hm-export {
    term 1 {
      then {
        community add export-comm-hm-ELAN_Hub_Spoke_QinQ_A11VLAN-65410:4;
        accept;
      }
    }
    term 2 {
      then reject;
    }
  }
}

```



```

policy-statement ELAN_Hub_Spoke_QinQ_AllVLAN-hm-import {
  term 1 {
    from {
      protocol bgp;
      community [ import-comm-hm-ELAN_Hub_Spoke_QinQ_AllVLAN-65410:5
import-comm-hm-ELAN_Hub_Spoke_QinQ_AllVLAN-65410:4 ];
    }
    then accept;
  }
  term 2 {
    then reject;
  }
}
community export-comm-hm-ELAN_Hub_Spoke_QinQ_AllVLAN-65410:4 members
target:65410:4;
community import-comm-hm-ELAN_Hub_Spoke_QinQ_AllVLAN-65410:4 members
target:65410:4;
community import-comm-hm-ELAN_Hub_Spoke_QinQ_AllVLAN-65410:5 members
target:65410:5;
}

firewall {
  family vpls {
    filter filter_in_ge-0/0/2_3 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/0/2_3;
          accept;
        }
      }
    }
  }

  policer policer_in_ge-0/0/2_3 {
    if-exceeding {
      bandwidth-limit 10m;
      burst-size-limit 15220;
    }
    then discard;
  }
}

ELAN_Hub_Spoke_QinQ_AllVLAN {
  instance-type vpls;
  interface ge-0/0/2.3;
  route-distinguisher 65410:9;
  vrf-import ELAN_Hub_Spoke_QinQ_AllVLAN-hm-import;
  vrf-export ELAN_Hub_Spoke_QinQ_AllVLAN-hm-export;
  protocols {
    vpls {
      mac-table-size {
        5120;
      }
      interface-mac-limit {
        1024;
      }
      no-tunnel-services;
      site Site_2 {
        site-identifier 2;
        site-preference primary;
      }
    }
  }
}

```

```

    }
  }
}

interface ge-0/0/2.3;
}

```

Configuration on Endpoint B

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint B (device SJC). This device is configured as a service hub.

```

interfaces {
  ge-0/0/4 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation flexible-ethernet-services
    unit 3 {
      encapsulation vlan-vpls;
      vlan-tags outer 3;
      family vpls {
        filter {
          input filter_in_ge-0/0/4_3;
        }
      }
    }
  }
}

policy-options {
  policy-statement ELAN_Hub_Spoke_QinQ_AllVLAN-hm-export {
    term 1 {
      then {
        community add export-comm-hm-ELAN_Hub_Spoke_QinQ_AllVLAN-65410:4;

        accept;
      }
    }
    term 2 {
      then reject;
    }
  }
  policy-statement ELAN_Hub_Spoke_QinQ_AllVLAN-hm-import {
    term 1 {
      from {
        protocol bgp;
        community [ import-comm-hm-ELAN_Hub_Spoke_QinQ_AllVLAN-65410:5
import-comm-hm-ELAN_Hub_Spoke_QinQ_AllVLAN-65410:4 ];
      }
      then accept;
    }
    term 2 {
      then reject;
    }
  }
  community export-comm-hm-ELAN_Hub_Spoke_QinQ_AllVLAN-65410:4 members
target:65410:4;
  community import-comm-hm-ELAN_Hub_Spoke_QinQ_AllVLAN-65410:4 members
target:65410:4;
  community import-comm-hm-ELAN_Hub_Spoke_QinQ_AllVLAN-65410:5 members
target:65410:5;
}

```

```

}

firewall {
  family vpls {
    filter filter_in_ge-0/0/4_3 {
      interface-specific;
      term 1 {
        then {
          policer policer_in_ge-0/0/4_3;
          accept;
        }
      }
    }
  }
  policer policer_in_ge-0/0/4_3 {
    if-exceeding {
      bandwidth-limit 10m;
      burst-size-limit 15220;
    }
    then discard;
  }
}

ELAN_Hub_Spoke_QinQ_AllVLAN {
  instance-type vpls;
  interface ge-0/0/4.3;
  route-distinguisher 65410:10;
  vrf-import ELAN_Hub_Spoke_QinQ_AllVLAN-hm-import;
  vrf-export ELAN_Hub_Spoke_QinQ_AllVLAN-hm-export;
  protocols {
    vpls {
      mac-table-size {
        5120;
      }
      interface-mac-limit {
        1024;
      }
      no-tunnel-services;
      site Site_3 {
        site-identifier 3;
        site-preference primary;
        interface ge-0/0/4.3;
      }
    }
  }
}

```

Configuration on Endpoint Z

The following statements show the interface configuration, the filter configuration, and connectivity configuration on endpoint Z (device Beijing). This device is configured as a service spoke.

```

interfaces {
  ge-5/0/2 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation flexible-ethernet-services;
    unit 1 {

```

```

        encapsulation vlan-vpls;
        vlan-tags outer 1;
        family vpls {
            filter {
                input filter_in_ge-5/0/2_1;
            }
        }
    }
}

policy-options {
    policy-statement ELAN_Hub_Spoke_QinQ_AllVLAN-export {
        term 1 {
            then {
                community add export-comm-ELAN_Hub_Spoke_QinQ_AllVLAN-65410:5;
                accept;
            }
        }
        term 2 {
            then reject;
        }
    }
    policy-statement ELAN_Hub_Spoke_QinQ_AllVLAN-import {
        term 1 {
            from {
                protocol bgp;
                community import-comm-ELAN_Hub_Spoke_QinQ_AllVLAN-65410:4;
            }
            then accept;
        }
        term 2 {
            then reject;
        }
    }
    community export-comm-ELAN_Hub_Spoke_QinQ_AllVLAN-65410:5 members
target:65410:5;
    community import-comm-ELAN_Hub_Spoke_QinQ_AllVLAN-65410:4 members
target:65410:4;
}

firewall {
    family vpls {
        filter filter_in_ge-5/0/2_1 {
            interface-specific;
            term 1 {
                then {
                    policer policer_in_ge-5/0/2_1;
                    accept;
                }
            }
        }
    }
    policer policer_in_ge-5/0/2_1 {
        if-exceeding {
            bandwidth-limit 10m;
            burst-size-limit 15220;
        }
        then discard;
    }
}

routing-instances {

```

```

ELAN_Hub_Spoke_QinQ_AllVLAN {
  instance-type vpls;
  interface ge-5/0/2.1;
  route-distinguisher 65410:8;
  vrf-import ELAN_Hub_Spoke_QinQ_AllVLAN-import;
  vrf-export ELAN_Hub_Spoke_QinQ_AllVLAN-export;
  protocols {
    vpls {
      mac-table-size {
        5120;
      }
      interface-mac-limit {
        1024;
      }
      no-tunnel-services;
      site Site_1 {
        site-identifier 1;
        site-preference primary;
        interface ge-5/0/2.1;
      }
    }
  }
}

```

Related Documentation

- [Creating a Point-to-Multipoint VPLS Service Definition on page 678](#)
- [Predefined Point-to-Point Service Definitions on page 517](#)
- [Predefined Multipoint-to-Multipoint Ethernet Service Definitions on page 551](#)

Predefined Full Mesh Layer 3 VPN Service Definitions

The Connectivity Services Director application section provides information about predefined service definitions used for creating Layer 3 VPN full mesh services.

If neither of the predefined service definitions described here is appropriate for your needs, you can create a service definition as described in [“Creating a Full-Mesh Layer 3 VPN Service Definition” on page 709](#).

The Connectivity Services Director application provides predefined service definitions for Layer 3 VPN services that use the BGP or OSPF protocols.

Information specific to each service instance, such as the device name, endpoint name, VLAN ID, Interface IP, Peer AS (BGP), and whether you want to allow a service provisioner to create static routes on the service, is provided in the service order.

[Table 71 on page 590](#) lists each of the standard VPLS service definitions. Each standard service definition is then described in detail in the sections that follow.

Table 71: Standard Full-Mesh Layer 3 VPN Service Definitions

Standard Service Definition Name	Predefined Service Attributes
L3VPN-OSPF-STATIC L3 VPN (Full Mesh)	<ul style="list-style-type: none"> VLAN ID selection: Auto pick Route target: Auto pick Route distinguisher: Auto pick Allowed Routing Protocols: OSPF/Static Route
L3VPN-BGP-STATIC L3 VPN (Full Mesh)	<ul style="list-style-type: none"> VLAN ID selection : Auto pick Route target: Auto pick Route distinguisher: Auto pick Allowed Routing Protocols: BGP/Static Route

Related Documentation

- [Creating a Full-Mesh Layer 3 VPN Service Definition on page 709](#)
- [Predefined Service Definitions on page 465](#)
- [Predefined Point-to-Point Service Definitions on page 517](#)
- [Predefined Multipoint-to-Multipoint Ethernet Service Definitions on page 551](#)
- [Predefined Point-to-Multipoint Ethernet Service Definitions on page 576](#)
- [Predefined Hub-and-Spoke Layer 3 VPN Service Definitions on page 590](#)

Predefined Hub-and-Spoke Layer 3 VPN Service Definitions

The Connectivity Services Director application provides predefined service definitions that use BGP or OSPF routing protocols that you, the service provisioner, can use to create a service order. You must have a Service Designer user role to use Layer 3 VPN hub-and-spoke service definitions.

You view predefined and custom service definitions in the **Service Design > Manage Service Definitions** inventory page. You can view service definition details or attributes in the **Manage Service Definitions** inventory page by clicking the service definition.

You can also view service instance details by selecting **Service Provisioning > Deploy Services > Manage Service Orders** in Deploy mode of Service View.

[Table 72 on page 591](#) describes the predefined or standard hub-and-spoke (one interface) service definitions and their preconfigured service attributes. You can not reconfigure attributes in these predefined services. However, if you need custom attributes, create a new hub-and-spoke service definition to use, as described in the *Creating a Layer 3 VPN Hub-and-Spoke Service Definition* topic.

Table 72: Standard Hub-and-Spoke Service Definitions

Standard Service Definition Name	Description	Predefined Service Attributes
L3VPN-OSPF-Static (Hub-Spoke-1-Interface)	L3VPN Hub and Spoke 1 interface with OSPF/Static as PE-CE routing protocol	<ul style="list-style-type: none"> • VLAN ID selection: Auto pick This attribute is editable in the service order. • Route target: Auto pick • Pick VLAN within this range: N/A • Route target: Auto pick • Route distinguisher: Auto pick This attribute is editable in the service order. The VRF table label option is selected. • Allowed Routing Protocols: OSPF/Static Route
L3VPN-BGP-Static (Hub-Spoke-1-Interface)	L3VPN Hub and Spoke 1 interface with BGP/Static as PE-CE routing protocol	<ul style="list-style-type: none"> • VLAN ID selection: Auto pick This attribute is editable in the service order. • Route target: Auto pick • Pick VLAN within this range: N/A • Route target: Auto pick • Route distinguisher: Auto pick This attribute is editable in the service order. The VRF table label option is selected. • Allowed Routing Protocols: BGP/Static Route

- Related Documentation**
- [Viewing Service Definitions on page 650](#)
 - [Creating a Hub-and-Spoke \(One Interface\) Layer 3 VPN Service Definition on page 719](#)
 - [Creating a Full-Mesh Layer 3 VPN Service Definition on page 709](#)

CHAPTER 25

Service Design: Managing Point-to-Point Service Definitions

- [Choosing a Predefined Service Definition or Creating a New Service Definition on page 593](#)
- [Creating a Point-to-Point ATM or TDM Pseudowire Service Definition on page 618](#)
- [Creating a Point-to-Point Ethernet Service Definition on page 625](#)
- [Modifying a Custom Service Definition on page 646](#)
- [Publishing a Custom Service Definition on page 647](#)
- [Unpublishing a Custom Service Definition on page 648](#)
- [Deleting a Customized Service Definition on page 649](#)
- [Viewing Service Definitions on page 650](#)

Choosing a Predefined Service Definition or Creating a New Service Definition

The Connectivity Services Director software provides a set of predefined service definitions for point-to-point services, multipoint-to-multipoint (full mesh) services, and point-to-multipoint (hub and spoke) services. These service definitions are capable of providing the basis for most of the service orders your organization will need to create. In case these predefined service definitions are not adequate for all your needs, however, the Connectivity Services Director software enables you to create service definitions of your own.

The following topics review the predefined service definitions and provide instructions on creating your own.

- [Choosing a Predefined Service Definition on page 593](#)
- [Creating a Point-to-Point Ethernet Service Definition on page 599](#)

Choosing a Predefined Service Definition

[Table 73 on page 594](#) lists the predefined service definitions that Junos Space provides for Ethernet point-to-point services that use LDP in the network core. [Table 74 on page 596](#) lists the predefined service definitions for multipoint-to-multipoint (full mesh) services. [Table 71 on page 590](#) lists the predefined service definitions for point-to-multipoint (hub and spoke) services.

Table 73: Standard Ethernet Point-to-Point Service Definitions

Standard Service Definition Name	Service Attributes
ELine-Dot1q-SingleVLAN	<ul style="list-style-type: none"> Point-to-point service for M Series and MX Series devices Gigabit Ethernet interfaces 802.1Q endpoint circuit types Customer traffic is single VLAN Flexible-ethernet-services physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
ELine-Dot1q-SingleVLAN-CCC	<ul style="list-style-type: none"> Point-to-point service for J Series, M Series, and MX Series devices Gigabit Ethernet interfaces 802.1Q endpoint circuit types Customer traffic is single VLAN Vlan-ccc physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
ELine-Dot1q-SingleVLAN-Ext-CCC	<ul style="list-style-type: none"> Point-to-point service for J Series, M Series, and MX Series devices Gigabit Ethernet interfaces 802.1Q endpoint circuit types Customer traffic is single VLAN Extended-vlan-ccc physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
ELine-PortBased	<ul style="list-style-type: none"> Point-to-point service for J Series, M Series, and MX Series devices Gigabit Ethernet interfaces 802.1Q endpoint circuit types Port-based UNI Rate limiting default 10 Mbps
ELine-QinQ-AllVLAN	<ul style="list-style-type: none"> Point-to-point service for M Series and MX Series devices Gigabit Ethernet interfaces Q-in-Q endpoint circuit types All customer traffic Flexible-ethernet-services physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment

Table 73: Standard Ethernet Point-to-Point Service Definitions (continued)

Standard Service Definition Name	Service Attributes
ELine-QinQ-AllVLAN-CCC	<ul style="list-style-type: none"> Point-to-point service for J Series, M Series, and MX Series devices Gigabit Ethernet interfaces Q-in-Q endpoint circuit types All customer traffic Vlan-ccc physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
ELine-QinQ-AllVLAN-Ext-CCC	<ul style="list-style-type: none"> Point-to-point service for J Series, M Series, and MX Series devices Gigabit Ethernet interfaces Q-in-Q endpoint circuit types All customer traffic Extended-vlan-ccc physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
ELine-QinQ-VLANRange	<ul style="list-style-type: none"> Point-to-point service for MX Series devices only Gigabit Ethernet interfaces Q-in-Q endpoint circuit types Customer traffic is range of VLANs Flexible-ethernet-services physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
ELine-QinQ-VLANRange-CCC	<ul style="list-style-type: none"> Point-to-point service for MX Series devices only Gigabit Ethernet interfaces Q-in-Q endpoint circuit types Customer traffic is range of VLANs Vlan-ccc physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
ELine-QinQ-VLANRange-Ext-CCC	<ul style="list-style-type: none"> Point-to-point service for MX Series devices only Gigabit Ethernet interfaces Q-in-Q endpoint circuit types Customer traffic is range of VLANs Extended-vlan-ccc physical encapsulation Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment

Table 73: Standard Ethernet Point-to-Point Service Definitions (continued)

Standard Service Definition Name	Service Attributes
Eline-BGP-QinQ-AllVLAN	<ul style="list-style-type: none"> Ethernet service for M/MX/ACX device family Gigabit Ethernet interface Q-in-Q endpoint interface type Transport all traffic Flexible-ethernet-services physical encapsulation type Rate limit from 10 Mbps to 100 Mbps with 10 Mbps increment
Eline-BGP-Dot1q-SingleVLAN	<ul style="list-style-type: none"> Ethernet service for M/MX/ACX device family Gigabit Ethernet interface 802.1Q endpoint interface types Single VLAN traffic Flexible-ethernet-services physical encapsulation type Rate limit from 10 Mbps to 100 Mbps with 10 Mbps increment
Eline-BGP-PortBased	<ul style="list-style-type: none"> Ethernet service for M/MX/ACX device family Gigabit Ethernet interface Port-based UNIs Ethernet-ccc physical encapsulation type Rate limit from 10 Mbps to 100 Mbps with 10 Mbps increment

Table 74: Standard Multipoint-to-Multipoint Service Definitions

Standard Service Definition Name	Service Attributes
ELAN-BGP-Dot1q-Normalized-VLAN-None	<ul style="list-style-type: none"> Multipoint-to-multipoint Ethernet service for M Series and MX Series devices Gigabit Ethernet interfaces Customer VLAN IDs not preserved 802.1Q endpoint circuit types Customer traffic is single VLAN Flexible-ethernet-services physical encapsulation type Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment

Table 74: Standard Multipoint-to-Multipoint Service Definitions (continued)

Standard Service Definition Name	Service Attributes
ELAN-BGP-Dot1Q-SingleVLAN	<ul style="list-style-type: none"> • Multipoint-to-multipoint Ethernet service for M Series and MX Series devices • Gigabit Ethernet interfaces • 802.1Q endpoint circuit types • Customer traffic is single VLAN • Flexible-ethernet-services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
ELAN-BGP-PortBased	<ul style="list-style-type: none"> • Multipoint-to-multipoint Ethernet service for M series and MX Series devices • Gigabit Ethernet interfaces • Port-based UNIs • Transports all customer traffic • Ethernet VPLS as physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
ELAN-BGP-QinQ-AllVLAN	<ul style="list-style-type: none"> • Multipoint-to-multipoint Ethernet service for M Series and MX Series devices • Gigabit Ethernet interfaces • Q-in-Q endpoint circuit types • All customer traffic • Flexible-ethernet-services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
ELAN-BGP-QinQ-AllVLAN-Normalized-All	<ul style="list-style-type: none"> • Multipoint-to-multipoint Ethernet service for M Series and MX Series devices • Gigabit Ethernet interfaces • Customer VLAN IDs preserved • Q-in-Q endpoint circuit types • All customer traffic • Flexible-ethernet-services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment

Table 74: Standard Multipoint-to-Multipoint Service Definitions (continued)

Standard Service Definition Name	Service Attributes
ELAN-BGP-QinQ-AllVLAN-Normalized-None-10-100M	<ul style="list-style-type: none"> • Multipoint-to-multipoint Ethernet service for M Series and MX Series devices • Gigabit Ethernet interfaces • Q-in-Q endpoint circuit types • VLAN IDs not preserved • All customer traffic • Flexible-ethernet-services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
ELAN-BGP-QinQ-Range-Normalized-VLAN	<ul style="list-style-type: none"> • Multipoint-to-multipoint Ethernet service for M Series and MX Series devices • Gigabit Ethernet interfaces • Customer VLAN IDs preserved • Q-in-Q endpoint circuit types • Transports specified VLAN range • Flexible Ethernet services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment

Table 75: Standard Point-to-Multipoint Service Definitions

Standard Service Definition Name	Service Attributes
ELAN-Hub-Spoke-QinQ-AllVLAN	<ul style="list-style-type: none"> • Point to-multipoint Ethernet service for M Series and MX Series devices • Gigabit Ethernet interfaces • Customer VLAN IDs are not preserved • Q-in-Q endpoint interface types • All customer traffic • Flexible-ethernet-services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment
ELAN-Hub-Spoke-QinQ-AllVLAN-No	<ul style="list-style-type: none"> • Point-to-multipoint Ethernet service for M Series or MX Series devices • Gigabit Ethernet interfaces • Customer VLAN IDs are preserved • Q-in-Q endpoint interface types • All customer traffic • Flexible-ethernet-services physical encapsulation type • Rate limiting from 10 Mbps to 100 Mbps with 10 Mbps increment

Many of the service attributes can be edited in the service order, which allows the flexibility for creating most of the service orders you will need from these predefined service definitions.

To view the contents of a predefined service definition, follow these steps:

1. in the Network Services > Connectivity view pane, select **Service Design > Manage Service Definitions**.

The **Manage Service Definitions** page appears and shows all the service definitions present on your system.

2. Double click the predefined service definition you want to review.

Details of the service definition replace the **Manage Service Definitions** page.



TIP: If predefined and customized service definitions both exist on your system, you can easily find the predefined ones in the service definition inventory page.

3. When you are done reviewing the service definition, click **Back** to return to the **Manage Service Definitions** page.

For detailed descriptions of each of the predefined service definitions and their service attributes, see [“Predefined Service Definitions” on page 465](#)

Creating a Point-to-Point Ethernet Service Definition

Use this procedure to create a definition for a point-to-point VPN service. The standard service definitions that came with your initial software installation are designed to be appropriate for most requirements. You can also create a customized service definition—for example, to set different bandwidth limits on the service than those offered in the standard service definitions.

After the new service definition is complete and published, network operators or service provisioners can use the completed service definition as a base for creating and then activating point-to-point VPN services on the network.

The windows appear in the order stated. You can, however, perform these steps in any order by accessing them through the task list in the right panel. If the panel is not visible, click the snap tool on the right side of the main display area.

To create a point-to-point service definition, complete these tasks, in the order shown:

1. [Specifying General Information on page 600](#)
2. [Specifying UNI Settings on page 603](#)
3. [Specifying Connectivity Information When Signaling Is LDP on page 614](#)

4. [Specifying Connectivity Information When Signaling Is BGP on page 615](#)
5. [Reviewing the Configured Settings on page 617](#)

Specifying General Information

A wizard is available to create a service order in an intuitive and easily-navigable format. The settings that you can configure in the service order are organized in separate pages of the wizard, which you can launch by clicking the appropriate buttons at the top of the Create a Service Definition page. Alternatively, you can proceed to the corresponding setting-related pages by clicking the **Back** and **Next** buttons at any point in the wizard during the creation of the service definition.

To specify the general information for a point-to-point Ethernet service definition:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. in the Network Services > Connectivity view pane, select **Service Design > Manage Service Definitions**.
 - Select **Point-to-Point** to create a point-to-point service definition.
 - Select **VPLS** to create a VPLS service definition.
 - Select **L3 VPN** to create a Layer 3 VPN service definition.

The **Manage Service Definitions** page displays an inventory of all available point-to-point service definitions.

4. Click the **New** icon at the top of the lower half of the page that displays previously created service orders, and click **Point-to-Point** from the Select Service Type dialog box appears. The **General** settings window appears.
5. Fill in the fields in the **General** window.

Field	Action
Service Definition Name	Enter a name for the service definition.
Service type	By default, the service type is Point-to-Point Pseudowire .

Field	Action
Signaling	<p>Select a signaling type:</p> <ul style="list-style-type: none"> • BGP • LDP <p>You cannot edit the Signaling type in the service order.</p> <p>NOTE: If the signaling type is BGP, the Static pseudowire and the Enable PW access to L3 VPN network check boxes are not available. You cannot edit the Signaling type in the service order.</p>
Description (Optional)	<p>Enter a brief description or other comment that you want to appear in the Service Definition table.</p> <p>Range: 0 through 200 characters. Spaces and special characters are allowed.</p>
Enable QoS	<p>When you enable QoS in the service definition, you can specify a QoS profile in the service order to classify traffic into defined service groups to provide the special treatment of traffic across the network service. For example, voice traffic can be sent across certain links, and data traffic can use other links.</p>
Interface type	<p>Select the interface type:</p> <ul style="list-style-type: none"> • Ethernet • TDM • ATM
Static pseudowire	<p>To enable static pseudowire, select the Static pseudowire check box. This check box is disabled if the signaling type is BGP.</p>
Enable PW access to L3 VPN network	<p>To enable the pseudowire access to L3 VPN network, select the Enable PW access to L3 VPN network check box. This check box is disabled if the signaling type is BGP, or if you have selected the interface type as TDM/ATM.</p> <p>If you select this check box, the Enable Multi Segment Pseudowire check box is disabled.</p>
Enable Multi Segment Pseudowire	<p>Select this check box to enable multi-segment pseudowire.</p> <p>If you select this check box, the Enable PW access to L3 VPN network check box is disabled.</p> <p>A multi-segment pseudowire (MS-PW) is a static or dynamically configured set of two or more contiguous pseudowire segments that behave and function as a single point-to-point pseudowire. Each end of an MS-PW, by definition, terminates on a T-PE.</p> <p>NOTE: The number of pseudowire segments that you can stitch is limited to two.</p> <p>For more information on point-to-point pseudowire stitching, see "Stitching Two Point-to-Point Pseudowires" on page 858.</p>

Field	Action
Enable PW Resiliency	To enable the pseudowire resiliency, select the Enable PW Resiliency check box. For more information on pseudowire redundancy, see “Redundant Pseudowires for Layer 2 Circuits and VPLS” on page 94.
Decouple Service Status From Port Status	<p>By default, all the events are saved in the OpenNMS database. To isolate the events related to an interface in the OpenNMS, select the Decouple Service Status From Port Status check box.</p> <p>NOTE: When you select this check box, only the pseudowire traps are monitored, and not the interface-related traps (such as jnxVpnIfUp or jnxVpnIfDown).</p>
Service Template	<p>(Optional) To include a service template for the service, click the Add icon or plus sign (+) to select a service template from the Service Template list. The list of available service templates is displayed. Select the check box beside the template you want and click OK. You are returned to the General Settings page.</p> <p>The selected service template appears in the Default Service Template field.</p> <p>You can select one or more service templates as the default service template. By default, the default service templates are attached to the endpoints.</p> <p>NOTE: You cannot add or delete a service template while creating a service order.</p> <p>The remaining service templates on the Service Template list are termed as optional service templates. You can attach the optional service templates to the endpoints on a need basis.</p> <p>In the View Service Definition Details window, the value for the default service template in the Default Service Template column is <i>True</i>.</p> <p>For instructions on creating a service template, see “Creating a Service Template” on page 1815.</p>
Threshold alarm profile	If you intend to run performance tests on services based on this service definition, select a TCA Profile .

- Click **Next** to save the information. You can proceed to [“Specifying UNI Settings” on page 603.](#)

Specifying UNI Settings

In this step, you provide the UNI service attributes for this service definition. The attributes you set depend on whether you are setting attributes for a port, an 802.1Q interface, a Q-in-Q interface, or a flexible VLAN tagging:

- [Specifying UNI Settings for Port-to-Port Services on page 603](#)
- [Specifying UNI Settings for Services with 802.1Q Interface Types on page 605](#)
- [Specifying UNI Settings for Services with Q-in-Q Interface Types on page 608](#)
- [UNI Settings for Services with Flexible VLAN Tagging \(Asymmetric Interface Types\) on page 611](#)

Specifying UNI Settings for Port-to-Port Services

To set UNI attributes for a port-to-port service, complete the following procedure.

1. Enter information in the UNI Settings window.
2. Fill in the fields in the **UNI Settings** window according to the following table.

Field	Action
Traffic Treatment Settings	
Ethernet option	<p>Select port-port from the list.</p> <p>The Ethernet option you choose determines the other options you can select and specify on the page.</p>
Customer traffic type	Select N/A . For port-to-port services, all traffic is always transported.
VLAN ID selection	In port-to-port services, all traffic and all VLANs on one port are transported to all other ports.
Editable in Service Order	Select this check box to allow the service provisioner to override the MTU setting.
Interface Settings	
Physical IF encapsulation	Select ethernet-vpls , the only valid physical interface encapsulation method allowed for port-to-port services.
Logical IF encapsulation	You cannot change this field because it is not relevant to port-to-port services.
MTU Settings	
Default MTU (Bytes)	<p>You can specify an MTU value in this field. The default value for MTU is 1522 bytes.</p> <p>To see the permitted range for the MTU value, select the Editable in Service Order check box. The MTU range is 1522 through 9192.</p>

Field	Action
MTU Range (Bytes)	<p>If you select the check box Editable in Service Order, you can specify a value range for MTU (in bytes). The permitted range for MTU is 1522 through 9192.</p> <p>NOTE: Ultimately, the system establishes the MTU by multiplying the value you specify in the Default MTU (Bytes) field by the value you specify for MTU Factor.</p>
Calculation of Burst-Size	
Calculate Burst Size	<p>Select the preferred option for calculating the burst size:</p> <ul style="list-style-type: none"> MTU Based If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902. The default value for MTU Factor is 10. Line Rate Based If you select the option Line Rate Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds. The default value for Burst Period is 1. <p>NOTE: The Calculate Burst Size list is enabled only when you select the Enable rate limiting check box.</p>
Bandwidth Settings	
Enable rate limiting (check box)	If you select this check box, you can override the MTU setting.
Default bandwidth (Mbps)	<p>Specify the default bandwidth value, in Mbps.</p> <p>Default: 10 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps</p>
Min Bandwidth (Kbps)	<p>To override the default bandwidth value, select the Editable in Service Order check box.</p> <p>Specify the minimum bandwidth value in Kbps:</p> <p>Default: 1000 Kbps</p> <p>Range: 64 Kbps through 100,000 Kbps</p>
Max Bandwidth (Mbps)	<p>Specify the maximum bandwidth value, in Mbps.</p> <p>Default: 100 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps</p>

Field	Action
-------	--------

The following table lists the **Max Bandwidth (Mbps)** for the M Series, MX Series, and ACX Series Routers:

Table 76: Maximum Bandwidth for M Series, MX Series, and ACX Series Routers

M Series IQ2E PIC		M Series IQ2 PIC		MX Series 3D PIC		MX Series Non-3D PIC		ACX 2000	
GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)
32,000 Mbps or 32 Gbps	32,000 Mbps or 32 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps	100,000 Mbps or 100 Gbps	100,000 Mbps or 100 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps

Increment (Kbps)	Specify a value in the range that is made available to the service provisioner.
------------------	---

- Click **Next** to proceed to specify the connectivity settings.

Specifying UNI Settings for Services with 802.1Q Interface Types

To set UNI attributes for a 802.1Q service, complete the following procedure.

- To set UNI attributes for 802.1Q interfaces:
- Fill in the fields in the **UNI Settings** window according to the following table:

Field	Action
-------	--------

Traffic Treatment Settings

Ethernet option

Select **dot1q** from the list.

The window expands to include options specific to dot1q interfaces.

Customer traffic type

Single VLAN is the only option for 802.1Q interface types.

- Select **Transport single vlan** to transport traffic for a specific VLAN across the network. When you select this option, the service provisioner is prompted for the VLAN-ID when creating a service order based on this service definition. You need to specify the **Outer Tag protocol ID**.
- Select **Transport VLAN range** to limit the traffic across the network to a specific range of VLANs. If you select this option, the service provisioner is prompted for the VLAN-ID range when creating a service order based on this service definition. You need to specify both **Outer Tag protocol ID** and **Inner Tag protocol ID**.

NOTE: Make sure to check **Editable in Service Order** if you want the service provisioner to be able to override this setting.

Field	Action
VLAN ID selection	<p>Indicate how the VLAN ID is selected during service order creation.</p> <ul style="list-style-type: none"> • Select manually—Allows the service provider to specify the VLAN ID. This option is normally used when no VLAN normalization is applied. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting. Specify the VLAN ID range in VLAN range for manual input.</p> <ul style="list-style-type: none"> • Auto pick—This option is normally used when VLAN normalization is applied. Specify the VLAN ID pool in VLAN range for auto-pick. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p> <p>NOTE: When the range of VLAN IDs that are automatically assigned by the system (with the auto-pick option enabled during the creation of a service definition) is less than or greater than the range of VLAN IDs that are manually specified (with the manual selection option enabled during the creation of a service definition), the following conditions apply during the creation of a service order with the Editable in Service Order check box selected during service definition creation:</p> <ul style="list-style-type: none"> • If you create a service order with the auto-pick option enabled, the VLAN ID is selected from the auto-pick range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range. • If you create a service order with the auto-pick option disabled, the VLAN ID is selected from the manually configured range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range.
VLAN range for auto-pick	<p>Specify the VLAN ID pool.</p> <p>Range: 1 through 4094</p>
VLAN range for manual input	<p>Specify the VLAN ID range.</p> <p>Range: 1 through 4094</p>
Outer Tag protocol ID	<p>Select the outer tag protocol ID if the Customer traffic type is Transport single VLAN:</p> <ul style="list-style-type: none"> • 0x88a8 • 0x8100 • 0x9100 <p>NOTE: For an interface, you must configure a physical port with the possible Tag Protocol Identifiers (TPIDs) either manually or through a template. Otherwise, the service creation fails for all TPIDs except 0x8100. To configure the TPIDs manually, use the following commands:</p> <pre>set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x9100 set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x88a8 set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x8100</pre>

Field	Action
Inner Tag protocol ID	<p>Select the inner tag protocol ID:</p> <ul style="list-style-type: none"> • 0x88a8 • 0x8100 • 0x9100 <p>NOTE: You cannot specify the Inner Tag protocol ID if the Customer traffic type is Transport single VLAN.</p>
Editable in Service Order	Select this check box to allow the service provisioner to override the MTU setting.
Interface Settings	
Physical IF encapsulation	Select the default physical encapsulation scheme to be used by service orders based on this service definition. We recommend you select flexible-ethernet-services .
Logical IF encapsulation	Constrained by your selection in the Physical IF encapsulation box. If you selected the recommended physical encapsulation mode of flexible-ethernet-services, then your only option is to select vlan-vpls for the logical encapsulation method.
MTU Settings	
Default MTU (Bytes)	<p>You can specify an MTU value in this field. The default value for MTU is 1522.</p> <p>To see the permitted range for the MTU value, select the Editable in Service Order check box. The MTU range is 1522 through 9192.</p>
MTU Range (Bytes)	<p>If you select the check box Editable in Service Order, you can specify a value range for MTU (in bytes). The permitted range for MTU is 1522 through 9192.</p> <p>NOTE: Ultimately, the system establishes the MTU by multiplying the value you specify in the Default MTU (Bytes) field by the value you specify for MTU Factor.</p>
Calculation of Burst-Size	
Calculate Burst Size	<p>Select the preferred option for calculating the burst size:</p> <ul style="list-style-type: none"> • MTU Based If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902. The default value for MTU Factor is 10. • Line Rate Based If you select the option Line Rate Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds. The default value for Burst Period is 1. <p>NOTE: The Calculate Burst Size list is enabled only when you select the Enable rate limiting check box.</p>

3. Click **Next** to continue with connectivity settings.

Specifying UNI Settings for Services with Q-in-Q Interface Types

To set UNI attributes for a Q-in-Q service, complete the following procedure.

1. To set UNI attributes for Q-in-Q interfaces:
2. Fill in the fields in the **UNI Settings** window according to the following table:

Field	Action
Traffic Treatment Settings	
Ethernet option	<p>Select qinq from the list.</p> <p>The window expands to include options specific to Q-in-Q interfaces.</p>
Customer traffic type	<p>Specify the customer traffic type:</p> <ul style="list-style-type: none">• Transport all traffic—Transports the traffic from all VLANs across the network. When you select this option, the service provisioner is prompted for the VLAN-ID when creating a service order based on this service definition. You need to specify only the Outer Tag protocol ID.• Transport single vlan—Transports traffic for a specific VLAN across the network. You need to specify both Outer Tag protocol ID and Inner Tag protocol ID.• Transport VLAN range—Limits the traffic across the network to a specific range of VLANs. If you select this option, the service provisioner is prompted for the VLAN-ID range when creating a service order based on this service definition. You need to specify both Outer Tag protocol ID and Inner Tag protocol ID. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p>

Field	Action
VLAN ID selection	<p>Indicate how the VLAN ID is selected during service order creation.</p> <ul style="list-style-type: none"> • Select manually—Allows the service provider to specify the VLAN ID. This option is normally used when no VLAN normalization is applied. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting. Specify the VLAN ID range in VLAN range for manual input.</p> <ul style="list-style-type: none"> • Auto pick—This option is normally used when VLAN normalization is applied. Specify the VLAN ID pool in VLAN range for auto-pick. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p> <p>NOTE: When the range of VLAN IDs that are automatically assigned by the system (with the auto-pick option enabled during the creation of a service definition) is less than or greater than the range of VLAN IDs that are manually specified (with the manual selection option enabled during the creation of a service definition), the following conditions apply during the creation of a service order with the Editable in Service Order check box selected during service definition creation:</p> <ul style="list-style-type: none"> • If you create a service order with the auto-pick option enabled, the VLAN ID is selected from the auto-pick range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range. • If you create a service order with the auto-pick option disabled, the VLAN ID is selected from the manually configured range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range.
VLAN range for auto-pick:	<p>Specify the VLAN ID pool.</p> <p>Range: 1 through 4094</p>
VLAN range for manual input	<p>Specify the VLAN ID range.</p> <p>Range: 1 through 4094</p>
Outer Tag protocol ID	<p>Select the outer tag protocol ID if the Customer traffic type is Transport single VLAN:</p> <ul style="list-style-type: none"> • 0x88a8 • 0x8100 • 0x9100 <p>NOTE: For an interface, you must configure a physical port with the possible Tag Protocol Identifiers (TPIDs) either manually or through a template. Otherwise, the service creation fails for all TPIDs except 0x8100. To configure the TPIDs manually, use the following commands:</p> <pre>set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x9100 set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x88a8 set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x8100</pre>

Field	Action
Inner Tag protocol ID	<p>Select the inner tag protocol ID:</p> <ul style="list-style-type: none"> • 0x88a8 • 0x8100 • 0x9100 <p>NOTE: You cannot specify the Inner Tag protocol ID if the Customer traffic type is Transport single VLAN.</p>
Editable in Service Order	Select this check box to allow the service provisioner to override the MTU setting.
Interface Settings	
Physical IF encapsulation	Select the default physical encapsulation scheme to be used by service orders based on this service definition. We recommend you select flexible-ethernet-services .
Logical IF encapsulation	Constrained by your selection in the Physical IF encapsulation box. If you selected the recommended physical encapsulation mode of flexible-ethernet-services, then your only option is to select vlan-vpls for the logical encapsulation method.
MTU Settings	
Default MTU (Bytes)	<p>You can specify an MTU value in this field. The default value for MTU is 1522.</p> <p>To see the permitted range for the MTU value, select the Editable in Service Order check box. The MTU range is 1522 through 9192.</p>
MTU Range (Bytes)	<p>If you select the check box Editable in Service Order, you can specify a value range for MTU (in bytes). The permitted range for MTU is 1522 through 9192.</p> <p>NOTE: Ultimately, the system establishes the MTU by multiplying the value you specify in the Default MTU (Bytes) field by the value you specify for MTU Factor.</p>
Calculation of Burst-Size	
Calculate Burst Size	<p>Select the preferred option for calculating the burst size:</p> <ul style="list-style-type: none"> • MTU Based If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902. The default value for MTU Factor is 10. • Line Rate Based If you select the option Line Rate Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds. The default value for Burst Period is 1. <p>NOTE: The Calculate Burst Size list is enabled only when you select the Enable rate limiting check box.</p>

3. Click **Next** to continue with connectivity settings.

UNI Settings for Services with Flexible VLAN Tagging (Asymmetric Interface Types)

You can specify the Ethernet option **asymmetric tag depth** to create a service that includes any combination of port-based interfaces, 802.1Q interfaces, and Q-in-Q interfaces.

1. Enter information in the UNI Settings window.
2. Specify the UNI Settings for asymmetric tag depth according to the following table:

Field	Action
Traffic Treatment Settings	
Ethernet option	Select asymmetric tag depth from the list.
Customer traffic type	<p>Select the customer traffic type:</p> <ul style="list-style-type: none"> • Transport all traffic—Transports the traffic from all VLANs across the network. When you select this option, the service provisioner is prompted for the VLAN-ID when creating a service order based on this service definition. You need to specify only the Outer Tag protocol ID and Inner Tag protocol ID. • Transport single vlan—Transports traffic for a specific VLAN across the network. You need to specify both Outer Tag protocol ID and Inner Tag protocol ID. • Transport VLAN range—Limits the traffic across the network to a specific range of VLANs. You need to specify both Outer Tag protocol ID and Inner Tag protocol ID. <p>If you select this option, the service provisioner is prompted for the VLAN-ID range when creating a service order based on this service definition.</p> <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p>

Field	Action
VLAN ID selection	<p>Indicate how the VLAN ID is selected during service order creation.</p> <ul style="list-style-type: none"> Select manually—Allows the service provider to specify the VLAN ID. This option is normally used when no VLAN normalization is applied. Specify the VLAN ID range in VLAN range for manual input. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p> <ul style="list-style-type: none"> Auto pick—This option is normally used when VLAN normalization is applied. Specify the VLAN ID pool in VLAN range for auto-pick. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting. Specify the VLAN ID pool in VLAN range for auto-pick.</p> <p>NOTE: When the range of VLAN IDs that are automatically assigned by the system (with the auto-pick option enabled during the creation of a service definition) is less than or greater than the range of VLAN IDs that are manually specified (with the manual selection option enabled during the creation of a service definition), the following conditions apply during the creation of a service order with the Editable in Service Order check box selected during service definition creation:</p> <ul style="list-style-type: none"> If you create a service order with the auto-pick option enabled, the VLAN ID is selected from the auto-pick range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range. If you create a service order with the auto-pick option disabled, the VLAN ID is selected from the manually configured range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range.
VLAN range for auto-pick:	<p>Specify the VLAN ID pool.</p> <p>Range: 1 through 4094</p>
VLAN range for manual input	<p>Specify the VLAN ID range.</p> <p>Range: 1 through 4094</p>
Outer Tag protocol ID	<p>Select the outer tag protocol ID if the Customer traffic type is Transport single VLAN:</p> <ul style="list-style-type: none"> 0x88a8 0x8100 0x9100 <p>NOTE: For an interface, you must configure a physical port with the possible Tag Protocol Identifiers (TPIDs) either manually or through a template. Otherwise, the service creation fails for all TPIDs except 0x8100. To configure the TPIDs manually, use the following commands:</p> <pre>set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x9100 set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x88a8 set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x8100</pre>

Field	Action
Inner Tag protocol ID	<p>Select the inner tag protocol ID:</p> <ul style="list-style-type: none"> • 0x88a8 • 0x8100 • 0x9100 <p>NOTE: You cannot specify the Inner Tag protocol ID if the Customer traffic type is Transport all traffic.</p>
Editable in Service Order	To allow the service provisioner to override the MTU setting, select the check box for those options.
Interface Settings	
Physical IF encapsulation	Select the default physical encapsulation scheme to be used by service orders based on this service definition. We recommend you select flexible-ethernet-services .
Logical IF encapsulation	Constrained by your selection in the Physical IF encapsulation box. If you selected the recommended physical encapsulation mode of flexible-ethernet-services, then your only option is to select vlan-vpls for the logical encapsulation method.
MTU Settings	
Default MTU (Bytes)	<p>You can specify an MTU value in this field. The default value for MTU is 1522.</p> <p>To see the permitted range for the MTU value, select the Editable in Service Order check box. The MTU range is 1522 through 9192.</p>
MTU Range (Bytes)	<p>If you select the check box Editable in Service Order, you can specify a value range for MTU (in bytes). The permitted range for MTU is 1522 through 9192.</p> <p>NOTE: Ultimately, the system establishes the MTU by multiplying the value you specify in the Default MTU (Bytes) field by the value you specify for MTU Factor.</p>
Calculation of Burst-Size	
Calculate Burst Size	<p>Select the preferred option for calculating the burst size:</p> <ul style="list-style-type: none"> • MTU Based If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902. The default value for MTU Factor is 10. • Line Rate Based If you select the option Line Rate Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds. The default value for Burst Period is 1. <p>NOTE: The Calculate Burst Size list is enabled only when you select the Enable rate limiting check box.</p>

3. Click **Next** to continue with specifying the connectivity settings.

Specifying Connectivity Information When Signaling Is LDP

The fields displayed in the **Connectivity** window depend on the **Signaling type** (LDP or BGP) that you selected in the **General** settings window.

To specify connectivity between sites across the network when signaling is LDP:

1. Fill in the fields in the **Connectivity** window.

Field	Action
VC ID selection	<p>The VC ID selection is available only if the Signaling type is LDP.</p> <p>In the VC ID selection box, specify how you want the VC ID to be chosen during service order creation:</p> <ul style="list-style-type: none"> • To allow the service provisioner to enter the VC ID, choose Select manually. • To cause the Junos Space software to assign a VC ID automatically from the VC ID pool, select Auto pick. <p>To allow the service provisioner to override the setting in the VC ID box, select Editable in Service Order.</p>
Default MTU	<p>In the Default MTU box, specify the MTU across the service provider network.</p> <p>To allow the service provisioner to override the MTU setting, select Editable in Service Order. In the MTU range, enter the highest and lowest MTU that the service provisioner can enter.</p>
Revert time (sec)	<p>This field is available if you selected the Enable PW Resiliency check box and if the Signaling is LDP in the General settings.</p> <p>Revert time (sec)—Revert time for redundant Layer 2 circuits and VPLS pseudowires.</p> <p>Default: 5 seconds</p> <p>Range: 0 through 65,535 seconds</p>
Switch Over Delay (sec)	<p>This field is available if you selected the Enable PW Resiliency check box and if the Signaling is LDP, in the General settings.</p> <p>Switch Over Delay (sec)—Delay to wait before the backup pseudowire takes over.</p> <p>Default: 0 second</p> <p>Range: 0 through 180 seconds</p>
VLAN Normalization	<p>The options available in the VLAN normalization drop-down list are based on the value set for the Ethernet interface.</p>
Outgoing label selection	<p>This field is available if you selected the Static pseudowire check box in the General settings. By default, the outgoing label selection is limited to manual.</p>

The following table presents the available **VLAN normalization** options:

Ethernet Option	Customer Traffic Type	VLAN Normalization
port-port	N/A	Normalization not required
		Normalization to Dot1q tag
		Normalization to QinQ tags
dot1q	Transport single vlan	Swap
		Normalize to None
		Normalization to Dot1q tag
		Normalization to QinQ tags
	Transport vlan range	Normalization not required
qinq	Transport all traffic	Swap
		Normalize to None
		Normalization to Dot1q tag
		Normalization to QinQ tags
	Transport single vlan	Swap
		Normalize to None
		Normalization to Dot1q tag
		Normalization to QinQ tags
	Transport vlan range	Normalization not required
Asymmetric	(Identical to qinq)	(Identical to qinq)

2. Click **Finish** to complete the service definition.

Specifying Connectivity Information When Signaling Is BGP

To specify connectivity between sites across the network when signaling is BGP, fill in the fields in the Connectivity window:

1. When the signaling type is BGP, fill in the fields in the **Connectivity** window.

- **Route Distinguisher**—Identifier attached to a route, enabling you to distinguish to which VPN the route belongs. Each routing instance must have a unique route distinguisher associated with it.

Range: 1.1.1.1 through 255.255.255.254:65535, or 1:1 through 65535:4294967295

- **Route Target**—Allows you to distribute VPN routes to only the routers that need them.

Range: 1.1.1.1 through 255.255.255.254:65535, or 1:1 through 65535:4294967295

- **Default MTU (Bytes)**—The default MTU established by the system.
- **MTU range (Bytes)**—Specify the range, in bytes, for the MTU.
- **VLAN normalization**—The options available in the **VLAN normalization** field are based on the value set for the Ethernet interface. The following table presents the options.

Ethernet Option	Customer Traffic Type	VLAN Normalization
port-port	N/A	Normalization not required Normalization to Dot1q tag Normalization to QinQ tags
dot1q	Transport single vlan	Swap Normalize to None Normalization to Dot1q tag Normalization to QinQ tags
	Transport vlan range	Normalization not required
qinq	Transport all traffic	Swap Normalize to None Normalization to Dot1q tag Normalization to QinQ tags
	Transport single vlan	Swap Normalize to None Normalization to Dot1q tag Normalization to QinQ tags
	Transport vlan range	Normalization not required
Asymmetric	(Identical to qinq)	(Identical to qinq)



NOTE: For a description of how the Connectivity Services Director software manipulates VLANs, see [“Understanding VLAN Manipulation \(Normalization and VLAN Mapping\) on Ethernet Services” on page 88.](#)

2. Click **Review** to analyze and verify the configured attributes for the service definition.

Reviewing the Configured Settings

The Review page of the service definition or service order creation and modification wizards enable you to view and evaluate the service parameters and components you configured in preceding steps or pages of the wizard. This page provides a comprehensive, single-page view of all the service elements configured in the different pages of the wizard. You can either click the buttons corresponding to the various settings at the top of the wizard page to directly traverse to the page you want to modify or click the

navigation buttons at the bottom of the wizard page to go to the different pages of the wizard.



NOTE: On the Review page, in the Service Templates section, the names of the service templates with which the service definition is associated are displayed. The Default Service Template column indicates whether the attached template is the default template.

To examine and modify the configured service definition settings:

1. Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify.
2. Click **Edit** next to the section that contains the parameter you want to modify. You are navigated to the corresponding page of the wizard in which the parameter settings are defined.
3. Click **Finish** to save the service definition or service order.
4. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

When the service definition is successfully created, you are returned to the Manage Service Definitions window.

**Related
Documentation**

- [Creating a Point-to-Point ATM or TDM Pseudowire Service Definition on page 618](#)
- [Creating a Point-to-Point Ethernet Service Definition on page 625](#)
- [Publishing a Custom Service Definition on page 647](#)
- [Unpublishing a Custom Service Definition on page 648](#)
- [Deleting a Customized Service Definition on page 649](#)
- [Viewing Service Definitions on page 650](#)

Creating a Point-to-Point ATM or TDM Pseudowire Service Definition

This procedure provides the steps to create a definition for a point-to-point ATM or TDM service. The standard service definitions that came with your initial software installation are designed to be appropriate for most requirements. You can also create a customized service definition—for example, to set different bandwidth limits on the service than those offered in the standard service definitions.

After the new service definition is complete and published, network operators or service provisioners can use the completed service definition as a base for creating and then activating point-to-point ATM or TDM services on the network.

The windows appear in the order shown. You can, however, perform these steps in any order by accessing them through the task list in the right panel. If the panel is not visible, click the snap tool on the right side of the main display area.

To create a point-to-point service definition, complete these tasks, in the order shown:

1. [Specifying General Information for the ATM or TDM Service on page 619](#)
2. [Specifying UNI Settings for ATM and TDM Service Definitions on page 621](#)
3. [Specifying UNI Settings for ATM Interfaces on page 621](#)
4. [Specifying UNI Settings for TDM Interfaces on page 621](#)
5. [Specifying Connectivity Information for an ATM or a TDM Service on page 622](#)
6. [Reviewing the Configured Settings on page 624](#)

Specifying General Information for the ATM or TDM Service

1. In the Build mode of the Network Services > Connectivity task pane, select **Service Design > Manage Service Definitions > New > P2P Service Definition**.

The first **Create Point-to-Point Service Definition** window appears.

2. In the **Name** box, type a name for the service definition.

3. Select the signaling type:

- LDP
- BGP



NOTE: If the signaling type is BGP, the **Static pseudowire**, **Enable PW Resiliency**, **Enable Multi Segment Pseudowire** and the **Enable PW access to L3 VPN network** check boxes are not available.

4. (Optional) In the **Description** box, type a brief description or other comment that you want to appear in the Service Definition table.
5. (Optional) To include a service template for the service, click the **Add** icon or plus sign (+) to select a service template from the Service Template list. The list of available service templates is displayed. Select the check box beside the template you want and click **OK**. You are returned to the General Settings page.

The selected service template appears in the **Default Service Template** field.

You can select one or more service templates as the default service template. By default, the default service templates are attached to the endpoints.



NOTE: You cannot add or delete a service template while creating a service order.

The remaining service templates on the **Service Template** list are termed as optional service templates. You can attach the optional service templates to the endpoints on a need basis.

In the View Service Definition Details window, the value for the default service template in the Default Service Template column is *True*.

For instructions on creating a service template, see [“Creating a Service Template” on page 1815](#).

6. Select the interface type. If you select TDM or ATM as the interface type, the **Enable PW access to L3 VPN network** check box is unavailable.

7. Select the **Enable Multi Segment Pseudowire** check box to enable multi-segment pseudowire. This check box is available for LDP signaling only

A multi-segment pseudowire is a static or dynamically configured set of two or more contiguous pseudowire segments that behave and function as a single point-to-point pseudowire. Each end of a multi-segment pseudowire, by definition, terminates on a T-PE.



NOTE: The number of pseudowire segments that you can stitch is limited to two.

For more information on point-to-point pseudowire stitching, see [“Stitching Two Point-to-Point Pseudowires” on page 858](#).

8. Select the **Static pseudowire** check box to indicate whether the point-to-point service definition is a static pseudowire.
9. To enable the pseudowire resiliency, select the **Enable PW Resiliency** check box. For more information on pseudowire redundancy, see [“Redundant Pseudowires for Layer 2 Circuits and VPLS” on page 94](#).
10. By default, all the events are saved in the OpenNMS database. To isolate the events related to an interface in the OpenNMS, select the **Decouple Service Status From Port Status** check box.



NOTE: When you select this check box, only the pseudowire traps are monitored, and not the interface-related traps (such as `jnxVpnIfUp` or `jnxVpnIfDown`).

11. Click **Next** to continue to the **Connectivity Settings** window.

Specifying UNI Settings for ATM and TDM Service Definitions

In this step, you provide the UNI service attributes for this service definition. The attributes you set depend on whether you are setting attributes for an ATM or for a TDM interface.

Specifying UNI Settings for ATM Interfaces

To specify the UNI settings for ATM interfaces:

1. Fill in the fields as indicated in the table.

Field	Action
Physical IF encapsulation	Select the type of encapsulation to apply to the interface. Use <code>atm-ccc-cell-relay</code> for ATM cell relay encapsulation. Use <code>atm-ccc-cell-mux</code> for ATM VC for CCC.
VPI selection	Select the virtual path identifier (VPI). The combination of the VPI and VCID defines the next destination for a cell in the ATM network.
VCID selection	Select the virtual channel identifier (VCID)—This integer uniquely identifies the virtual circuit that the service uses. The VCID can be either set automatically by the Junos Space software, or the service provisioner can set it manually in the service order. The service definition can force the system to pick the VCID, force the service provisioner to pick the VCID, or allow the service provisioner to override the settings in the service definition. We recommend allocating the VCID automatically; however, service providers with their own systems for allocating VCIDs may choose the manual setting. In the previous example, by default, the system picks a VCID from its pool automatically, but allows the service provisioner to override this value in the service order. Clear the check box to override the service definition setting. The form expands to include an additional field for entering the VCID manually.
Cell bundle size	The range for the cell bundle size can be 1 through 34.

2. Click **Next** to go to the **Connectivity Settings** window.

Specifying UNI Settings for TDM Interfaces

To specify the UNI settings for TDM interfaces:

1. Select the type of **Physical IF encapsulation**.

- SAToP—Structure-Agnostic time-division multiplexing (TDM) over Packet (SAToP), as defined in RFC 4553, Structure-Agnostic TDM over Packet (SAToP) is used for pseudowire encapsulation for TDM bits (T1, E1). The encapsulation disregards any structure imposed on the T1 and E1 streams, in particular the structure imposed by standard TDM framing. SAToP is used over packet-switched networks, where the provider edge (PE) routers do not need to interpret TDM data or participate in the TDM signaling.
- CESoPSN—Circuit Emulation Service over Packet-Switched Network (CESoPSN) bundle represents an IP circuit emulation flow. With CESoPSN bundles, you can group multiple DSOs on one IP circuit, and you can have more than one circuit emulation IP flow created from a single physical interface. For example, some DSO channels from a T1 interface can go in an IP flow to destination A, and other DSO channels from that same T1 interface can go to destination B.



NOTE: The Physical IF encapsulation is not editable in service order.

2. Fill in the SAToP and CESoPSN fields as indicated in the table.

SAToP Field	Value Range	Default Value
Jitter buffer	M Series: 1 through 340	5
		There is no default value for the jitter buffer on BX7000 Gateway devices. You must specify a value.
Idle pattern	0 through 255	255
Excessive packet loss rate	1 through 100%	20%
Payload size	M Series: 64 through 1024	192
NOTE: If the Physical IF encapsulation type is CESoPSN, the Payload size is unavailable.		NOTE: For M Series, the value you specify must be a multiple of 32.

3. Click **Next** to go to the **Connectivity Settings** window.

Specifying Connectivity Information for an ATM or a TDM Service

In this step, you specify the attributes that define the connectivity between remote sites across the service provider network. A sample window follows.

1. Provide the following information to create connectivity between sites across the network:

Field	Action
VC ID selection	<p>This box is available only if the Signaling is LDP.</p> <p>Specify how you want the VC ID chosen during service order creation:</p> <ul style="list-style-type: none"> • To allow the service provisioner to type the VC ID, choose Select manually. • To cause the Junos Space software to assign a VC ID automatically from the VC ID pool, select Auto pick. <p>To allow the service provisioner to override the setting in the VC ID box, select Editable in Service Order.</p>
Default MTU (Bytes)	<p>Specify the MTU across the service provider network.</p> <p>To allow the service provisioner to override the MTU setting, select Editable in Service Order.</p>
MTU range (Bytes)	<p>Specify the highest and lowest MTU that the service provisioner can type.</p> <p>Range: 1522 bytes through 9192 bytes</p>
Revert time (sec)	<p>This box is available only if the Signaling is LDP.</p> <p>Revert time for redundant Layer 2 circuits and VPLS pseudowires.</p> <p>Default: 5 seconds</p> <p>Range: 0 through 65,535 seconds</p>
Switch Over Delay (sec)	<p>This box is available only if the Signaling type is LDP.</p> <p>Specify the delay to wait before the backup pseudowire takes over.</p> <p>Default: 0 second</p> <p>Range: 0 through 180 seconds</p>
Route Distinguisher	<p>This box is available only if the Signaling type is BGP.</p> <p>Specify an identifier attached to a route, enabling you to distinguish to which VPN the route belongs. Each routing instance must have a unique route distinguisher associated with it.</p> <p>Range: 1.1.1.1 through 255.255.255.254:65535, or 1:1 through 65535:4294967295</p>
Route Target	<p>This box is available only if the Signaling is BGP.</p> <p>Allows you to distribute VPN routes to only the routers that need them.</p> <p>Range: 1.1.1.1 through 255.255.255.254:65535, or 1:1 through 65535:4294967295</p>
Outgoing label selection	<p>This field is available only if you have selected the Static pseudowire check box in the General settings. By default, the outgoing label selection is limited to manual.</p>

2. Click **Review** to examine the settings configured for the point-to-point ATM/TDM service definition.

Reviewing the Configured Settings

The Review page of the service definition or service order creation and modification wizards enable you to view and evaluate the service parameters and components you configured in preceding steps or pages of the wizard. This page provides a comprehensive, single-page view of all the service elements configured in the different pages of the wizard. You can either click the buttons corresponding to the various settings at the top of the wizard page to directly traverse to the page you want to modify or click the navigation buttons at the bottom of the wizard page to go to the different pages of the wizard.



NOTE: On the Review page, in the Service Templates section, the names of the service templates with which the service definition is associated are displayed. The Default Service Template column indicates whether the attached template is the default template.

To examine and modify the configured service definition settings:

1. Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify.
2. Click **Edit** next to the section that contains the parameter you want to modify. You are navigated to the corresponding page of the wizard in which the parameter settings are defined.
3. Click **Finish** to save the service definition or service order.
4. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

When the service definition is successfully created, you are returned to the Manage Service Definitions window.

Related Documentation

- [Choosing a Predefined Service Definition or Creating a New Service Definition on page 593](#)
- [Creating a Point-to-Point Ethernet Service Definition on page 625](#)
- [Publishing a Custom Service Definition on page 647](#)
- [Unpublishing a Custom Service Definition on page 648](#)
- [Deleting a Customized Service Definition on page 649](#)
- [Viewing Service Definitions on page 650](#)

Creating a Point-to-Point Ethernet Service Definition

Use this procedure to create a definition for a point-to-point VPN service. The standard service definitions that came with your initial software installation are designed to be appropriate for most requirements. You can also create a customized service definition—for example, to set different bandwidth limits on the service than those offered in the standard service definitions.

After the new service definition is complete and published, network operators or service provisioners can use the completed service definition as a base for creating and then activating point-to-point VPN services on the network.

The windows appear in the order stated. You can, however, perform these steps in any order by accessing them through the task list in the right panel. If the panel is not visible, click the snap tool on the right side of the main display area.

To create a point-to-point service definition, complete these tasks, in the order shown:

1. [Specifying General Information on page 625](#)
2. [Specifying UNI Settings on page 628](#)
3. [Specifying Connectivity Information When Signaling Is LDP on page 640](#)
4. [Specifying Connectivity Information When Signaling Is BGP on page 643](#)

Specifying General Information

To specify the general information for a point-to-point Ethernet service definition:

1. In the Build mode of the Network Services > Connectivity task pane, select **Service Design > Manage Service Definitions > New > P2P Service Definition**. The **General** settings window of the Create Point-to-Point Service Definition wizard appears.

The screenshot shows the 'Create Point-to-Point Service Definition' wizard in the 'General' tab. The wizard has four steps: General, UNI Settings, Connectivity Settings, and Review. The 'General' tab is currently active. Below the step indicators, it says 'You are here: General'. The main content area is divided into three sections: General Settings, Service Extension, and Service Templates. In the General Settings section, the 'Service definition name*' is 'P2P_BGP_SD', 'Service Type' is 'Point-to-Point Pseudowire', 'Signalling' is 'BGP', and 'Pseudowire Type' is 'Ethernet'. The 'Description' field is empty. In the Service Extension section, there are two checkboxes: 'Enable Multihoming' (checked) and 'Decouple Service Status from Port Status' (unchecked). In the Service Templates section, there is a 'Select Templates' dialog box with an 'Add' button, a 'Delete' button, and a search bar. Below the dialog box is a table with two columns: 'Name' and 'Default'. The table is currently empty. At the bottom of the wizard, there are four buttons: 'Back', 'Next', 'Done', and 'Cancel'.

2. Fill in the fields in the **General** window.

Field	Action
Name	Enter a name for the service definition.
Service type	By default, the service type is Point-to-Point Pseudowire .
Signaling	<p>Select a signaling type:</p> <ul style="list-style-type: none"> • BGP • LDP <p>You cannot edit the Signaling type in the service order.</p> <p>NOTE: If the signaling type is BGP, the Static pseudowire and the Enable PW access to L3 VPN network check boxes are not available. You cannot edit the Signaling type in the service order.</p>
Description (Optional)	<p>Enter a brief description or other comment that you want to appear in the Service Definition table.</p> <p>Range: 0 through 200 characters. Spaces and special characters are allowed.</p>
Enable QoS	<p>When you enable QoS in the service definition, you can specify a QoS profile in the service order to classify traffic into defined service groups to provide the special treatment of traffic across the network service. For example, voice traffic can be sent across certain links, and data traffic can use other links.</p> <p>QoS settings can be defined in service templates and attached to a service order to classify traffic into defined service groups to provide the special treatment of traffic across the network service. For example, voice traffic can be sent across certain links, and data traffic can use other links.</p>
Interface type	<p>Select the interface type:</p> <ul style="list-style-type: none"> • Ethernet • TDM • ATM
Static pseudowire	To enable static pseudowire, select the Static pseudowire check box. This check box is disabled if the signaling type is BGP.
Enable PW access to L3 VPN network	<p>To enable the pseudowire access to L3 VPN network, select the Enable PW access to L3 VPN network check box. This check box is disabled if the signaling type is BGP, or if you have selected the interface type as TDM/ATM.</p> <p>If you select this check box, the Enable Multi Segment Pseudowire check box is disabled.</p>

Field	Action
Enable Multi Segment Pseudowire	<p>Select this check box to enable multi-segment pseudowire.</p> <p>If you select this check box, the Enable PW access to L3 VPN network check box is disabled.</p> <p>A multi-segment pseudowire (MS-PW) is a static or dynamically configured set of two or more contiguous pseudowire segments that behave and function as a single point-to-point pseudowire. Each end of an MS-PW, by definition, terminates on a T-PE.</p> <p>NOTE: The number of pseudowire segments that you can stitch is limited to two.</p> <p>For more information on point-to-point pseudowire stitching, see “Stitching Two Point-to-Point Pseudowires” on page 858.</p>
Enable PW Resiliency	<p>To enable the pseudowire resiliency, select the Enable PW Resiliency check box. For more information on pseudowire redundancy, see “Redundant Pseudowires for Layer 2 Circuits and VPLS” on page 94.</p>
Decouple Service Status From Port Status	<p>By default, all the events are saved in the OpenNMS database. To isolate the events related to an interface in the OpenNMS, select the Decouple Service Status From Port Status check box.</p> <p>NOTE: When you select this check box, only the pseudowire traps are monitored, and not the interface-related traps (such as jnxVpnIfUp or jnxVpnIfDown).</p>
Service Template	<p>(Optional) To include a service template for the service, click the Add icon or plus sign (+) to select a service template from the Service Template list. The list of available service templates is displayed. Select the check box beside the template you want and click OK. You are returned to the General Settings page.</p> <p>The selected service template appears in the Default Service Template field.</p> <p>You can select one or more service templates as the default service template. By default, the default service templates are attached to the endpoints.</p> <p>NOTE: You cannot add or delete a service template while creating a service order.</p> <p>The remaining service templates on the Service Template list are termed as optional service templates. You can attach the optional service templates to the endpoints on a need basis.</p> <p>In the View Service Definition Details window, the value for the default service template in the Default Service Template column is <i>True</i>.</p> <p>For instructions on creating a service template, see “Creating a Service Template” on page 1815.</p>

Field	Action
Threshold alarm profile	If you intend to run performance tests on services based on this service definition, select a TCA Profile .

- Click **Next** to save the information. You can proceed to [“Specifying UNI Settings” on page 603](#).

Specifying UNI Settings

In this step, you provide the UNI service attributes for this service definition. The attributes you set depend on whether you are setting attributes for a port, an 802.1Q interface, a Q-in-Q interface, or a flexible VLAN tagging:

- [Specifying UNI Settings for Port-to-Port Services on page 628](#)
- [Specifying UNI Settings for Services with 802.1Q Interface Types on page 631](#)
- [Specifying UNI Settings for Services with Q-in-Q Interface Types on page 634](#)
- [UNI Settings for Services with Flexible VLAN Tagging \(Asymmetric Interface Types\) on page 637](#)

Specifying UNI Settings for Port-to-Port Services

To set UNI attributes for a port-to-port service, complete the following procedure.

- Enter information in the UNI Settings window.

Create Point-to-Point Service Definition.

General > **UNI Settings** > Connectivity Settings > Review

You are here: UNI Settings

PE-CE Traffic Treatment

Ethernet Option*: port

VLAN Normalization*: Normalize to Dot1q tag

☒ Auto Pick VLAN Id ☐ Editable in service order

VLAN Selection Range

Auto-pick: 1 - 4094

Manual Input: 1 - 4094

Tag Protocol ID

Outer: ☐ Editable in service order

Inner: ☐ Editable in service order

PE-CE UNI Settings

Encapsulation

Physical Interface*:

MTU Settings

Interface MTU (Bytes): 1522 ☐ Editable in service order

MTU Range: 1522 - 9192

QoS

☒ Enable QoS

Bandwidth

2. Fill in the fields in the **UNI Settings** window according to the following table.

Field	Action
Traffic Treatment Settings	
Ethernet option	<p>Select port-port from the list.</p> <p>The Ethernet option you choose determines the other options you can select and specify on the page.</p>
Customer traffic type	Select N/A . For port-to-port services, all traffic is always transported.
VLAN ID selection	In port-to-port services, all traffic and all VLANs on one port are transported to all other ports.
Editable in Service Order	Select this check box to allow the service provisioner to override the MTU setting.
Interface Settings	
Physical IF encapsulation	Select ethernet-vpls , the only valid physical interface encapsulation method allowed for port-to-port services.
Logical IF encapsulation	You cannot change this field because it is not relevant to port-to-port services.
MTU Settings	
Default MTU (Bytes)	<p>You can specify an MTU value in this field. The default value for MTU is 1522 bytes.</p> <p>To see the permitted range for the MTU value, select the Editable in Service Order check box. The MTU range is 1522 through 9192.</p>
MTU Range (Bytes)	<p>If you select the check box Editable in Service Order, you can specify a value range for MTU (in bytes). The permitted range for MTU is 1522 through 9192.</p> <p>NOTE: Ultimately, the system establishes the MTU by multiplying the value you specify in the Default MTU (Bytes) field by the value you specify for MTU Factor.</p>
Calculation of Burst-Size	
 <p>Bandwidth Burst-Size Settings</p> <p>Burst Size: MTU Based</p> <p>MTU Factor: 10 <input type="checkbox"/> Editable in service order</p>	

Field	Action
Calculate Burst Size	<p>Select the preferred option for calculating the burst size:</p> <ul style="list-style-type: none"> MTU Based If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902. The default value for MTU Factor is 10. Line Rate Based If you select the option Line Rate Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds. The default value for Burst Period is 1. <p>NOTE: The Calculate Burst Size list is enabled only when you select the Enable rate limiting check box.</p>

Bandwidth Settings

Enable rate limiting (check box)	If you select this check box, you can override the MTU setting.
Default bandwidth (Mbps)	<p>Specify the default bandwidth value, in Mbps.</p> <p>Default: 10 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps</p>
Min Bandwidth (Kbps)	<p>To override the default bandwidth value, select the Editable in Service Order check box.</p> <p>Specify the minimum bandwidth value in Kbps:</p> <p>Default: 1000 Kbps</p> <p>Range: 64 Kbps through 100,000 Kbps</p>
Max Bandwidth (Mbps)	<p>Specify the maximum bandwidth value, in Mbps.</p> <p>Default: 100 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps</p>

Field	Action
-------	--------

The following table lists the **Max Bandwidth (Mbps)** for the M Series, MX Series, and ACX Series Routers:

Table 77: Maximum Bandwidth for M Series, MX Series, and ACX Series Routers

M Series IQ2E PIC		M Series IQ2 PIC		MX Series 3D PIC		MX Series Non-3D PIC		ACX 2000	
GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)
32,000 Mbps or 32 Gbps	32,000 Mbps or 32 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps	100,000 Mbps or 100 Gbps	100,000 Mbps or 100 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps

Increment (Kbps)

Specify a value in the range that is made available to the service provisioner.

- Click **Next** to continue with connectivity settings.

Specifying UNI Settings for Services with 802.1Q Interface Types

To set UNI attributes for 802.1Q interfaces complete the following procedure.

- Enter information in the UNI Settings window.

The screenshot shows the 'Create Point-to-Point Service Definition' window with the 'UNI Settings' tab active. The window is divided into several sections:

- PE-CE Traffic Treatment:** Includes 'Ethernet Option' (set to dot1q), 'Customer Traffic Type' (set to Transport Single VLAN), and 'VLAN Normalization' (set to Normalize to Dot1q tag). There is a checkbox for 'Auto Pick VLAN Id' and an 'Editable in service order' checkbox.
- VLAN Selection Range:** Includes 'Auto-pick' and 'Manual Input' sections, both showing a range from 1 to 4094.
- Tag Protocol ID:** Includes 'Outer' and 'Inner' sections, both with dropdown menus and 'Editable in service order' checkboxes.
- PE-CE UNI Settings:** Includes 'Encapsulation' (Physical and Logical Interface) with dropdown menus.
- MTU Settings:** Includes 'Interface MTU (Bytes)' (set to 1522) and 'MTU Range' (set to 1522 to 9192), both with 'Editable in service order' checkboxes.
- QoS:** A section at the bottom that is currently collapsed.

At the bottom right, there are buttons for 'Back', 'Next', 'Done', and 'Cancel'.

- Fill in the fields in the **UNI Settings** window according to the following table:

Field	Action
-------	--------

Traffic Treatment Settings

Field	Action
Ethernet option	<p>Select do1q from the list.</p> <p>The Ethernet option you choose determines the other options you can select and specify on the page.</p>
Customer traffic type	<p>Single VLAN is the only option for 802.1Q interface types.</p> <p>Specify the customer traffic type:</p> <ul style="list-style-type: none"> • Transport single vlan—Transports traffic for a specific VLAN across the network. You need to specify both Outer Tag protocol ID and Inner Tag protocol ID. • Transport VLAN range—Limits the traffic across the network to a specific range of VLANs. If you select this option, the service provisioner is prompted for the VLAN-ID range when creating a service order based on this service definition. You need to specify both Outer Tag protocol ID and Inner Tag protocol ID. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p>
VLAN ID selection	<p>Indicate how the VLAN ID is selected during service order creation.</p> <ul style="list-style-type: none"> • Select manually—Allows the service provider to specify the VLAN ID. This option is normally used when no VLAN normalization is applied. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting. Specify the VLAN ID range in VLAN range for manual input.</p> • Auto pick—This option is normally used when VLAN normalization is applied. Specify the VLAN ID pool in VLAN range for auto-pick. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p> <p>NOTE: When the range of VLAN IDs that are automatically assigned by the system (with the auto-pick option enabled during the creation of a service definition) is less than or greater than the range of VLAN IDs that are manually specified (with the manual selection option enabled during the creation of a service definition), the following conditions apply during the creation of a service order with the Editable in Service Order check box selected during service definition creation:</p> <ul style="list-style-type: none"> • If you create a service order with the auto-pick option enabled, the VLAN ID is selected from the auto-pick range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range. • If you create a service order with the auto-pick option disabled, the VLAN ID is selected from the manually configured range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range.
VLAN range for auto-pick	<p>Specify the VLAN ID pool.</p> <p>Range: 1 through 4094</p>
VLAN range for manual input	<p>Specify the VLAN ID range.</p> <p>Range: 1 through 4094</p>

Field	Action
Outer Tag protocol ID	<p>Select the outer tag protocol ID if the Customer traffic type is Transport single VLAN:</p> <ul style="list-style-type: none"> • 0x88a8 • 0x8100 • 0x9100 <p>NOTE: For an interface, you must configure a physical port with the possible Tag Protocol Identifiers (TPIDs) either manually or through a template. Otherwise, the service creation fails for all TPIDs except 0x8100. To configure the TPIDs manually, use the following commands:</p> <pre>set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x9100 set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x88a8 set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x8100</pre>
Editable in Service Order	Select this check box to allow the service provisioner to override the MTU setting.
Interface Settings	
Physical IF encapsulation	Select the default physical encapsulation scheme to be used by service orders based on this service definition. We recommend you select flexible-ethernet-services .
Logical IF encapsulation	Constrained by your selection in the Physical IF encapsulation box. If you selected the recommended physical encapsulation mode of flexible-ethernet-services, then your only option is to select vlan-vpls for the logical encapsulation method.
MTU Settings	
Default MTU (Bytes)	<p>You can specify an MTU value in this field. The default value for MTU is 1522.</p> <p>To see the permitted range for the MTU value, select the Editable in Service Order check box. The MTU range is 1522 through 9192.</p>
MTU Range (Bytes)	<p>If you select the check box Editable in Service Order, you can specify a value range for MTU (in bytes). The permitted range for MTU is 1522 through 9192.</p> <p>NOTE: Ultimately, the system establishes the MTU by multiplying the value you specify in the Default MTU (Bytes) field by the value you specify for MTU Factor.</p>
Calculation of Burst-Size	
<div> <div> <div>Bandwidth Burst-Size Settings</div> <div> <div>Burst Size:</div> <div>MTU Based</div> </div> <div> <div>MTU Factor:</div> <div>10</div> </div> <div> <input type="checkbox"/> Editable in service order </div> </div> </div>	

Field	Action
Calculate Burst Size	<p>Select the preferred option for calculating the burst size:</p> <ul style="list-style-type: none"> MTU Based If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902. The default value for MTU Factor is 10. Line Rate Based If you select the option Line Rate Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds. The default value for Burst Period is 1. <p>NOTE: The Calculate Burst Size list is enabled only when you select the Enable rate limiting check box.</p>

3. Click **Next** to continue with connectivity settings.

Specifying UNI Settings for Services with Q-in-Q Interface Types

To set UNI attributes for a Q-in-Q service, complete the following procedure.

1. To set UNI attributes for Q-in-Q interfaces:

The screenshot displays the 'Create Point-to-Point Service Definition' window with the 'UNI Settings' tab active. The 'You are here: UNI Settings' breadcrumb is visible. The configuration is divided into two main sections: 'PE-CE Traffic Treatment' and 'PE-CE UNI Settings'. In the first section, 'Ethernet Option' is set to 'qinq', 'Customer Traffic Type' is 'Transport VLAN Range', and 'VLAN Normalization' is 'Normalization not required'. The 'VLAN Selection Range' is configured with 'Auto-pick' and a range of 1 to 4094. The 'Tag Protocol ID' section has 'Outer' and 'Inner' dropdowns, both marked as 'Editable in service order'. The second section, 'PE-CE UNI Settings', includes 'Encapsulation' and 'MTU Settings'. 'Encapsulation' has 'Physical Interface' and 'Logical Interface' dropdowns. 'MTU Settings' shows 'Interface MTU (Bytes)' as 1522 and 'MTU Range' as 1522 to 9192, both marked as 'Editable in service order'. At the bottom right, there are four buttons: 'Back', 'Next', 'Done', and 'Cancel'.

2. Fill in the fields in the **UNI Settings** window according to the following table:

Field	Action
Traffic Treatment Settings	

Field	Action
Ethernet option	<p>Select qinq from the list.</p> <p>The window expands to include options specific to Q-in-Q interfaces.</p>
Customer traffic type	<p>Specify the customer traffic type:</p> <ul style="list-style-type: none"> • Transport all traffic—Transports the traffic from all VLANs across the network. When you select this option, the service provisioner is prompted for the VLAN-ID when creating a service order based on this service definition. You need to specify only the Outer Tag protocol ID. • Transport single vlan—Transports traffic for a specific VLAN across the network. You need to specify both Outer Tag protocol ID and Inner Tag protocol ID. • Transport VLAN range—Limits the traffic across the network to a specific range of VLANs. If you select this option, the service provisioner is prompted for the VLAN-ID range when creating a service order based on this service definition. You need to specify both Outer Tag protocol ID and Inner Tag protocol ID. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p>
VLAN ID selection	<p>Indicate how the VLAN ID is selected during service order creation.</p> <ul style="list-style-type: none"> • Select manually—Allows the service provider to specify the VLAN ID. This option is normally used when no VLAN normalization is applied. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting. Specify the VLAN ID range in VLAN range for manual input.</p> • Auto pick—This option is normally used when VLAN normalization is applied. Specify the VLAN ID pool in VLAN range for auto-pick. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p> <p>NOTE: When the range of VLAN IDs that are automatically assigned by the system (with the auto-pick option enabled during the creation of a service definition) is less than or greater than the range of VLAN IDs that are manually specified (with the manual selection option enabled during the creation of a service definition), the following conditions apply during the creation of a service order with the Editable in Service Order check box selected during service definition creation:</p> <ul style="list-style-type: none"> • If you create a service order with the auto-pick option enabled, the VLAN ID is selected from the auto-pick range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range. • If you create a service order with the auto-pick option disabled, the VLAN ID is selected from the manually configured range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range.
VLAN range for auto-pick:	<p>Specify the VLAN ID pool.</p> <p>Range: 1 through 4094</p>
VLAN range for manual input	<p>Specify the VLAN ID range.</p> <p>Range: 1 through 4094</p>

Field	Action
Outer Tag protocol ID	<p>Select the outer tag protocol ID if the Customer traffic type is Transport single VLAN:</p> <ul style="list-style-type: none"> • 0x88a8 • 0x8100 • 0x9100 <p>NOTE: For an interface, you must configure a physical port with the possible Tag Protocol Identifiers (TPIDs) either manually or through a template. Otherwise, the service creation fails for all TPIDs except 0x8100. To configure the TPIDs manually, use the following commands:</p> <pre>set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x9100 set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x88a8 set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x8100</pre>
Inner Tag protocol ID	<p>Select the inner tag protocol ID:</p> <ul style="list-style-type: none"> • 0x88a8 • 0x8100 • 0x9100 <p>NOTE: You cannot specify the Inner Tag protocol ID if the Customer traffic type is Transport single VLAN.</p>
Editable in Service Order	Select this check box to allow the service provisioner to override the MTU setting.
Interface Settings	
Physical IF encapsulation	Select the default physical encapsulation scheme to be used by service orders based on this service definition. We recommend you select flexible-ethernet-services .
Logical IF encapsulation	Constrained by your selection in the Physical IF encapsulation box. If you selected the recommended physical encapsulation mode of flexible-ethernet-services, then your only option is to select vlan-vpls for the logical encapsulation method.
MTU Settings	
Default MTU (Bytes)	<p>You can specify an MTU value in this field. The default value for MTU is 1522.</p> <p>To see the permitted range for the MTU value, select the Editable in Service Order check box. The MTU range is 1522 through 9192.</p>
MTU Range (Bytes)	<p>If you select the check box Editable in Service Order, you can specify a value range for MTU (in bytes). The permitted range for MTU is 1522 through 9192.</p> <p>NOTE: Ultimately, the system establishes the MTU by multiplying the value you specify in the Default MTU (Bytes) field by the value you specify for MTU Factor.</p>

Field	Action
Calculation of Burst-Size	
<div> <div>Bandwidth Burst-Size Settings</div> <div> <div>Burst Size:</div> <div>MTU Based</div> </div> <div> <div>MTU Factor:</div> <div>10</div> </div> <div> <input type="checkbox"/> Editable in service order </div> </div>	

Calculate Burst Size

Select the preferred option for calculating the burst size:

- MTU Based**
 If you select the option **MTU Based**, you can specify a value for **MTU Factor** in the range 1 through 1087902.
 The default value for **MTU Factor** is 10.
- Line Rate Based**
 If you select the option **Line Rate Based**, you can specify a value for **Burst Period** in the range 1 through 7450 milliseconds.
 The default value for **Burst Period** is 1.

NOTE: The **Calculate Burst Size** list is enabled only when you select the **Enable rate limiting** check box.

- Click **Next** to continue with connectivity settings.

UNI Settings for Services with Flexible VLAN Tagging (Asymmetric Interface Types)

You can specify the Ethernet option **asymmetric tag depth** to create a service that includes any combination of port-based interfaces, 802.1Q interfaces, and Q-in-Q interfaces.

- Enter information in the UNI Settings window.

The screenshot displays the 'Create Point-to-Point Service Definition' window with the 'UNI Settings' tab selected. The breadcrumb trail shows 'General' > 'UNI Settings' > 'Connectivity Settings' > 'Review'. The 'You are here: UNI Settings' section is active. The configuration is organized into several expandable sections:

- PE-CE Traffic Treatment:**
 - Ethernet Option*:** Set to 'asymmetric tag depth'.
 - Customer Traffic Type*:** Set to 'Transport Single VLAN'.
 - VLAN Normalization*:** Set to 'None'.
 - ☒ **Auto Pick VLAN Id** (with 'Editable in service order' checkbox).
 - VLAN Selection Range:**
 - Auto-pick:** Range 1 to 4094.
 - Manual Input:** Range 1 to 4094.
 - Tag Protocol ID:**
 - Outer:** Set to 'None' (with 'Editable in service order' checkbox).
 - Inner:** Set to 'None' (with 'Editable in service order' checkbox).
- PE-CE UNI Settings:**
 - Encapsulation:**
 - Physical Interface*:** (Empty dropdown).
 - Logical Interface*:** (Empty dropdown).
 - MTU Settings:**
 - Interface MTU (Bytes):** Set to 1522 (with 'Editable in service order' checkbox).
 - MTU Range:** Set to 1522 - 9192.
 - QoS:** (Section header, details not visible).

At the bottom right, there are four navigation buttons: 'Back', 'Next', 'Done', and 'Cancel'.

2. Specify the UNI Settings for asymmetric tag depth according to the following table:

Field	Action
Traffic Treatment Settings	
Ethernet option	Select asymmetric tag depth from the list.
Customer traffic type	<p>Select the customer traffic type:</p> <ul style="list-style-type: none"> • Transport all traffic—Transports the traffic from all VLANs across the network. When you select this option, the service provisioner is prompted for the VLAN-ID when creating a service order based on this service definition. You need to specify only the Outer Tag protocol ID and Inner Tag protocol ID. • Transport single vlan—Transports traffic for a specific VLAN across the network. You need to specify both Outer Tag protocol ID and Inner Tag protocol ID. • Transport VLAN range—Limits the traffic across the network to a specific range of VLANs. You need to specify both Outer Tag protocol ID and Inner Tag protocol ID. <p>If you select this option, the service provisioner is prompted for the VLAN-ID range when creating a service order based on this service definition.</p> <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p>
VLAN ID selection	<p>Indicate how the VLAN ID is selected during service order creation.</p> <ul style="list-style-type: none"> • Select manually—Allows the service provider to specify the VLAN ID. This option is normally used when no VLAN normalization is applied. Specify the VLAN ID range in VLAN range for manual input. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p> <ul style="list-style-type: none"> • Auto pick—This option is normally used when VLAN normalization is applied. Specify the VLAN ID pool in VLAN range for auto-pick. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting. Specify the VLAN ID pool in VLAN range for auto-pick.</p> <p>NOTE: When the range of VLAN IDs that are automatically assigned by the system (with the auto-pick option enabled during the creation of a service definition) is less than or greater than the range of VLAN IDs that are manually specified (with the manual selection option enabled during the creation of a service definition), the following conditions apply during the creation of a service order with the Editable in Service Order check box selected during service definition creation:</p> <ul style="list-style-type: none"> • If you create a service order with the auto-pick option enabled, the VLAN ID is selected from the auto-pick range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range. • If you create a service order with the auto-pick option disabled, the VLAN ID is selected from the manually configured range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range.
VLAN range for auto-pick:	<p>Specify the VLAN ID pool.</p> <p>Range: 1 through 4094</p>

Field	Action
VLAN range for manual input	Specify the VLAN ID range. Range: 1 through 4094
Outer Tag protocol ID	<p>Select the outer tag protocol ID if the Customer traffic type is Transport single VLAN:</p> <ul style="list-style-type: none"> • 0x88a8 • 0x8100 • 0x9100 <p>NOTE: For an interface, you must configure a physical port with the possible Tag Protocol Identifiers (TPIDs) either manually or through a template. Otherwise, the service creation fails for all TPIDs except 0x8100. To configure the TPIDs manually, use the following commands:</p> <pre>set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x9100 set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x88a8 set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x8100</pre>
Inner Tag protocol ID	<p>Select the inner tag protocol ID:</p> <ul style="list-style-type: none"> • 0x88a8 • 0x8100 • 0x9100 <p>NOTE: You cannot specify the Inner Tag protocol ID if the Customer traffic type is Transport all traffic.</p>
Editable in Service Order	To allow the service provisioner to override the MTU setting, select the check box for those options.
Interface Settings	
Physical IF encapsulation	Select the default physical encapsulation scheme to be used by service orders based on this service definition. We recommend you select flexible-ethernet-services .
Logical IF encapsulation	Constrained by your selection in the Physical IF encapsulation box. If you selected the recommended physical encapsulation mode of flexible-ethernet-services, then your only option is to select vlan-vpls for the logical encapsulation method.
MTU Settings	
Default MTU (Bytes)	<p>You can specify an MTU value in this field. The default value for MTU is 1522.</p> <p>To see the permitted range for the MTU value, select the Editable in Service Order check box. The MTU range is 1522 through 9192.</p>
MTU Range (Bytes)	<p>If you select the check box Editable in Service Order, you can specify a value range for MTU (in bytes). The permitted range for MTU is 1522 through 9192.</p> <p>NOTE: Ultimately, the system establishes the MTU by multiplying the value you specify in the Default MTU (Bytes) field by the value you specify for MTU Factor.</p>

Field	Action
Calculation of Burst-Size	
<div> <div> <div>Bandwidth Burst-Size Settings</div> <div> <div>Burst Size:</div> <div>MTU Based</div> </div> <div> <div>MTU Factor:</div> <div>10</div> </div> <div> <div>Editable in service order</div> </div> </div> </div>	

Calculate Burst Size

Select the preferred option for calculating the burst size:

- MTU Based**

If you select the option **MTU Based**, you can specify a value for **MTU Factor** in the range 1 through 1087902.

The default value for **MTU Factor** is 10.

- Line Rate Based**

If you select the option **Line Rate Based**, you can specify a value for **Burst Period** in the range 1 through 7450 milliseconds.

The default value for **Burst Period** is 1.

NOTE: The **Calculate Burst Size** list is enabled only when you select the **Enable rate limiting** check box.

3. Click **Next** to continue with connectivity settings.

Specifying Connectivity Information When Signaling Is LDP

The fields displayed in the **Connectivity** window depend on the **Signaling type** (LDP or BGP) that you selected in the **General** settings window.

Create Point-to-Point Service Definition.

General

UNI Settings

Connectivity Settings

Review

You are here: Connectivity Settings

Connectivity Settings

Auto-pick Route Target

Auto-pick Route Distinguisher

MTU (Bytes):

1522

MTU Range (Bytes):

1522

-

9192

Editable in service order

Editable in service order

Editable in service order

Back

Next

Done

Cancel

To specify connectivity between sites across the network when signaling is LDP:

1. Fill in the fields in the **Connectivity** window.

Field	Action
VC ID selection	<p>The VC ID selection is available only if the Signaling type is LDP.</p> <p>In the VC ID selection box, specify how you want the VC ID to be chosen during service order creation:</p> <ul style="list-style-type: none"> • To allow the service provisioner to enter the VC ID, choose Select manually. • To cause the Junos Space software to assign a VC ID automatically from the VC ID pool, select Auto pick. <p>To allow the service provisioner to override the setting in the VC ID box, select Editable in Service Order.</p>
Default MTU	<p>In the Default MTU box, specify the MTU across the service provider network.</p> <p>To allow the service provisioner to override the MTU setting, select Editable in Service Order. In the MTU range, enter the highest and lowest MTU that the service provisioner can enter.</p>
Revert time (sec)	<p>This field is available if you selected the Enable PW Resiliency check box and if the Signaling is LDP in the General settings.</p> <p>Revert time (sec)—Revert time for redundant Layer 2 circuits and VPLS pseudowires.</p> <p>Default: 5 seconds</p> <p>Range: 0 through 65,535 seconds</p>
Switch Over Delay (sec)	<p>This field is available if you selected the Enable PW Resiliency check box and if the Signaling is LDP, in the General settings.</p> <p>Switch Over Delay (sec)—Delay to wait before the backup pseudowire takes over.</p> <p>Default: 0 second</p> <p>Range: 0 through 180 seconds</p>
VLAN Normalization	<p>The options available in the VLAN normalization are based on the value set for the Ethernet interface.</p>
Outgoing label selection	<p>This field is available if you selected the Static pseudowire check box in the General settings. By default, the outgoing label selection is limited to manual.</p>

The following table presents the available **VLAN normalization** options:

Ethernet Option	Customer Traffic Type	VLAN Normalization
port-port	N/A	<p>Normalization not required</p> <p>Normalization to Dot1q tag</p> <p>Normalization to QinQ tags</p> <p>NOTE: Starting with Release 1.0R2, when you newly install Connectivity Services Director, if you select the option to not require normalization in a service definition, the auto-pick option for VLAN IDs and the option to edit the auto-pick behavior in service order are disabled in the service definition. When you create a service order by associating with that service definition, you need to manually enter the VLAN IDs for the interfaces and cannot use the auto-pick functionality. This same behavior also applies to default service templates in which if you select the normalization-not-required functionality, the auto-pick option for VLAN IDs is disabled.</p>
dot1q	Transport single vlan	<p>Swap</p> <p>Normalize to None</p> <p>Normalization to Dot1q tag</p> <p>Normalization to QinQ tags</p>
	Transport vlan range	Normalization not required
qinq	Transport all traffic	<p>Swap</p> <p>Normalize to None</p> <p>Normalization to Dot1q tag</p> <p>Normalization to QinQ tags</p>
	Transport single vlan	<p>Swap</p> <p>Normalize to None</p> <p>Normalization to Dot1q tag</p> <p>Normalization to QinQ tags</p>
	Transport vlan range	Normalization not required
	Asymmetric	(Identical to qinq)

- Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.



NOTE: On the Review page, in the Service Templates section, the names of the service templates with which the service definition is associated are displayed. The Default Service Template column indicates whether the attached template is the default template.

Create Point-to-Point Service Definition.

General > UNI Settings > Connectivity Settings > **Review**

You are here: Review

General

General Settings

Service Definition Name: P2P_BGP_SD
 Service Type: Point-to-Point Pseudowire
 Signalling: BGP
 Pseudowire Type: Ethernet

Service Templates

Selected Templates: All_Services_Interface_Option

Service Extension

Enable Multihoming: false
 Decouple Service Status from Port Status: false

UNI Settings

PE-CE Traffic Treatment

Ethernet Option: dot1q
 Customer Traffic Type: Transport vlan range
 VLAN Normalization: Normalization not required

☐ VLAN Selection Range

Back Next Done Cancel

After you complete reviewing the settings, click **Finish** to complete the service definition creation.

Specifying Connectivity Information When Signaling Is BGP

To specify connectivity between sites across the network when signaling is BGP, fill in the fields in the Connectivity window:

- When the signaling type is BGP, fill in the fields in the **Connectivity** window.
 - Route Distinguisher**—Identifier attached to a route, enabling you to distinguish to which VPN the route belongs. Each routing instance must have a unique route distinguisher associated with it.
 Range: 1.1.1.1 through 255.255.255.254:65535, or 1:1 through 65535:4294967295
 - Route Target**—Allows you to distribute VPN routes to only the routers that need them.
 Range: 1.1.1.1 through 255.255.255.254:65535, or 1:1 through 65535:4294967295
 - Default MTU (Bytes)**—The default MTU established by the system.
 - MTU range (Bytes)**—Specify the range, in bytes, for the MTU.
 - VLAN normalization**—The options available in the **VLAN normalization** field are based on the value set for the Ethernet interface. The following table presents the options.



.....

NOTE: Starting with Release 1.0R2, when you newly install Connectivity Services Director, if you select the option to not require normalization in a service definition, the auto-pick option for VLAN IDs and the option to edit the auto-pick behavior in service order are disabled in the service definition. When you create a service order by associating with that service definition, you need to manually enter the VLAN IDs for the interfaces and cannot use the auto-pick functionality. This same behavior also applies to default service templates in which if you select the normalization-not-required functionality, the auto-pick option for VLAN IDs is disabled.

.....

Ethernet Option	Customer Traffic Type	VLAN Normalization
port-port	N/A	Normalization not required Normalization to Dot1q tag Normalization to QinQ tags
dot1q	Transport single vlan	Swap Normalize to None Normalization to Dot1q tag Normalization to QinQ tags
	Transport vlan range	Normalization not required
qinq	Transport all traffic	Swap Normalize to None Normalization to Dot1q tag Normalization to QinQ tags
	Transport single vlan	Swap Normalize to None Normalization to Dot1q tag Normalization to QinQ tags
	Transport vlan range	Normalization not required
Asymmetric	(Identical to qinq)	(Identical to qinq)



NOTE: For a description of how the Connectivity Services Director software manipulates VLANs, see [“Understanding VLAN Manipulation \(Normalization and VLAN Mapping\) on Ethernet Services” on page 88.](#)

- Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

The screenshot shows the 'Create Point-to-Point Service Definition' wizard in the 'Review' tab. The breadcrumb trail at the top indicates the sequence: General > UNI Settings > Connectivity Settings > Review. The 'You are here: Review' status is shown. The main content area is divided into three sections: General, Service Templates, and UNI Settings. The General section includes 'General Settings' (Service Definition Name: P2P_BGP_SD, Service Type: Point-to-Point Pseudowire, Signalling: BGP, Pseudowire Type: Ethernet), 'Service Templates' (Selected Templates: All_Services_Interface_Option), and 'Service Extension' (Enable Multihoming: false, Decouple Service Status from Port Status: false). The UNI Settings section includes 'PE-CE Traffic Treatment' (Ethernet Option: dot1q, Customer Traffic Type: Transport vlan range, VLAN Normalization: Normalization not required) and a collapsed 'VLAN Selection Range' section. At the bottom right, there are four buttons: Back, Next, Done, and Cancel.

After you complete reviewing the settings, click **Finish** to complete the service definition creation.

Related Documentation

- [Choosing a Predefined Service Definition or Creating a New Service Definition on page 593](#)
- [Creating a Point-to-Point ATM or TDM Pseudowire Service Definition on page 618](#)
- [Publishing a Custom Service Definition on page 647](#)
- [Unpublishing a Custom Service Definition on page 648](#)
- [Deleting a Customized Service Definition on page 649](#)
- [Viewing Service Definitions on page 650](#)

Modifying a Custom Service Definition

You can modify a customized service definition only when it is in the unpublished state. Predefined service definitions are by default in the published state and cannot be modified.



NOTE: Templates associated with the service definition can be added or deleted while modifying a service definition. You can delete a template associated with a service definition when there is no service or service order associated with the service definition.

To modify a service definition:

1. In the Connectivity Services Director application, select **Service View** from the Views selector.
2. Click the **Build** tab on the Task Categories banner.
3. From the Service View pane, select **Network Services > Connectivity**.
4. From the Tasks pane, select **Service Design > Manage Service Definitions**.
5. In the Manage Service Definitions page, select the customized service definition you want to modify.
6. Click the **Edit** button.

The Edit Service Definition wizard for the selected service type is displayed

7. Modify the settings, as necessary, using the wizard, and save your changes by clicking **Done**.

The **Manage Service Definitions** page reappears. The selected service definition is now modified with the redefined settings.

Related Documentation

- [Choosing a Predefined Service Definition or Creating a New Service Definition on page 593](#)
- [Creating a Point-to-Point ATM or TDM Pseudowire Service Definition on page 618](#)
- [Creating a Point-to-Point Ethernet Service Definition on page 625](#)
- [Unpublishing a Custom Service Definition on page 648](#)
- [Deleting a Customized Service Definition on page 649](#)
- [Viewing Service Definitions on page 650](#)

Publishing a Custom Service Definition

You can use service definition in a service order only when it is in the published state. A customized service definition, by default, is in the unpublished state when created. You must publish the customized service definition before it can be used to create a service request.



NOTE: By default, predefined service definitions are in the published state.

To publish a service definition:

1. In the Connectivity Services Director application, select **Service View** from the Views selector.
2. Click the **Build** tab on the Task Categories banner.
3. From the Service View pane, select **Network Services > Connectivity**.
4. From the Tasks pane, select **Service Design > Manage Service Definitions**.
5. In the Manage Service Definitions page, select the unpublished customized service definition you want to publish.
6. Click **Publish**.

The Information window is displayed.

7. Click **Yes** in the Information window to publish the service definition.

The **Manage Service Definitions** page reappears. The selected customized service definition is now in the published state.

Related Documentation

- [Choosing a Predefined Service Definition or Creating a New Service Definition on page 593](#)
- [Creating a Point-to-Point ATM or TDM Pseudowire Service Definition on page 618](#)
- [Creating a Point-to-Point Ethernet Service Definition on page 625](#)
- [Unpublishing a Custom Service Definition on page 648](#)
- [Deleting a Customized Service Definition on page 649](#)
- [Viewing Service Definitions on page 650](#)

Unpublishing a Custom Service Definition

You can unpublish a customized service definition to make it unavailable. This allows you to delete or add templates to the service definition. A service definition can be unpublished even if there are service orders (pending or active) associated with it. However, an unpublished service definition cannot be deleted or modified if it has services associated with it.

To unpublish a service definition:

1. In the Connectivity Services Director application, select **Service View** from the Views selector.
2. Click the **Build** tab on the Task Categories banner.

3. From the Service View pane, select **Network Services > Connectivity**.
4. From the Tasks pane, select **Service Design > Manage Service Definitions**.
5. In the Manage Service Definitions page, select the customized service definition you want to unpublish.
6. Click **Unpublish**.
The Information window is displayed.
7. Click **Yes** in the Information window to unpublish the service definition.
The Manage Service Definition page reappears. The selected customized service definition is now in the unpublished state.

Related Documentation

- [Publishing a Custom Service Definition on page 647](#)

Deleting a Customized Service Definition

You can delete a customized service definition only when it is in the unpublished state. You cannot delete an unpublished service definition if it has services or service orders associated with it.



NOTE: You cannot delete a predefined service definition.

To delete a customized service definition:

1. In the Connectivity Services Director application, select **Service View** from the Views selector.
2. Click the **Build** tab on the Task Categories banner.
3. From the Service View pane, select **Network Services > Connectivity**.
4. From the Tasks pane, select **Service Design > Manage Service Definitions**.
5. In the Manage Service Definitions page, select the customized service definition you want to delete.



NOTE: You must unpublish the service definition before you can delete it. To unpublish a service definition, see [“Unpublishing a Custom Service Definition” on page 648](#).

6. Click **Delete**.

The Information window is displayed.

7. Click **Yes** in the Information window to confirm deletion.

The Manage Service Definition page refreshes with the selected service definition removed.

Related Documentation

- [Unpublishing a Custom Service Definition on page 648](#)

Viewing Service Definitions

The Manage Service Definitions inventory page allows you, the Service Designer, to view the status of service definitions and list of service definitions that you have created to include in service orders.

Service definitions are listed by name.

Select **Service Design > Manage Service Definitions** to view and perform actions on service definitions. From the Manage Service Definitions inventory page, you can publish, unpublish, and delete service definitions.

- [Tabular View on page 650](#)
- [Searching for Service Definitions on page 651](#)
- [Viewing Service Definition Details on page 651](#)
- [Performing Actions on Service Definitions on page 652](#)

Tabular View

In tabular view, service definition information appears in table rows and columns.

[Table 78 on page 650](#) describes the information presented in the table.

Table 78: Service Definition Table Fields

Column	Meaning
Name	The unique name assigned to the service definition.
State	One of the following values: <ul style="list-style-type: none">• Published—The service definition is available for use by service provisioners.• Unpublished—The service definition is not yet available for use by service provisioners.

Table 78: Service Definition Table Fields (continued)

Column	Meaning
Service Type	One of the following: <ul style="list-style-type: none"> • Point-to-point pseudowire (LDP) • Point-to-point pseudowire (BGP) • VPLS (MultiPoint-to-MultiPoint) • VPLS (Point-to-MultiPoint) • L3VPN (Full Mesh) • L3VPN (Hub-Spoke 1 Interface)
Signaling	One of the following values: <ul style="list-style-type: none"> • BGP • LDP
Pseudowire	Type of pseudowire configured for the service.
Description	A brief comment or easily-identifiable description specified for the service definition.
Use Count	Number of service orders with which this service definition has been associated.
Created By	The screen name of the user who created the service definition.
Created Date	The date and Pacific Daylight Time (PDT) time when you created the service definition.
Service Templates	Names of the service templates with which the service definition is associated. The Default Service Template column indicates whether the attached template is the default template.

Searching for Service Definitions

To search for a specific service definition, start typing its name in the Search field. The service definition name(s) starting with the letters you type are listed in the Search drop-down list box.

If you create tags to categorize service definitions, start typing the tag name in the Search field. Service definitions with the tag you type appears.

Viewing Service Definition Details

To view service definition detailed information, double-click the service definition row.

The Service Definition Details page displays a summary of the service definition settings: General, Connectivity, and UNI settings.

Performing Actions on Service Definitions

From the Manage Service Definitions inventory page you can perform the following actions:

- **Publish Service Definition**—See [“Publishing a Custom Service Definition” on page 647](#).
- **Unpublish Service Definition**—See [“Unpublishing a Custom Service Definition” on page 648](#).

Related Documentation

- [Creating a Point-to-Point ATM or TDM Pseudowire Service Definition on page 618](#)
- [Creating a Point-to-Point Ethernet Service Definition on page 625](#)
- [Creating a Multipoint-to-Multipoint VPLS Service Definition on page 653](#)
- [Creating a Point-to-Multipoint VPLS Service Definition on page 678](#)
- [Creating a Full-Mesh Layer 3 VPN Service Definition on page 709](#)
- [Creating a Hub-and-Spoke \(One Interface\) Layer 3 VPN Service Definition on page 719](#)

Service Design: Managing VPLS Service Definitions

- [Creating a Multipoint-to-Multipoint VPLS Service Definition on page 653](#)
- [Creating a Point-to-Multipoint VPLS Service Definition on page 678](#)
- [Creating a Service Definition for VPLS Access into Layer 3 Networks on page 705](#)

Creating a Multipoint-to-Multipoint VPLS Service Definition

This procedure provides the steps to create a definition for a multipoint-to-multipoint VPLS service.

The standard service definitions that came with your initial software installation are designed to be appropriate for most requirements. You can also create a customized service definition—for example, to set different bandwidth limits on the service than those offered in the standard service definitions.

When the new service definition is complete and published, network operators or service provisioners can use the completed service definition as a base for creating and then activating multipoint-to-multipoint Ethernet services on the network.

The windows appear in the order stated. You can, however, perform these steps in any order by accessing them through the task list in the right panel. If the panel is not visible, click the snap tool on the right side of the main display area.

To create a multipoint-to-multipoint Ethernet service definition, complete these tasks, in the order shown. As you finish a section and click **Next**, the attributes from the current window are saved and the next window in the sequence appears.

- [Specifying General Information for Multipoint-to-Multipoint VPLS Service Definitions on page 654](#)
- [Specifying Advanced Settings on page 657](#)
- [Specifying Site Settings for Multipoint-to-Multipoint VPLS Service Definitions on page 660](#)
- [UNI or Site Settings for Port-to-Port Interfaces in VPLS Services on page 660](#)
- [UNI or Site Settings for 802.1Q Interfaces in VPLS Services on page 664](#)
- [UNI or Site Settings for Q-in-Q Interfaces in VPLS Services on page 668](#)

- [UNI Settings for Services with Flexible VLAN Tagging \(Asymmetric Interface Types\)](#) on page 672
- [Reviewing the Configured Settings](#) on page 677

Specifying General Information for Multipoint-to-Multipoint VPLS Service Definitions

To specify the general information for a multipoint-to-multipoint service definition, in the Network Services > Connectivity view pane, select **Service Design** > **Manage Service Definitions** > **New** > **VPLS Service Definition**.

The **General** window appears.

The screenshot shows the 'Create VPLS Service Definition' window with the 'General Settings' tab selected. The 'General Settings' section includes fields for 'Service Definition Name*' (Vpls_MP2MP_SO), 'Description', 'Service Type*' (VPLS(MultiPoint-MultiPoint)), and 'Signalling Protocol*' (BGP). There is also an 'Enable L3 Access' checkbox. The 'BGP Connectivity Settings' section has checkboxes for 'Auto pick Route Target' and 'Auto pick Route Distinguisher', each with an 'Editable in service order' checkbox. The 'Service Templates' section includes 'MAC Settings' with checkboxes for 'Enable MAC learning' and 'Enable MAC statistics', each with an 'Editable in service order' checkbox. There are also numeric input fields for 'Interface MAC Limit' (1024) and 'MAC Table Size' (5120), each with an 'Editable in service order' checkbox. At the bottom, there are 'Back', 'Next', 'Done', and 'Cancel' buttons.

To specify the general information for a multipoint-to-multipoint service definition:

1. Fill in the fields on the **General** window.

Field	Action
Service Definition Name	Type a name for the service definition.
Service type	Select Multipoint-to-Multipoint Ethernet (VPLS)

Field	Action
Signaling	<p>Select a signaling type:</p> <ul style="list-style-type: none"> • BGP— If BGP signaling is selected, the following fields are available in the Connectivity section of the General Settings page: <ul style="list-style-type: none"> • Auto-pick Route Target • Auto-pick Route Distinguisher • LDP—If LDP signaling is selected, the following fields are available in the Connectivity section of the General Settings page: <ul style="list-style-type: none"> • Enable BGP-based Auto Discovery • Auto-pick Route Target, if Auto Discovery is enabled • Auto-pick Route Distinguisher, if Auto Discovery is enabled • Auto-pick VPLS ID, if Auto Discovery is disabled • Auto-pick VPN ID, if Auto Discovery is enabled <p>NOTE: You cannot edit the Signaling type in the service order.</p>
Description (Optional)	<p>Type a brief description or other comment that you want to appear in the Service Definition table.</p> <p>Range: 0 through 200 characters. Space and special characters are allowed.</p>
Enable QoS	<p>When you enable QoS in the service definition, you can specify a QoS profile in the service order to classify traffic into defined service groups to provide the special treatment of traffic across the network service. For example, voice traffic can be sent across certain links, and data traffic can use other links.</p>
Enable L3 Access	<p>Select this check box to create the link into Layer 3. If this check box is selected, the available Ethernet option in the Site Settings window are:</p> <ul style="list-style-type: none"> • dot1q • qinq
Enable Static PW Labels	<p>Select this check box to enable a pseudowire connection by configuring static values.</p> <p>NOTE: The Enable Static PW Labels check box is enabled only when the signaling type is LDP.</p>
Service Template	<p>(Optional) To include a service template for the service, click the Add icon or plus sign (+) to select a service template from the Service Template list. The list of available service templates is displayed. Select the check box beside the template you want and click OK. You are returned to the General Settings page.</p> <p>The selected service template appears in the Default Service Template field.</p> <p>You can select one or more service templates as the default service template. By default, the default service templates are attached to the endpoints.</p> <p>NOTE: You cannot add or delete a service template while creating a service order.</p> <p>The remaining service templates on the Service Template list are termed as optional service templates. You can attach the optional service templates to the endpoints on a need basis.</p> <p>In the View Service Definition Details window, the value for the default service template in the Default Service Template column is <i>True</i>.</p> <p>For instructions on creating a service template, see “Creating a Service Template” on page 1815.</p>

Field	Action
BGP Connectivity Settings —This section is displayed if you select the signaling type as BGP.	
Auto-pick Route Target	<p>Select this check box to enable route target to be configured automatically. Deselect the check box if you want the route target to be manually configured. By default, manual configuration of route target is enabled.</p> <p>To override this setting in the service order, select the Editable in Service Order check box.</p>
Auto-pick Route Distinguisher	<p>Define a route distinguisher option:</p> <ul style="list-style-type: none"> • Select the check box to enable the service provider to specify the route distinguisher. • Select the check box to enable the route distinguisher to be selected automatically. <p>To override this setting in the service order, select the Editable in Service Order check box.</p>
LDP Connectivity Settings —This section is displayed if you select the signaling type as LDP.	
Enable BGP-based Auto Discovery	<p>The Auto Discovery check box is available only if the signaling type is LDP.</p> <p>NOTE: If the Enable Static PW Labels check box in the General window is checked for LDP signaling, then the Auto Discovery check box is disabled.</p> <p>The Auto Discovery check box is not available when the signaling type is BGP.</p> <p>On disabling the auto discovery specify the VPLS ID.</p>
Auto-pick VPLS ID or VPN ID	<p>This field is available only if the signaling type is LDP and auto discovery is disabled.</p> <p>Identifies the virtual circuit identifier used for the VPLS routing instance and the VPN ID associated with the router.</p> <p>Select this check box to enable the VPLS ID and VPN ID to be configured automatically. Deselect the check box if you want these attributes to be manually configured. By default, manual configuration is enabled.</p>
Auto-pick Route Target	<p>Select this check box to enable route target to be configured automatically. Deselect the check box if you want the route target to be manually configured. By default, manual configuration of route target is enabled.</p>
Auto-pick Route Distinguisher	<p>Define a route distinguisher option:</p> <ul style="list-style-type: none"> • Select the check box to enable the service provider to specify the route distinguisher. • Select the check box to enable the route distinguisher to be selected automatically. <p>To override this setting in the service order, select the Editable in Service Order check box.</p>
MAC Settings	
MAC learning	To enable MAC learning , select the check box.
Interface MAC limit	<p>Maximum number of MAC addresses learned from an interface.</p> <p>Range: 1 through 131071 MAC addresses per interface</p>
MAC statistics	To enable MAC statistic , select the check box.

Field	Action
MAC Table Size	<p>Modify the size of the MAC address table for the bridge domain.</p> <p>Range: 16 through 1048575</p> <p>To allow the service provisioner to override the MAC settings, select Editable in Service Order.</p>

- Click **Next** to save the information and continue with UNI or site settings.

Specifying Advanced Settings

In this step, you can specify the parameters that define advanced connectivity between sites across the service provider network. These settings can be configured in the **Advanced** settings section of the General Settings page of the Create VPLS Service Definition wizard.

BGP Connectivity Settings

- ☒ Auto pick Route Target ☐ Editable in service order
- ☒ Auto pick Route Distinguisher ☐ Editable in service order

Service Templates

- ☐ Enable MAC learning ☐ Editable in service order
- ☐ Enable MAC statistics ☐ Editable in service order

MAC Settings

- Interface MAC Limit: 1024 ☐ Editable in service order
- MAC Table Size: 5120 ☐ Editable in service order

Advanced Settings

- ☒ Include Tunnel Services ☒ Disable/Enable ☐ Editable in service order
- ☒ Include Local Switching ☒ Disable/Enable ☐ Editable in service order
- ☒ Include Reroute Priority low ☐ Editable in service order
- ☒ Include Connectivity type ce ☐ Editable in service order
- ☒ Include Label block size 8 ☐ Editable in service order

To specify advanced settings:

1. Fill in the fields as indicated in the table.

Advanced Settings—This section enables you to specify the parameters that define advanced connectivity between sites across the service provider network

Include	<p>Select the Include check box for each advanced setting that you want to include in the service definition.</p> <p>NOTE: If you select any advanced parameters for a service definition, you must also select the Include check box for the Disable tunnel services parameter, and select or clear the Disable tunnel services check box.</p> <p>For MX Series devices, if you deploy a VPLS service without selecting the Include check box for Disable tunnel services parameter, the VPLS service is down. As a work around, you can push the configuration to each PE device for the service by running the following command:</p> <pre>root@test_device# set chassis fpc 0 pic 1 tunnel-services bandwidth 1g</pre>
Disable Tunnel Services	<p>Enable or disable tunnel-services to specify that traffic for particular VPLS routing instances be forwarded to specific virtual tunnel (VT) interfaces.</p> <ul style="list-style-type: none"> To enable tunnel-services, clear the Disable Tunnel Services check box. To disable tunnel-services, select the Disable Tunnel Services check box (default).
Disable Local Switching	<p>Enable or disable local switching. In local switching mode, you can terminate multiple Layer 2 circuit pseudowires at a single VPLS mesh group:</p> <ul style="list-style-type: none"> To enable local switching across the network, clear the Disable Local Switching check box. To disable local switching across the network, select the Disable Local Switching check box (default).
Fast Reroute-Priority	<p>In this drop-down list, specify the reroute priority for a VPLS routing instance:</p> <ul style="list-style-type: none"> HIGH—Set the fast reroute priority for a VPLS routing instance to high. During a fast reroute event, the router repairs next hops for high-priority VPLS routing instances first. MEDIUM—Set the fast reroute priority for a VPLS routing instance to medium. During a fast reroute event, the router repairs next hops for medium-priority VPLS instances after high-priority VPLS routing instances but before low-priority VPLS routing instances. LOW—Set the fast reroute priority for a VPLS routing instance to low, which is the default. During a fast reroute event, the router repairs next hops for low-priority VPLS routing instances last.
Label Block Size	<p>Configure the label block size for VPLS labels by using one of the following values.</p> <ul style="list-style-type: none"> 2—Allocate the label blocks in increments of 2. Use this setting for a VPLS domain that has only two sites with no future expansion plans. 4—Allocate the label blocks in increments of 4. 8—Allocate the label blocks in increments of 8. This is the default. 16—Allocate the label blocks in increments of 16. A label block size of 16 enables you to minimize the number of routes in the VPLS domain. Use this setting only if the number of routes is the primary concern. <p>NOTE: This field is unavailable if the Signaling type is LDP and the Auto discovery check box is enabled.</p>

Connectivity type

Select a connection-type to specify when a VPLS connection is taken down, depending on whether the interface for the VPLS routing instance is customer-facing or integrated routing and bridging (IRB):

- **ce**—Require that for the VPLS connection to be up, the customer-facing interface for the VPLS routing instance must also be up. If the customer-facing interface fails, the VPLS connection is taken down. This is the default.
- **irb**—Allow a VPLS connection to remain up so long as an IRB interface is configured for the VPLS routing instance.

NOTE: This field is unavailable if the **Signaling** type is LDP and the **Auto discovery** is enabled.

Editable in Service Order

By default, each advanced setting that you include in the service definition can be edited in the service order. To prevent the service provisioner from overriding an advanced setting in the service order, clear the **Editable in Service Order** check box.

2. Click **Next** to define the UNI or site parameters. Alternatively, click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.
3. Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.
4. After you complete reviewing the settings, click **Finish** to complete the service definition creation.

Specifying Site Settings for Multipoint-to-Multipoint VPLS Service Definitions

In this step, you provide the UNI attributes for this service definition. The attributes you set depend on the type of interface you are using in this VPLS service definition. The following interface types are supported:

- ports
- 802.1Q interfaces
- Q-in-Q interfaces
- asymmetric interface

UNI or Site Settings for Port-to-Port Interfaces in VPLS Services

The **Site Settings** window provides four expanding or collapsing panels: Traffic Treatment, Interface Settings, MTU Settings, and Bandwidth Settings.

Create VPLS Service Definition.

General Settings

Site Settings

Review

You are here: Site Settings

PE-CE Interface Settings- Ethernet Encapsulation

VLAN Tagging*:port-port

Physical Interface Encapsulation:ethernet-vpls

Logical Interface Encapsulation:N/A

Traffic Type:

VLAN Normalization:Normalization not required

☐ Auto Pick VLAN ID

VLAN ID range for auto-pick:14094

VLAN ID range for manual-config:14094

Outer Tag Protocol ID:

Inner Tag Protocol ID:

Default Interface MTU:1522

MTU range for manual-config:15229192

☐ Editable in Service Order

☐ Editable in Service Order

PE-CE Interface Rate Limiting Settings

Back

Next

Done

Cancel

To specify the UNI Settings for Port-to-Port interfaces:

- 1. Fill in the fields on the **Site Settings** window.

Field	Action
PE-CE UNI Settings- Ethernet Encapsulation	
VLAN Tagging	<p>Select port-port from the list.</p> <p>The VLAN tagging option you choose determines the other options you can select and specify on the page.</p>
Editable in Service Order	<p>To allow the service provisioner to override the VLAN tagging or Ethernet option attribute, select the check box.</p>
Physical Interface Encapsulation	<p>Select ethernet-vpls, the only valid physical interface encapsulation method allowed for port-to-port services.</p>
Logical Interface Encapsulation	<p>You cannot select a choice in this field because it is not relevant to port-to-port services.</p>
Customer VLANs	<p>This drop-down list is disabled for port-to-port services. For port-to-port services, all traffic is always transported.</p>

Copyright © 2019, Juniper Networks, Inc.

661

Field	Action
VLAN Normalization	<p>Select a value:</p> <ul style="list-style-type: none"> • Normalize to VLAN all—To preserve customer VLAN IDs (and customer QoS priorities) across the network. <p>NOTE: For services that transport a range of VLANs, you must select VLAN Normalization to all. You cannot transport a range of VLANs without normalization.</p> <ul style="list-style-type: none"> • Normalized VLAN none—To preserve no VLAN IDs across the network. • Not normalized—If VLAN IDs are to be provided manually and are required to match. • Normalized to Dot1q—To transport only single-tagged frames across the network core. All port, dot1q, and Q-in-Q traffic is transported across the network • Normalized to QinQ—To transport only double-tagged frames across the network core. All port, dot1q, and Q-in-Q traffic is transported across the network. • Normalization not required—To specify no normalization for port-to-port services <p>NOTE: Starting with Release 1.0R2, when you newly install Connectivity Services Director, if you select the option to not require normalization in a service definition, the auto-pick option for VLAN IDs and the option to edit the auto-pick behavior in service order are disabled in the service definition. When you create a service order by associating with that service definition, you need to manually enter the VLAN IDs for the interfaces and cannot use the auto-pick functionality. This same behavior also applies to default service templates in which if you select the normalization-not-required functionality, the auto-pick option for VLAN IDs is disabled.</p> <p>For more information about VLAN normalization, see “Junos Space Layer 2 Services Overview” on page 55.</p> <p>For information about VLAN manipulation, see “Understanding VLAN Manipulation (Normalization and VLAN Mapping) on Ethernet Services” on page 88.</p>
Auto Pick VLAN ID	This check box is disabled because in port-to-port services, all traffic and all VLANs on one port are transported to all other ports.
Editable in Service Order	To allow the service provisioner to override the VLAN ID setting, select the check box. This check box is not applicable for port-to-port services.
Default Interface MTU (Bytes)	The default MTU value is 1522 bytes.
MTU Range for manual-config (Bytes)	<p>Specify the low and high values to define the MTU range that you want to define.</p> <p>The default range is 1522 through 9192 bytes.</p>
PE-CE Interface Rate-Limiting Settings	
Enable Interface Rate Limiting	<p>To enable a service provisioner to limit the available bandwidth, select this check box, and type a default bandwidth limit.</p> <p>NOTE: Bandwidth settings are available in the service definition when CoS profiles are associated.</p>
Default bandwidth (Mbps)	<p>Specify the default bandwidth value in Mbps.</p> <p>Default: 10 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps</p>

Field	Action
Min Bandwidth (Kbps)	Specify the minimum bandwidth value in Kbps. Default: 1000 Kbps Range: 64 Kbps through 100,000 Kbps
Max Bandwidth (Mbps)	Specify the maximum bandwidth value in Mbps. For more information on maximum bandwidth see Table 79 on page 663 Default: 100 Mbps Range: 1 Mbps through 100,000 Mbps
Increment (Kbps)	Specify a value that defines which values in the range is made available to the service provisioner. Default: 1000 Kbps Range: 64 Kbps through 100,000 Kbps
Bandwidth – Burst Size Settings	
Burst Size Calculator	<p>Select the preferred option for calculating the burst size:</p> <ul style="list-style-type: none"> • MTU Based If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902. The default value for MTU Factor is 10. • Burst Period Based If you select the option Burst Period Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds. The default value for Burst Period is 1. <p>NOTE: The Burst Size Calculator list is enabled only when you select the Enable Interface Rate Limiting check box.</p>

The following table lists the **Max Bandwidth (Mbps)** for the M Series, MX Series, and ACX Series Routers:

Table 79: Maximum Bandwidth for M Series, MX Series, and ACX Series Routers

M Series IQ2E PIC		M Series IQ2 PIC		MX Series 3D PIC		MX Series Non-3D PIC		ACX 2000	
GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)
32,000 Mbps or 32 Gbps	32,000 Mbps or 32 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps	100,000 Mbps or 100 Gbps	100,000 Mbps or 100 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps

2. Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to

modify. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

After you complete reviewing the settings, click **Finish** to complete the service definition creation.

UNI or Site Settings for 802.1Q Interfaces in VPLS Services

To specify the UNI Settings for 802.1Q interfaces:

1. Fill in the fields on the **Site Settings** window.

Field	Action
PE-CE UNI Settings- Ethernet Encapsulation	
VLAN Tagging	<p>Select dot1q from the list.</p> <p>The Ethernet option you choose determines the other options you can select and specify on the page.</p>
Physical Interface Encapsulation	Select the default physical encapsulation scheme to be used by service orders based on this service definition. We recommend you select flexible-ethernet-services .
Logical Interface Encapsulation	Constrained by your selection in the Physical IF encapsulation box. If you selected the recommended physical encapsulation mode of flexible-ethernet-services , then your only option is to select vlan-vpls for the logical encapsulation method.

Field	Action
Customer VLANs	<p>Single VLAN is the only option for 802.1Q interface types.</p> <p>Select Transport single vlan to transport the traffic for a specific VLAN across the network. When you select this option, the service provisioner is prompted for the VLAN-ID when creating a service order based on this service definition. You need to specify the Outer Tag protocol ID.</p> <p>Select Transport VLAN range to limit the traffic across the network to a specific range of VLANs.</p> <p>If you select this option, the service provisioner is prompted for the VLAN-ID range when creating a service order based on this service definition.</p> <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p>
VLAN Normalization	<p>Select a value:</p> <ul style="list-style-type: none"> • Normalize to VLAN all—To preserve customer VLAN IDs (and customer QoS priorities) across the network. <p>NOTE: For services that transport a range of VLANs, you must select VLAN Normalization to all. You cannot transport a range of VLANs without normalization.</p> • Normalized VLAN none—To preserve no VLAN IDs across the network. • Not normalized—If VLAN IDs are to be provided manually and are required to match. • Normalized to Dot1q—To transport only single-tagged frames across the network core. All port, dot1q, and Q-in-Q traffic is transported across the network • Normalized to QinQ—To transport only double-tagged frames across the network core. All port, dot1q, and Q-in-Q traffic is transported across the network. • Normalization not required—To specify no normalization for port-to-port services <p>NOTE: Starting with Release 1.0R2, when you newly install Connectivity Services Director, if you select the option to not require normalization in a service definition, the auto-pick option for VLAN IDs and the option to edit the auto-pick behavior in service order are disabled in the service definition. When you create a service order by associating with that service definition, you need to manually enter the VLAN IDs for the interfaces and cannot use the auto-pick functionality. This same behavior also applies to default service templates in which if you select the normalization-not-required functionality, the auto-pick option for VLAN IDs is disabled.</p> <p>For more information about VLAN normalization, see "Junos Space Layer 2 Services Overview" on page 55.</p> <p>For information about VLAN manipulation, see "Understanding VLAN Manipulation (Normalization and VLAN Mapping) on Ethernet Services" on page 88.</p>

Field	Action
Auto Pick VLAN ID	<p>Indicate how the VLAN ID is determined. By default, this check box is disabled.</p> <ul style="list-style-type: none"> Clear this check box to allow the service provider to specify the VLAN ID. This option is normally used when no VLAN normalization is applied. Specify the VLAN ID range in VLAN range for manual input. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p> <ul style="list-style-type: none"> Select this check box when VLAN normalization is applied. Specify the VLAN ID pool in VLAN range for auto-pick. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p> <p>NOTE: When the range of VLAN IDs that are automatically assigned by the system (with the auto-pick option enabled during the creation of a service definition) is less than or greater than the range of VLAN IDs that are manually specified (with the manual selection option enabled during the creation of a service definition), the following conditions apply during the creation of a service order with the Editable in Service Order check box selected during service definition creation:</p> <ul style="list-style-type: none"> If you create a service order with the auto-pick option enabled, the VLAN ID is selected from the auto-pick range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range. If you create a service order with the auto-pick option disabled, the VLAN ID is selected from the manually configured range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range.
VLAN range for auto-pick	<p>Specify the VLAN ID pool.</p> <p>Range: 1 through 4094</p>
VLAN range for manual input	<p>Specify the VLAN ID range.</p> <p>Range: 1 through 4094</p>
Outer Tag Protocol ID	<p>Select the outer tag protocol ID if the Customer traffic type is Transport single VLAN:</p> <ul style="list-style-type: none"> 0x88a8 0x8100 0x9100 <p>NOTE: For an interface, you must configure a physical port with the possible Tag Protocol Identifiers (TPID) either manually or through a template. Otherwise, the service creation fails for all TPIDs except 0x8100. To configure the TPIDs manually, use the following commands:</p>
Editable in Service Order	<p>To allow the service provisioner to override the outer tag protocol ID setting, select the check box for those options.</p>
Default Interface MTU (Bytes)	<p>The default MTU value is 1522 bytes. To allow the service provisioner to override the MTU setting, select the Editable in Service Order check box.</p>

Field	Action
MTU range for manual-config	<p>In the MTU range fields, type the lowest and highest values for MTU for each UNI.</p> <p>NOTE: To allow the service provisioner to override the MTU setting, select Editable in Service Order and, in the MTU range fields, type the highest and lowest MTU values.</p>
PE-CE Interface Rate-Limiting Settings	
Enable Interface Rate Limiting	<p>To enable a service provisioner to limit the available bandwidth, select this check box, and type a default bandwidth limit.</p> <p>NOTE: Bandwidth settings are available in the service definition when Manage CoS Profiles page is configured with CoS profiles.</p>
Default bandwidth (Mbps)	<p>Specify the default bandwidth value in Mbps.</p> <p>Default: 10 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps</p>
Min Bandwidth (Kbps)	<p>Specify the minimum bandwidth value in Kbps.</p> <p>Default: 1000 Kbps</p> <p>Range: 64 Kbps through 100,000 Kbps</p>
Max Bandwidth (Mbps)	<p>Specify the maximum bandwidth value in Mbps. For more information on maximum bandwidth see Table 79 on page 663</p> <p>Default: 100 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps</p>
Increment (Kbps)	<p>Specify a value that defines which values in the range is made available to the service provisioner.</p> <p>Default: 1000 Kbps</p> <p>Range: 64 Kbps through 100,000 Kbps</p>
Bandwidth – Burst Size Settings	
Burst Size Calculator	<p>Select the preferred option for calculating the burst size:</p> <ul style="list-style-type: none"> MTU Based If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902. The default value for MTU Factor is 10. Burst Period Based If you select the option Burst Period Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds. The default value for Burst Period is 1. <p>NOTE: The Burst Size Calculator list is enabled only when you select the Enable Interface Rate Limiting check box.</p>

2. Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

After you complete reviewing the settings, click **Finish** to complete the service definition creation.

UNI or Site Settings for Q-in-Q Interfaces in VPLS Services

To specify the site or UNI settings for q-in-q interfaces:

1. Fill in the fields on the **Site Settings** window.

Field	Action
PE-CE UNI Settings- Ethernet Encapsulation	
VLAN Tagging	<p>Select qinq from the list.</p> <p>The window expands to include options specific to Q-in-Q interfaces</p>
Physical Interface Encapsulation	Select the default physical encapsulation scheme to be used by service orders based on this service definition. We recommend you select flexible-ethernet-services .
Logical Interface Encapsulation	Constrained by your selection in the Physical IF encapsulation box. If you selected the recommended physical encapsulation mode of flexible-ethernet-services, then your only option is to select vlan-vpls for the logical encapsulation method.

Field	Action
Customer VLANs	<p>Transport all traffic Transports the traffic from all VLANs across the network. When you select this option, the service provisioner is prompted for the VLAN-ID when creating a service order based on this service definition. You need to specify only the Outer Tag protocol ID.</p> <p>Transport single vlan Transports traffic for a specific VLAN across the network. You need to specify both Outer Tag protocol ID and Inner Tag protocol ID.</p> <p>Transport VLAN range Limits the traffic across the network to a specific range of VLANs.</p> <p>If you select this option, the service provisioner is prompted for the VLAN-ID range when creating a service order based on this service definition. You need to specify both Outer Tag protocol ID and Inner Tag protocol ID.</p> <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p>
VLAN Normalization	<p>Select a value:</p> <ul style="list-style-type: none"> • Normalize to VLAN all—To preserve customer VLAN IDs (and customer QoS priorities) across the network. <p>NOTE: For services that transport a range of VLANs, you must select VLAN Normalization to all. You cannot transport a range of VLANs without normalization.</p> • Normalized VLAN none—To preserve no VLAN IDs across the network. • Not normalized—If VLAN IDs are to be provided manually and are required to match. • Normalized to Dot1q—To transport only single-tagged frames across the network core. All port, dot1q, and Q-in-Q traffic is transported across the network • Normalized to QinQ—To transport only double-tagged frames across the network core. All port, dot1q, and Q-in-Q traffic is transported across the network. • Normalization not required—To specify no normalization for port-to-port services <p>NOTE: Starting with Release 1.0R2, when you newly install Connectivity Services Director, if you select the option to not require normalization in a service definition, the auto-pick option for VLAN IDs and the option to edit the auto-pick behavior in service order are disabled in the service definition. When you create a service order by associating with that service definition, you need to manually enter the VLAN IDs for the interfaces and cannot use the auto-pick functionality. This same behavior also applies to default service templates in which if you select the normalization-not-required functionality, the auto-pick option for VLAN IDs is disabled.</p> <p>For more information about VLAN normalization, see “Junos Space Layer 2 Services Overview” on page 55.</p> <p>For information about VLAN manipulation, see “Understanding VLAN Manipulation (Normalization and VLAN Mapping) on Ethernet Services” on page 88.</p>

Field	Action
Auto Pick VLAN ID	<p>Indicate how the VLAN ID is determined. By default, this check box is disabled.</p> <ul style="list-style-type: none"> Clear this check box to allow the service provider to specify the VLAN ID. This option is normally used when no VLAN normalization is applied. Specify the VLAN ID range in VLAN range for manual input. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p> <ul style="list-style-type: none"> Select this check box when VLAN normalization is applied. Specify the VLAN ID pool in VLAN range for auto-pick. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p> <p>NOTE: When the range of VLAN IDs that are automatically assigned by the system (with the auto-pick option enabled during the creation of a service definition) is less than or greater than the range of VLAN IDs that are manually specified (with the manual selection option enabled during the creation of a service definition), the following conditions apply during the creation of a service order with the Editable in Service Order check box selected during service definition creation:</p> <ul style="list-style-type: none"> If you create a service order with the auto-pick option enabled, the VLAN ID is selected from the auto-pick range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range. If you create a service order with the auto-pick option disabled, the VLAN ID is selected from the manually configured range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range.
VLAN range for auto-pick:	<p>Specify the VLAN ID pool.</p> <p>Range: 1 through 4094</p>
VLAN range for manual input	<p>Specify the VLAN ID range.</p> <p>Range: 1 through 4094</p>
Outer Tag Protocol ID	<p>Select the outer tag protocol ID if the Customer traffic type is Transport single VLAN:</p> <ul style="list-style-type: none"> 0x88a8 0x8100 0x9100 <p>NOTE: For an interface, you must configure a physical port with the possible Tag Protocol Identifiers (TPID) either manually or through a template. Otherwise, the service creation fails for all TPIDs except 0x8100. To configure the TPIDs manually, use the following commands:</p> <pre> set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x9100 set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x88a8 set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x8100 </pre>

Field	Action
Inner Tag Protocol ID	<p>Select the inner tag protocol ID:</p> <ul style="list-style-type: none"> • 0x88a8 • 0x8100 • 0x9100 <p>NOTE: You cannot specify the Inner Tag protocol ID if the Customer traffic type is Transport single VLAN.</p>
Editable in Service Order	To allow the service provisioner to override the outer and inner tag protocol IDs, select the check boxes for those options.
Default Interface MTU (Bytes)	The default MTU value is 1522 bytes. To allow the service provisioner to override the MTU setting, select the Editable in Service Order check box.
MTU range for manual-config	<p>In the MTU range fields, type the lowest and highest values for MTU for each UNI.</p> <p>NOTE: To allow the service provisioner to override the MTU setting, select Editable in Service Order and, in the MTU range fields, type the highest and lowest MTU values.</p>
PE-CE Interface Rate-Limiting Settings	
Enable Interface Rate Limiting	<p>To enable a service provisioner to limit the available bandwidth, select this check box, and type a default bandwidth limit.</p> <p>NOTE: Bandwidth settings are available in the service definition when Manage CoS Profiles page is configured with CoS profiles.</p>
Default bandwidth (Mbps)	<p>Specify the default bandwidth value in Mbps.</p> <p>Default: 10 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps</p>
Min Bandwidth (Kbps)	<p>Specify the minimum bandwidth value in Kbps.</p> <p>Default: 1000 Kbps</p> <p>Range: 64 Kbps through 100,000 Kbps</p>
Max Bandwidth (Mbps)	<p>Specify the maximum bandwidth value in Mbps. For more information on maximum bandwidth see Table 79 on page 663</p> <p>Default: 100 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps</p>
Increment (Kbps)	<p>Specify a value that defines which values in the range is made available to the service provisioner.</p> <p>Default: 1000 Kbps</p> <p>Range: 64 Kbps through 100,000 Kbps</p>
Bandwidth – Burst Size Settings	

Field	Action
Burst Size Calculator	<p>Select the preferred option for calculating the burst size:</p> <ul style="list-style-type: none"> MTU Based If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902. The default value for MTU Factor is 10. Burst Period Based If you select the option Burst Period Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds. The default value for Burst Period is 1. <p>NOTE: The Burst Size Calculator list is enabled only when you select the Enable Interface Rate Limiting check box.</p>

- Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

After you complete reviewing the settings, click **Finish** to complete the service definition creation.

UNI Settings for Services with Flexible VLAN Tagging (Asymmetric Interface Types)

You can specify the Ethernet option **asymmetric tag depth** to create a service that includes any combination of port-based interfaces, 802.1Q interfaces, and Q-in-Q interfaces.

To specify the UNI Settings for q-in-q interfaces:

Create VPLS Service Definition.

General Settings

Site Settings

Review

You are here: Site Settings

PE-CE Interface Settings- Ethernet Encapsulation

VLAN Tagging:

asymmetric tag depth

Physical Interface Encapsulation:

flexible-ethernet-services

Logical Interface Encapsulation:

vlan-vpls

Traffic Type:

Transport single vlan

VLAN Normalization:

Normalization not required

☒ Auto Pick VLAN ID

☐ Editable in Service Order

VLAN ID range for auto-pick:

1 - 4094

VLAN ID range for manual-config:

1 - 4094

Outer Tag Protocol ID:

Inner Tag Protocol ID:

Default Interface MTU:

1522

☐ Editable in Service Order

MTU range for manual-config:

1522 - 9192

PE-CE Interface Rate Limiting Settings

Back

Next

Done

Cancel

1. Fill in the fields on the **Site Settings** window.

Field	Action
PE-CE UNI Settings- Ethernet Encapsulation	
VLAN Tagging	Select asymmetric tag depth from the list.
Physical Interface Encapsulation	<p>Select the default physical encapsulation scheme to be used by service orders based on this service definition. We recommend you select flexible-ethernet-services.</p> <p>For multipoint-to-multipoint services with Q-in-Q interfaces, the only option is flexible-ethernet-services</p>
Logical Interface Encapsulation	Constrained by your selection in the Physical IF encapsulation box. If you selected the recommended physical encapsulation mode of flexible-ethernet-services, then your only option is to select vlan-vpls for the logical encapsulation method.
Customer VLANs	<p>Transport all traffic Transports the traffic from all VLANs across the network. When you select this option, the service provisioner is prompted for the VLAN-ID when creating a service order based on this service definition. You need to specify only the Outer Tag protocol ID and Inner Tag protocol ID.</p> <p>Transport single vlan Transports traffic for a specific VLAN across the network. You need to specify both Outer Tag protocol ID and Inner Tag protocol ID.</p> <p>Transport VLAN range Limits the traffic across the network to a specific range of VLANs. You need to specify both Outer Tag protocol ID and Inner Tag protocol ID.</p> <p>If you select this option, the service provisioner is prompted for the VLAN-ID range when creating a service order based on this service definition.</p> <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p>

Field	Action
VLAN Normalization	<p>Select a value:</p> <ul style="list-style-type: none"> • Normalize to VLAN all—To preserve customer VLAN IDs (and customer QoS priorities) across the network. <p>NOTE: For services that transport a range of VLANs, you must select VLAN Normalization to all. You cannot transport a range of VLANs without normalization.</p> <ul style="list-style-type: none"> • Normalized VLAN none—To preserve no VLAN IDs across the network. • Not normalized—If VLAN IDs are to be provided manually and are required to match. • Normalized to Dot1q—To transport only single-tagged frames across the network core. All port, dot1q, and Q-in-Q traffic is transported across the network • Normalized to QinQ—To transport only double-tagged frames across the network core. All port, dot1q, and Q-in-Q traffic is transported across the network. • Normalization not required—To specify no normalization for port-to-port services <p>NOTE: Starting with Release 1.0R2, when you newly install Connectivity Services Director, if you select the option to not require normalization in a service definition, the auto-pick option for VLAN IDs and the option to edit the auto-pick behavior in service order are disabled in the service definition. When you create a service order by associating with that service definition, you need to manually enter the VLAN IDs for the interfaces and cannot use the auto-pick functionality. This same behavior also applies to default service templates in which if you select the normalization-not-required functionality, the auto-pick option for VLAN IDs is disabled.</p> <p>For more information about VLAN normalization, see “Junos Space Layer 2 Services Overview” on page 55.</p> <p>For information about VLAN manipulation, see “Understanding VLAN Manipulation (Normalization and VLAN Mapping) on Ethernet Services” on page 88.</p>

Field	Action
Auto Pick VLAN ID	<p>Indicate how the VLAN ID is determined. By default, this check box is disabled.</p> <ul style="list-style-type: none"> Clear this check box to allow the service provider to specify the VLAN ID. This option is normally used when no VLAN normalization is applied. Specify the VLAN ID range in VLAN range for manual input. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p> <ul style="list-style-type: none"> Select this check box when VLAN normalization is applied. Specify the VLAN ID pool in VLAN range for auto-pick. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p> <p>NOTE: When the range of VLAN IDs that are automatically assigned by the system (with the auto-pick option enabled during the creation of a service definition) is less than or greater than the range of VLAN IDs that are manually specified (with the manual selection option enabled during the creation of a service definition), the following conditions apply during the creation of a service order with the Editable in Service Order check box selected during service definition creation:</p> <ul style="list-style-type: none"> If you create a service order with the auto-pick option enabled, the VLAN ID is selected from the auto-pick range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range. If you create a service order with the auto-pick option disabled, the VLAN ID is selected from the manually configured range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range.
VLAN range for auto-pick:	<p>Specify the VLAN ID pool.</p> <p>Range: 1 through 4094</p>
VLAN range for manual input	<p>Specify the VLAN ID range.</p> <p>Range: 1 through 4094</p>
Outer Tag Protocol ID	<p>Select the outer tag protocol ID if the Customer traffic type is Transport single VLAN:</p> <ul style="list-style-type: none"> 0x88a8 0x8100 0x9100 <p>NOTE: For an interface, you must configure a physical port with the possible Tag Protocol Identifiers (TPID) either manually or through a template. Otherwise, the service creation fails for all TPIDs except 0x8100. To configure the TPIDs manually, use the following commands:</p> <pre> set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x9100 set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x88a8 set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x8100 </pre>

Field	Action
Inner Tag Protocol ID	<p>Select the inner tag protocol ID:</p> <ul style="list-style-type: none"> • 0x88a8 • 0x8100 • 0x9100 <p>NOTE: You cannot specify the Inner Tag protocol ID if the Customer traffic type is Transport all traffic.</p>
Editable in Service Order	To allow the service provisioner to override the outer and inner tag protocol IDs, select the check boxes for those options.
MTU range for manual-config	<p>In the MTU range fields, type the lowest and highest values for MTU that the service provisioner can type, for each UNI</p> <p>NOTE: To allow the service provisioner to override the MTU setting, select Editable in Service Order and, in the MTU range fields, type the highest and lowest MTU values that the service provisioner can type.</p>
Default Interface MTU (Bytes)	The default MTU value is 1522 bytes. To allow the service provisioner to override the MTU setting, select the Editable in Service Order check box.
PE-CE Interface Rate-Limiting Settings	
Enable Interface Rate Limiting	<p>To enable a service provisioner to limit the available bandwidth, select this check box, and type a default bandwidth limit.</p> <p>NOTE: Bandwidth settings are available in the service definition when Manage CoS Profiles page is configured with CoS profiles.</p>
Default bandwidth (Mbps)	<p>Specify the default bandwidth value in Mbps.</p> <p>Default: 10 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps</p>
Min Bandwidth (Kbps)	<p>Specify the minimum bandwidth value in Kbps.</p> <p>Default: 1000 Kbps</p> <p>Range: 64 Kbps through 100,000 Kbps</p>
Max Bandwidth (Mbps)	<p>Specify the maximum bandwidth value in Mbps. For more information on maximum bandwidth see Table 79 on page 663</p> <p>Default: 100 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps</p>
Increment (Kbps)	<p>Specify a value that defines which values in the range is made available to the service provisioner.</p> <p>Default: 1000 Kbps</p> <p>Range: 64 Kbps through 100,000 Kbps</p>

Field	Action
Bandwidth – Burst Size Settings	
Burst Size Calculator	<p>Select the preferred option for calculating the burst size:</p> <ul style="list-style-type: none"> MTU Based If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902. The default value for MTU Factor is 10. Burst Period Based If you select the option Burst Period Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds. The default value for Burst Period is 1. <p>NOTE: The Burst Size Calculator list is enabled only when you select the Enable Interface Rate Limiting check box.</p>

- Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

After you complete reviewing the settings, click **Finish** to complete the service definition creation.

Reviewing the Configured Settings

The Review page of the service definition or service order creation and modification wizards enable you to view and evaluate the service parameters and components you configured in preceding steps or pages of the wizard. This page provides a comprehensive, single-page view of all the service elements configured in the different pages of the wizard. You can either click the buttons corresponding to the various settings at the top of the wizard page to directly traverse to the page you want to modify or click the navigation buttons at the bottom of the wizard page to go to the different pages of the wizard.



NOTE: On the Review page, in the Service Templates section, the names of the service templates with which the service definition is associated are displayed. The Default Service Template column indicates whether the attached template is the default template.

To examine and modify the configured service definition settings:

1. Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify.
2. Click **Edit** next to the section that contains the parameter you want to modify. You are navigated to the corresponding page of the wizard in which the parameter settings are defined.
3. Click **Finish** to save the service definition or service order.
4. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

The service order inventory window appears.

**Related
Documentation**

- [Creating a Multipoint-to-Multipoint VPLS Service Definition on page 653](#)
- [Creating a Service Definition for VPLS Access into Layer 3 Networks on page 705](#)

Creating a Point-to-Multipoint VPLS Service Definition

This procedure provides the steps to create a definition for a point-to-multipoint Ethernet service. Point-to-multipoint services are also known as hub and spoke services.

The standard service definitions that came with your initial software installation are designed to be appropriate for most requirements. You can also create a customized service definition—for example, to set different bandwidth limits on the service than those offered in the standard service definitions.

When the new service definition is complete and published, network operators or service provisioners can use the completed service definition as a base for creating and then activating point-to-multipoint Ethernet services on the network.

The windows appear in the order stated. You can, however, perform these steps in any order by accessing them through the task list in the right panel. If the panel is not visible, click the snap tool on the right side of the main display area.

- [Specifying General Information for Point-to-Multipoint VPLS Service Definitions on page 679](#)
- [Specifying Advanced Settings on page 684](#)
- [Specifying UNI or Site Settings for Point-to-Multipoint VPLS Service Definitions on page 686](#)
- [UNI or Site Settings for Port-to-Port Interfaces in VPLS Services on page 686](#)
- [UNI or Site Settings for 802.1Q Interfaces in VPLS Services on page 689](#)

- [UNI or Site Settings for Q-in-Q Interfaces in VPLS Services](#) on page 694
- [UNI or Site Settings for Services with Flexible VLAN Tagging \(Asymmetric Interface Types\)](#) on page 699
- [Reviewing the Configured Settings](#) on page 704

Specifying General Information for Point-to-Multipoint VPLS Service Definitions

in the Network Services > Connectivity view pane, select **Service Design > Manage Service Definitions > New > VPLS Service Definition**. The **General** settings window appears.

To specify the general information for a point-to-multipoint service definition:

1. Fill in the fields on the **General** page of the wizard that enables you to create a service definition.

Field	Action
Service Definition Name	Type a name for the service definition.
Service Type	Select Point-to-Multipoint Ethernet (VPLS)
Signaling	<p>Select a signaling type:</p> <ul style="list-style-type: none"> • BGP— If BGP signaling is selected, the following fields are available in the Connectivity section of the General Settings page: <ul style="list-style-type: none"> • Route target • Route distinguisher • VLAN normalization • MAC Settings • VCID, if Enable PW Extension is enabled • LDP—If LDP signaling is selected, the following fields are available in the Connectivity section of the General Settings page: <ul style="list-style-type: none"> • Enable BGP-based Auto Discovery • Auto-pick Route target, if Auto Discovery is enabled • Auto-pick Route distinguisher, if Auto Discovery is enabled • Auto-pick VPLS ID, if Auto Discovery is disabled • Auto-pick VPN ID, if Auto Discovery is enabled • VLAN normalization • Mac Security Settings <p>NOTE: You cannot edit the Signaling type in the service order.</p>
Description (Optional)	<p>Type a brief description or other comment that you want to appear in the Service Definition table.</p> <p>Range: 0 through 200 characters. Space and special characters are allowed.</p>
Enable QoS	<p>When you enable QoS in the service definition, you can specify a QoS profile in the service order to classify traffic into defined service groups to provide the special treatment of traffic across the network service. For example, voice traffic can be sent across certain links, and data traffic can use other links.</p>

Field	Action
Enable L3 Access	<p>Select this check box to create the link into Layer 3. If this check box is selected, the available Ethernet option in the Site Settings window are:</p> <ul style="list-style-type: none"> • dot1q • qinq
Enable PW Extension	Select this check box to enable pseudowire extension. You cannot edit this check box in the service order.
Enable PW Resiliency	<p>Select this check box to enable resiliency. You cannot edit this field in the service order.</p> <p>If the Signaling type is BGP, you need to select the Enable PW Extension check box to enable the Enable PW Resiliency check box.</p> <p>For more information of pseudowire redundancy, see "Redundant Pseudowires for Layer 2 Circuits and VPLS" on page 94.</p>
Enable Static PW Labels	<p>Select this check box to enable a pseudowire connection by configuring static values.</p> <p>NOTE: The Enable Static PW Labels check box is enabled for both signaling types: LDP and BGP.</p> <p>When the signaling type is BGP, selection of this check box enables the Enable PW Resiliency check box and automatically selects the Enable PW Extension check box.</p>
Service Template	<p>(Optional) To include a service template for the service, click the Add icon or plus sign (+) to select a service template from the Service Template list. The list of available service templates is displayed. Select the check box beside the template you want and click OK. You are returned to the General Settings page.</p> <p>The selected service template appears in the Default Service Template field.</p> <p>You can select one or more service templates as the default service template. By default, the default service templates are attached to the endpoints.</p> <p>NOTE: You cannot add or delete a service template while creating a service order.</p> <p>The remaining service templates on the Service Template list are termed as optional service templates. You can attach the optional service templates to the endpoints on a need basis.</p> <p>In the View Service Definition Details window, the value for the default service template in the Default Service Template column is <i>True</i>.</p> <p>For instructions on creating a service template, see "Creating a Service Template" on page 1815.</p>
BGP Connectivity Settings —This section is displayed if you select the signaling type as BGP.	
Auto-pick Route Target	<p>Select this check box to enable route target to be configured automatically. Deselect the check box if you want the route target to be manually configured. By default, manual configuration of route target is enabled.</p> <p>To override this setting in the service order, select the Editable in Service Order check box.</p>

Field	Action
Auto-pick Route Distinguisher	<p>Define a route distinguisher option:</p> <ul style="list-style-type: none"> • Select the check box to enable the service provider to specify the route distinguisher. • Select the check box to enable the route distinguisher to be selected automatically. <p>To override this setting in the service order, select the Editable in Service Order check box.</p>
LDP Connectivity Settings —This section is displayed if you select the signaling type as LDP.	
Enable BGP-based Auto Discovery	<p>You cannot enable or disable the Auto Discovery check box if you have enabled the Enable PW Extension or the Enable PW Resiliency check boxes.</p> <p>This check box is available only if the signaling type is LDP.</p> <p>NOTE: If the Enable Static PW Labels check box in the General window is checked for the LDP signaling, then the Auto Discovery check box is disabled in the Connectivity Settings page.</p> <p>The Auto Discovery check box is not available in the Connectivity Settings page when the signaling type is BGP.</p> <p>On enabling the auto discovery, the following fields are available:</p> <ul style="list-style-type: none"> • Route target • Route distinguisher • VPN ID <p>On disabling the auto discovery specify the VPLS ID.</p>
Auto-pick VPLS ID or VPN ID	<p>This field is available only if the signaling type is LDP and auto discovery is disabled.</p> <p>Identifies the virtual circuit identifier used for the VPLS routing instance and the VPN ID associated with the router.</p> <p>Select this check box to enable the VPLS ID and VPN ID to be configured automatically. Deselect the check box if you want these attributes to be manually configured. By default, manual configuration is enabled.</p>
Auto-pick Route Target	Select this check box to enable route target to be configured automatically. Deselect the check box if you want the route target to be manually configured. By default, manual configuration of route target is enabled.
Auto-pick Route Distinguisher	<p>Define a route distinguisher option:</p> <ul style="list-style-type: none"> • Select the check box to enable the service provider to specify the route distinguisher. • Select the check box to enable the route distinguisher to be selected automatically. <p>To override this setting in the service order, select the Editable in Service Order check box.</p>
MAC Settings	
MAC learning	To enable MAC learning , select the check box.
Interface MAC limit	<p>Maximum number of MAC addresses learned from an interface.</p> <p>Range: 1 through 131071 MAC addresses per interface</p>

Field	Action
MAC statistics	To enable MAC statistic , select the check box.
MAC Table Size	<p>Modify the size of the MAC address table for the bridge domain.</p> <p>Range: 16 through 1048575</p> <p>To allow the service provisioner to override the MAC settings, select Editable in Service Order.</p>
Enable L3 Access	<p>Select this check box to create the link into Layer 3. If you enable the Layer 3 access, the available Ethernet option in the Site Settings are:</p> <ul style="list-style-type: none"> • port-port • dot1q • QinQ • asymmetric tag depth
Enable PW Extension	Select this check box to enable pseudowire extension. You cannot edit this check box in the service order.
Enable PW Resiliency	<p>Select this check box to enable resiliency. You cannot edit this field in the service order.</p> <p>If the Signaling type is BGP, you need to select the Enable PW Extension check box to enable the Enable PW Resiliency check box.</p> <p>For more information of pseudowire redundancy, see “Redundant Pseudowires for Layer 2 Circuits and VPLS” on page 94.</p>
Enable Static PW Labels	<p>Select this check box to enable a pseudowire connection by configuring static values.</p> <p>NOTE: The Enable Static PW Labels check box is enabled for both signaling types: LDP and BGP.</p> <p>When the signaling type is BGP, selection of this check box enables the Enable PW Resiliency check box and automatically selects the Enable PW Extension check box.</p>
Service Template Definition	<p>(Optional) To include a service template for the service, click the Add icon or plus sign (+) to select a service template from the Service Template list. The list of available service templates is displayed. Select the check box beside the template you want and click OK. You are returned to the General Settings page.</p> <p>The selected service template appears in the Default Service Template field.</p> <p>You can select one or more service templates as the default service template. By default, the default service templates are attached to the endpoints.</p> <p>NOTE: You cannot add or delete a service template while creating a service order.</p> <p>The remaining service templates on the Service Template list are termed as optional service templates. You can attach the optional service templates to the endpoints on a need basis.</p> <p>In the View Service Definition Details window, the value for the default service template in the Default Service Template column is <i>True</i>.</p> <p>For instructions on creating a service template, see “Creating a Service Template” on page 1815.</p>

2. Click **Next** to save the information. Continue with [“Specifying Advanced Settings”](#) on [page 684](#).

Specifying Advanced Settings

In this step, you can specify the parameters that define advanced connectivity between sites across the service provider network. These settings can be configured in the **Advanced** settings section of the General Settings page of the Create VPLS Service Definition wizard.

1. Fill in the fields as indicated in the table.

Advanced Settings—This section enables you to specify the parameters that define advanced connectivity between sites across the service provider network

Include	<p>Select the Include check box for each advanced setting that you want to include in the service definition.</p> <p>NOTE: If you select any advanced parameters for a service definition, you must also select the Include check box for the Disable tunnel services parameter, and select or clear the Disable tunnel services check box.</p> <p>For MX Series devices, if you deploy a VPLS service without selecting the Include check box for Disable tunnel services parameter, the VPLS service is down. As a work around, you can push the configuration to each PE device for the service by running the following command:</p> <pre>root@test_device# set chassis fpc 0 pic 1 tunnel-services bandwidth 1g</pre>
Disable Tunnel Services	<p>Enable or disable tunnel-services to specify that traffic for particular VPLS routing instances be forwarded to specific virtual tunnel (VT) interfaces.</p> <ul style="list-style-type: none"> To enable tunnel-services, clear the Disable Tunnel Services check box. To disable tunnel-services, select the Disable Tunnel Services check box (default).
Disable Local Switching	<p>Enable or disable local switching. In local switching mode, you can terminate multiple Layer 2 circuit pseudowires at a single VPLS mesh group:</p> <ul style="list-style-type: none"> To enable local switching across the network, clear the Disable Local Switching check box. To disable local switching across the network, select the Disable Local Switching check box (default).
Fast Reroute-Priority	<p>In this drop-down list, specify the reroute priority for a VPLS routing instance:</p> <ul style="list-style-type: none"> HIGH—Set the fast reroute priority for a VPLS routing instance to high. During a fast reroute event, the router repairs next hops for high-priority VPLS routing instances first. MEDIUM—Set the fast reroute priority for a VPLS routing instance to medium. During a fast reroute event, the router repairs next hops for medium-priority VPLS instances after high-priority VPLS routing instances but before low-priority VPLS routing instances. LOW—Set the fast reroute priority for a VPLS routing instance to low, which is the default. During a fast reroute event, the router repairs next hops for low-priority VPLS routing instances last.
Label Block Size	<p>Configure the label block size for VPLS labels by using one of the following values.</p> <ul style="list-style-type: none"> 2—Allocate the label blocks in increments of 2. Use this setting for a VPLS domain that has only two sites with no future expansion plans. 4—Allocate the label blocks in increments of 4. 8—Allocate the label blocks in increments of 8. This is the default. 16—Allocate the label blocks in increments of 16. A label block size of 16 enables you to minimize the number of routes in the VPLS domain. Use this setting only if the number of routes is the primary concern. <p>NOTE: This field is unavailable if the Signaling type is LDP and the Auto discovery check box is enabled.</p>

Connectivity type

Select a connection-type to specify when a VPLS connection is taken down, depending on whether the interface for the VPLS routing instance is customer-facing or integrated routing and bridging (IRB):

- **ce**—Require that for the VPLS connection to be up, the customer-facing interface for the VPLS routing instance must also be up. If the customer-facing interface fails, the VPLS connection is taken down. This is the default.
- **irb**—Allow a VPLS connection to remain up so long as an IRB interface is configured for the VPLS routing instance.

NOTE: This field is unavailable if the **Signaling** type is LDP and the **Auto discovery** is enabled.

Editable in Service Order

By default, each advanced setting that you include in the service definition can be edited in the service order. To prevent the service provisioner from overriding an advanced setting in the service order, clear the **Editable in Service Order** check box.

2. Click **Next** to define the UNI or site parameters. Alternatively, click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.
3. Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.
4. After you complete reviewing the settings, click **Finish** to complete the service definition creation.

Specifying UNI or Site Settings for Point-to-Multipoint VPLS Service Definitions

In this step, you provide the UNI attributes for this service definition. The attributes you set depend on the type of interface you are using in this VPLS service definition. The following interface types are supported:

- ports
- 802.1Q interfaces
- Q-in-Q interfaces
- asymmetric interface

UNI or Site Settings for Port-to-Port Interfaces in VPLS Services

The **Site Settings** window provides four expanding or collapsing panels: Traffic Treatment, Interface Settings, MTU Settings, and Bandwidth Settings.

To specify the UNI Settings for Port-to-Port interfaces:

1. Fill in the fields on the **Site Settings** window.

Field	Action
PE-CE UNI Settings- Ethernet Encapsulation	
VLAN Tagging	<p>Select port-port from the list.</p> <p>The VLAN tagging option you choose determines the other options you can select and specify on the page.</p>
Editable in Service Order	To allow the service provisioner to override the VLAN tagging or Ethernet option attribute, select the check box.
LDP PW Extension Settings	
<p>NOTE: The LDP PW Extension Settings is available only if you have selected the Enable PW Extension check box in the General tab.</p>	
Physical Interface Encapsulation	In the Physical IF encapsulation box, select ethernet-ccc , which is the only valid physical interface encapsulation method for port-to-port services.
Logical Interface Encapsulation	You can not select a choice in this field because it is not relevant to port-to-port services.
Customer VLANs	This drop-down list is disabled for port-to-port services. For port-to-port services, all traffic is always transported.
VLAN Normalization	<p>Select a value:</p> <ul style="list-style-type: none"> • Normalize to VLAN all—To preserve customer VLAN IDs (and customer QoS priorities) across the network. <p>NOTE: For services that transport a range of VLANs, you must select VLAN Normalization to all. You cannot transport a range of VLANs without normalization.</p> <ul style="list-style-type: none"> • Normalized VLAN none—To preserve no VLAN IDs across the network. • Not normalized—If VLAN IDs are to be provided manually and are required to match. • Normalized to Dot1q—To transport only single-tagged frames across the network core. All port, dot1q, and Q-in-Q traffic is transported across the network • Normalized to QinQ—To transport only double-tagged frames across the network core. All port, dot1q, and Q-in-Q traffic is transported across the network. • Normalization not required—To specify no normalization for port-to-port services <p>NOTE: Starting with Release 1.0R2, when you newly install Connectivity Services Director, if you select the option to not require normalization in a service definition, the auto-pick option for VLAN IDs and the option to edit the auto-pick behavior in service order are disabled in the service definition. When you create a service order by associating with that service definition, you need to manually enter the VLAN IDs for the interfaces and cannot use the auto-pick functionality. This same behavior also applies to default service templates in which if you select the normalization-not-required functionality, the auto-pick option for VLAN IDs is disabled.</p> <p>For more information about VLAN normalization, see “Junos Space Layer 2 Services Overview” on page 55.</p> <p>For information about VLAN manipulation, see “Understanding VLAN Manipulation (Normalization and VLAN Mapping) on Ethernet Services” on page 88.</p>

Field	Action
Auto Pick VLAN ID	This check box is disabled because in port-to-port services, all traffic and all VLANs on one port are transported to all other ports.
Editable in Service Order	To allow the service provisioner to override the VLAN ID setting, select the check box. This check box is not applicable for port-to-port services.
Default Interface MTU (Bytes)	The default MTU value is 1522 bytes.
MTU Range for manual-config(Bytes)	Specify the low and high values to define the MTU range that you want to define. The default range is 1522 through 9192 bytes.
PE-CE Interface Rate-Limiting Settings	
Enable Interface Rate Limiting	To enable a service provisioner to limit the available bandwidth, select this check box, and type a default bandwidth limit. NOTE: Bandwidth settings are available in the service definition when Manage CoS Profiles page is configured with CoS profiles.
Default bandwidth (Mbps)	Specify the default bandwidth value in Mbps. Default: 10 Mbps Range: 1 Mbps through 100,000 Mbps
Min Bandwidth (Kbps)	Specify the minimum bandwidth value in Kbps. Default: 1000 Kbps Range: 64 Kbps through 100,000 Kbps
Max Bandwidth (Mbps)	Specify the maximum bandwidth value in Mbps. For more information on maximum bandwidth see Table 79 on page 663 Default: 100 Mbps Range: 1 Mbps through 100,000 Mbps
Increment (Kbps)	Specify a value that defines which values in the range is made available to the service provisioner. Default: 1000 Kbps Range: 64 Kbps through 100,000 Kbps
Bandwidth – Burst Size Settings	

Field	Action
Burst Size Calculator	<p>Select the preferred option for calculating the burst size:</p> <ul style="list-style-type: none"> MTU Based If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902. The default value for MTU Factor is 10. Burst Period Based If you select the option Burst Period Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds. The default value for Burst Period is 1. <p>NOTE: The Burst Size Calculator list is enabled only when you select the Enable Interface Rate Limiting check box.</p>

The following table lists the **Max Bandwidth (Mbps)** for the M Series, MX Series, and ACX Series Routers:

Table 80: Maximum Bandwidth for M Series, MX Series, and ACX Series Routers

M Series IQ2E PIC		M Series IQ2 PIC		MX Series 3D PIC		MX Series Non-3D PIC		ACX 2000	
GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)
32,000 Mbps or 32 Gbps	32,000 Mbps or 32 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps	100,000 Mbps or 100 Gbps	100,000 Mbps or 100 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps

- Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

After you complete reviewing the settings, click **Finish** to complete the service definition creation.

UNI or Site Settings for 802.1Q Interfaces in VPLS Services

To specify the UNI Settings for 802.1Q interfaces:

- Fill in the fields on the **Site Settings** window.

Field	Action
PE-CE UNI Settings- Ethernet Encapsulation	

Field	Action
VLAN Tagging	<p>Select dot1q from the list.</p> <p>The Ethernet option you choose determines the other options you can select and specify on the page.</p>
Physical IF encapsulation	In the Physical IF encapsulation box, select the default physical encapsulation scheme to be used by service orders based on this service definition. For point-to-multipoint services with 802.1Q interfaces, the only option is flexible-ethernet-services .
Logical IF encapsulation	The Logical IF encapsulation field is constrained by your selection in the Physical IF encapsulation field. For the physical encapsulation mode of flexible-ethernet-services, your only option is to select vlan-vpls for the logical encapsulation method.
LDP PW Extension Settings	
<p>NOTE: The LDP PW Extension Settings is available only if you have selected the Enable PW Extension check box in the General tab.</p>	
Physical IF encapsulation	<p>In the Physical IF encapsulation box, select one of the following options:</p> <ul style="list-style-type: none"> vlan-ccc extended-vlan-ccc flexible-ethernet-services
Logical IF encapsulation	<p>The Logical IF encapsulation field is constrained by your selection in the Physical IF encapsulation field.</p> <p>For the physical encapsulation mode of vlan-ccc or flexible-ethernet-services, your only option is to select vlan-ccc for the logical encapsulation method.</p> <p>For the physical encapsulation mode of extended-vlan-ccc, your only option is to select extended-vlan-ccc for the logical encapsulation method.</p>
Customer VLANs	<p>Single VLAN is the only option for 802.1Q interface types.</p> <p>Select Transport single vlan to transport the traffic for a specific VLAN across the network. When you select this option, the service provisioner is prompted for the VLAN-ID when creating a service order based on this service definition. You need to specify the Outer Tag protocol ID.</p> <p>Select Transport VLAN range to limit the traffic across the network to a specific range of VLANs.</p> <p>If you select this option, the service provisioner is prompted for the VLAN-ID range when creating a service order based on this service definition.</p> <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p>

Field	Action
VLAN Normalization	<p>Select a value:</p> <ul style="list-style-type: none"> • Normalize to VLAN all—To preserve customer VLAN IDs (and customer QoS priorities) across the network. <p>NOTE: For services that transport a range of VLANs, you must select VLAN Normalization to all. You cannot transport a range of VLANs without normalization.</p> <ul style="list-style-type: none"> • Normalized VLAN none—To preserve no VLAN IDs across the network. • Not normalized—If VLAN IDs are to be provided manually and are required to match. • Normalized to Dot1q—To transport only single-tagged frames across the network core. All port, dot1q, and Q-in-Q traffic is transported across the network • Normalized to QinQ—To transport only double-tagged frames across the network core. All port, dot1q, and Q-in-Q traffic is transported across the network. • Normalization not required—To specify no normalization for port-to-port services <p>NOTE: Starting with Release 1.0R2, when you newly install Connectivity Services Director, if you select the option to not require normalization in a service definition, the auto-pick option for VLAN IDs and the option to edit the auto-pick behavior in service order are disabled in the service definition. When you create a service order by associating with that service definition, you need to manually enter the VLAN IDs for the interfaces and cannot use the auto-pick functionality. This same behavior also applies to default service templates in which if you select the normalization-not-required functionality, the auto-pick option for VLAN IDs is disabled.</p> <p>For more information about VLAN normalization, see “Junos Space Layer 2 Services Overview” on page 55.</p> <p>For information about VLAN manipulation, see “Understanding VLAN Manipulation (Normalization and VLAN Mapping) on Ethernet Services” on page 88.</p>

Field	Action
Auto Pick VLAN ID	<p>Indicate how the VLAN ID is determined. By default, this check box is disabled.</p> <ul style="list-style-type: none"> Clear this check box to allow the service provider to specify the VLAN ID. This option is normally used when no VLAN normalization is applied. Specify the VLAN ID range in VLAN range for manual input. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p> <ul style="list-style-type: none"> Select this check box when VLAN normalization is applied. Specify the VLAN ID pool in VLAN range for auto-pick. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p> <p>NOTE: When the range of VLAN IDs that are automatically assigned by the system (with the auto-pick option enabled during the creation of a service definition) is less than or greater than the range of VLAN IDs that are manually specified (with the manual selection option enabled during the creation of a service definition), the following conditions apply during the creation of a service order with the Editable in Service Order check box selected during service definition creation:</p> <ul style="list-style-type: none"> If you create a service order with the auto-pick option enabled, the VLAN ID is selected from the auto-pick range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range. If you create a service order with the auto-pick option disabled, the VLAN ID is selected from the manually configured range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range.
VLAN range for auto-pick	<p>Specify the VLAN ID pool.</p> <p>Range: 1 through 4094</p>
VLAN range for manual input	<p>Specify the VLAN ID range.</p> <p>Range: 1 through 4094</p>
Outer Tag Protocol ID	<p>Select the outer tag protocol ID if the Customer traffic type is Transport single VLAN:</p> <ul style="list-style-type: none"> 0x88a8 0x8100 0x9100 <p>NOTE: For an interface, you must configure a physical port with the possible Tag Protocol Identifiers (TPID) either manually or through a template. Otherwise, the service creation fails for all TPIDs except 0x8100. To configure the TPIDs manually, use the following commands:</p> <pre> set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x9100 set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x88a8 set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x8100 </pre>
Editable in Service Order	<p>To allow the service provisioner to override the outer tag protocol ID setting, select the check box for those options.</p>

Field	Action
Default Interface MTU (Bytes)	The default MTU value is 1522 bytes. To allow the service provisioner to override the MTU setting, select the Editable in Service Order check box.
MTU range for manual-config	<p>In the MTU range fields, type the lowest and highest values for MTU for each UNI.</p> <p>NOTE: To allow the service provisioner to override the MTU setting, select Editable in Service Order and, in the MTU range fields, type the highest and lowest MTU values.</p>
PE-CE Interface Rate-Limiting Settings	
Enable Interface Rate Limiting	<p>To enable a service provisioner to limit the available bandwidth, select this check box, and type a default bandwidth limit.</p> <p>NOTE: Bandwidth settings are available in the service definition when Manage CoS Profiles page is configured with CoS profiles.</p>
Default bandwidth (Mbps)	<p>Specify the default bandwidth value in Mbps.</p> <p>Default: 10 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps</p>
Min Bandwidth (Kbps)	<p>Specify the minimum bandwidth value in Kbps.</p> <p>Default: 1000 Kbps</p> <p>Range: 64 Kbps through 100,000 Kbps</p>
Max Bandwidth (Mbps)	<p>Specify the maximum bandwidth value in Mbps. For more information on maximum bandwidth see Table 79 on page 663</p> <p>Default: 100 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps</p>
Increment (Kbps)	<p>Specify a value that defines which values in the range is made available to the service provisioner.</p> <p>Default: 1000 Kbps</p> <p>Range: 64 Kbps through 100,000 Kbps</p>
Bandwidth – Burst Size Settings	

Field	Action
Burst Size Calculator	<p>Select the preferred option for calculating the burst size:</p> <ul style="list-style-type: none"> • MTU Based If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902. The default value for MTU Factor is 10. • Burst Period Based If you select the option Burst Period Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds. The default value for Burst Period is 1. <p>NOTE: The Burst Size Calculator list is enabled only when you select the Enable Interface Rate Limiting check box.</p>

2. Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

After you complete reviewing the settings, click **Finish** to complete the service definition creation.

UNI or Site Settings for Q-in-Q Interfaces in VPLS Services

To specify the UNI Settings for q-in-q interfaces:

1. Fill in the fields on the **Site Settings** window.

Field	Action
PE-CE UNI Settings- Ethernet Encapsulation	
VLAN Tagging	<p>Select qinq from the list.</p> <p>The window expands to include options specific to Q-in-Q interfaces</p>
Physical IF encapsulation	<p>In the Physical IF encapsulation box, select the default physical encapsulation scheme to be used by service orders based on this service definition. For point-to-multipoint services with 802.1Q interfaces, the only option is flexible-ethernet-services.</p>
Logical IF encapsulation	<p>The Logical IF encapsulation field is constrained by your selection in the Physical IF encapsulation field. For the physical encapsulation mode of flexible-ethernet-services, your only option is to select vlan-vpls for the logical encapsulation method.</p>

LDP PW Extension Settings

NOTE: The **LDP PW Extension Settings** is available only if you have selected the **Enable PW Extension** check box in the General tab.

Field	Action
Physical IF encapsulation	<p>In the Physical IF encapsulation box, select one of the following options:</p> <ul style="list-style-type: none"> • vlan-ccc • extended-vlan-ccc • flexible-ethernet-services
Logical IF encapsulation	<p>The Logical IF encapsulation field is constrained by your selection in the Physical IF encapsulation field.</p> <p>For the physical encapsulation mode of vlan-ccc or flexible-ethernet-services, your only option is to select vlan-ccc for the logical encapsulation method.</p> <p>For the physical encapsulation mode of extended-vlan-ccc, your only option is to select extended-vlan-ccc for the logical encapsulation method.</p>
Customer VLANs	<p>Transport all traffic Transports the traffic from all VLANs across the network. When you select this option, the service provisioner is prompted for the VLAN-ID when creating a service order based on this service definition. You need to specify only the Outer Tag protocol ID.</p> <p>Transport single vlan Transports traffic for a specific VLAN across the network. You need to specify both Outer Tag protocol ID and Inner Tag protocol ID.</p> <p>Transport VLAN range Limits the traffic across the network to a specific range of VLANs.</p> <p>If you select this option, the service provisioner is prompted for the VLAN-ID range when creating a service order based on this service definition. You need to specify both Outer Tag protocol ID and Inner Tag protocol ID.</p> <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p>

Field	Action
VLAN Normalization	<p>Select a value:</p> <ul style="list-style-type: none"> • Normalize to VLAN all—To preserve customer VLAN IDs (and customer QoS priorities) across the network. <p>NOTE: For services that transport a range of VLANs, you must select VLAN Normalization to all. You cannot transport a range of VLANs without normalization.</p> <ul style="list-style-type: none"> • Normalized VLAN none—To preserve no VLAN IDs across the network. • Not normalized—If VLAN IDs are to be provided manually and are required to match. • Normalized to Dot1q—To transport only single-tagged frames across the network core. All port, dot1q, and Q-in-Q traffic is transported across the network • Normalized to QinQ—To transport only double-tagged frames across the network core. All port, dot1q, and Q-in-Q traffic is transported across the network. • Normalization not required—To specify no normalization for port-to-port services <p>NOTE: Starting with Release 1.0R2, when you newly install Connectivity Services Director, if you select the option to not require normalization in a service definition, the auto-pick option for VLAN IDs and the option to edit the auto-pick behavior in service order are disabled in the service definition. When you create a service order by associating with that service definition, you need to manually enter the VLAN IDs for the interfaces and cannot use the auto-pick functionality. This same behavior also applies to default service templates in which if you select the normalization-not-required functionality, the auto-pick option for VLAN IDs is disabled.</p> <p>For more information about VLAN normalization, see “Junos Space Layer 2 Services Overview” on page 55.</p> <p>For information about VLAN manipulation, see “Understanding VLAN Manipulation (Normalization and VLAN Mapping) on Ethernet Services” on page 88.</p>

Field	Action
Auto Pick VLAN ID	<p>Indicate how the VLAN ID is determined. By default, this check box is disabled.</p> <ul style="list-style-type: none"> Clear this check box to allow the service provider to specify the VLAN ID. This option is normally used when no VLAN normalization is applied. Specify the VLAN ID range in VLAN range for manual input. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p> <ul style="list-style-type: none"> Select this check box when VLAN normalization is applied. Specify the VLAN ID pool in VLAN range for auto-pick. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p> <p>NOTE: When the range of VLAN IDs that are automatically assigned by the system (with the auto-pick option enabled during the creation of a service definition) is less than or greater than the range of VLAN IDs that are manually specified (with the manual selection option enabled during the creation of a service definition), the following conditions apply during the creation of a service order with the Editable in Service Order check box selected during service definition creation:</p> <ul style="list-style-type: none"> If you create a service order with the auto-pick option enabled, the VLAN ID is selected from the auto-pick range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range. If you create a service order with the auto-pick option disabled, the VLAN ID is selected from the manually configured range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range.
VLAN range for auto-pick:	<p>Specify the VLAN ID pool.</p> <p>Range: 1 through 4094</p>
VLAN range for manual input	<p>Specify the VLAN ID range.</p> <p>Range: 1 through 4094</p>
Outer Tag Protocol ID	<p>Select the outer tag protocol ID if the Customer traffic type is Transport single VLAN:</p> <ul style="list-style-type: none"> 0x88a8 0x8100 0x9100 <p>NOTE: For an interface, you must configure a physical port with the possible Tag Protocol Identifiers (TPID) either manually or through a template. Otherwise, the service creation fails for all TPIDs except 0x8100. To configure the TPIDs manually, use the following commands:</p> <pre>set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x9100 set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x88a8 set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x8100</pre>

Field	Action
Inner Tag Protocol ID	<p>Select the inner tag protocol ID:</p> <ul style="list-style-type: none"> • 0x88a8 • 0x8100 • 0x9100 <p>NOTE: You cannot specify the Inner Tag protocol ID if the Customer traffic type is Transport single VLAN.</p>
Editable in Service Order	To allow the service provisioner to override the outer and inner tag protocol IDs, select the check boxes for those options.
Default Interface MTU (Bytes)	The default MTU value is 1522 bytes. To allow the service provisioner to override the MTU setting, select the Editable in Service Order check box.
MTU range for manual-config	<p>In the MTU range fields, type the lowest and highest values for MTU for each UNI.</p> <p>NOTE: To allow the service provisioner to override the MTU setting, select Editable in Service Order and, in the MTU range fields, type the highest and lowest MTU values.</p>
PE-CE Interface Rate-Limiting Settings	
Enable Interface Rate Limiting	<p>To enable a service provisioner to limit the available bandwidth, select this check box, and type a default bandwidth limit.</p> <p>NOTE: Bandwidth settings are available in the service definition when Manage CoS Profiles page is configured with CoS profiles.</p>
Default bandwidth (Mbps)	<p>Specify the default bandwidth value in Mbps.</p> <p>Default: 10 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps</p>
Min Bandwidth (Kbps)	<p>Specify the minimum bandwidth value in Kbps.</p> <p>Default: 1000 Kbps</p> <p>Range: 64 Kbps through 100,000 Kbps</p>
Max Bandwidth (Mbps)	<p>Specify the maximum bandwidth value in Mbps. For more information on maximum bandwidth see Table 79 on page 663</p> <p>Default: 100 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps</p>
Increment (Kbps)	<p>Specify a value that defines which values in the range is made available to the service provisioner.</p> <p>Default: 1000 Kbps</p> <p>Range: 64 Kbps through 100,000 Kbps</p>
Bandwidth – Burst Size Settings	

Field	Action
Burst Size Calculator	<p>Select the preferred option for calculating the burst size:</p> <ul style="list-style-type: none"> • MTU Based If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902. The default value for MTU Factor is 10. • Burst Period Based If you select the option Burst Period Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds. The default value for Burst Period is 1. <p>NOTE: The Burst Size Calculator list is enabled only when you select the Enable Interface Rate Limiting check box.</p>

2. Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

After you complete reviewing the settings, click **Finish** to complete the service definition creation.

UNI or Site Settings for Services with Flexible VLAN Tagging (Asymmetric Interface Types)

You can specify the Ethernet option **asymmetric tag depth** to create a service that includes any combination of port-based interfaces, 802.1Q interfaces, and Q-in-Q interfaces.

To specify the UNI Settings for q-in-q interfaces:

1. Fill in the fields on the **Site Settings** window.

Field	Action
PE-CE UNI Settings- Ethernet Encapsulation	
VLAN Tagging	Select asymmetric tag depth from the list.
Physical IF encapsulation	In the Physical IF encapsulation box, select the default physical encapsulation scheme to be used by service orders based on this service definition. For point-to-multipoint services with 802.1Q interfaces, the only option is flexible-ethernet-services .
Logical IF encapsulation	The Logical IF encapsulation field is constrained by your selection in the Physical IF encapsulation field. For the physical encapsulation mode of flexible-ethernet-services, your only option is to select vlan-vpls for the logical encapsulation method.

LDP PW Extension Settings

NOTE: The **LDP PW Extension Settings** is available only if you have selected the **Enable PW Extension** check box in the General tab.

Field	Action
Physical IF encapsulation	<p>In the Physical IF encapsulation box, select one of the following options:</p> <ul style="list-style-type: none"> • vlan-ccc • extended-vlan-ccc • flexible-ethernet-services
Logical IF encapsulation	<p>The Logical IF encapsulation field is constrained by your selection in the Physical IF encapsulation field.</p> <p>For the physical encapsulation mode of vlan-ccc or flexible-ethernet-services, your only option is to select vlan-ccc for the logical encapsulation method.</p> <p>For the physical encapsulation mode of extended-vlan-ccc, your only option is to select extended-vlan-ccc for the logical encapsulation method.</p>
Customer VLANs	<p>Transport all traffic Transports the traffic from all VLANs across the network. When you select this option, the service provisioner is prompted for the VLAN-ID when creating a service order based on this service definition. You need to specify only the Outer Tag protocol ID and Inner Tag protocol ID.</p> <p>Transport single vlan Transports traffic for a specific VLAN across the network. You need to specify both Outer Tag protocol ID and Inner Tag protocol ID.</p> <p>Transport VLAN range Limits the traffic across the network to a specific range of VLANs. You need to specify both Outer Tag protocol ID and Inner Tag protocol ID.</p> <p>If you select this option, the service provisioner is prompted for the VLAN-ID range when creating a service order based on this service definition.</p> <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p>

Field	Action
VLAN Normalization	<p>Select a value:</p> <ul style="list-style-type: none"> • Normalize to VLAN all—To preserve customer VLAN IDs (and customer QoS priorities) across the network. <p>NOTE: For services that transport a range of VLANs, you must select VLAN Normalization to all. You cannot transport a range of VLANs without normalization.</p> <ul style="list-style-type: none"> • Normalized VLAN none—To preserve no VLAN IDs across the network. • Not normalized—If VLAN IDs are to be provided manually and are required to match. • Normalized to Dot1q—To transport only single-tagged frames across the network core. All port, dot1q, and Q-in-Q traffic is transported across the network • Normalized to QinQ—To transport only double-tagged frames across the network core. All port, dot1q, and Q-in-Q traffic is transported across the network. • Normalization not required—To specify no normalization for port-to-port services <p>NOTE: Starting with Release 1.0R2, when you newly install Connectivity Services Director, if you select the option to not require normalization in a service definition, the auto-pick option for VLAN IDs and the option to edit the auto-pick behavior in service order are disabled in the service definition. When you create a service order by associating with that service definition, you need to manually enter the VLAN IDs for the interfaces and cannot use the auto-pick functionality. This same behavior also applies to default service templates in which if you select the normalization-not-required functionality, the auto-pick option for VLAN IDs is disabled.</p> <p>For more information about VLAN normalization, see “Junos Space Layer 2 Services Overview” on page 55.</p> <p>For information about VLAN manipulation, see “Understanding VLAN Manipulation (Normalization and VLAN Mapping) on Ethernet Services” on page 88.</p>

Field	Action
Auto Pick VLAN ID	<p>Indicate how the VLAN ID is determined. By default, this check box is disabled.</p> <ul style="list-style-type: none"> Clear this check box to allow the service provider to specify the VLAN ID. This option is normally used when no VLAN normalization is applied. Specify the VLAN ID range in VLAN range for manual input. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p> <ul style="list-style-type: none"> Select this check box when VLAN normalization is applied. Specify the VLAN ID pool in VLAN range for auto-pick. <p>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</p> <p>NOTE: When the range of VLAN IDs that are automatically assigned by the system (with the auto-pick option enabled during the creation of a service definition) is less than or greater than the range of VLAN IDs that are manually specified (with the manual selection option enabled during the creation of a service definition), the following conditions apply during the creation of a service order with the Editable in Service Order check box selected during service definition creation:</p> <ul style="list-style-type: none"> If you create a service order with the auto-pick option enabled, the VLAN ID is selected from the auto-pick range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range. If you create a service order with the auto-pick option disabled, the VLAN ID is selected from the manually configured range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range.
VLAN range for auto-pick:	<p>Specify the VLAN ID pool.</p> <p>Range: 1 through 4094</p>
VLAN range for manual input	<p>Specify the VLAN ID range.</p> <p>Range: 1 through 4094</p>
Outer Tag Protocol ID	<p>Select the outer tag protocol ID if the Customer traffic type is Transport single VLAN:</p> <ul style="list-style-type: none"> 0x88a8 0x8100 0x9100 <p>NOTE: For an interface, you must configure a physical port with the possible Tag Protocol Identifiers (TPID) either manually or through a template. Otherwise, the service creation fails for all TPIDs except 0x8100. To configure the TPIDs manually, use the following commands:</p> <pre> set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x9100 set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x88a8 set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x8100 </pre>

Field	Action
Inner Tag Protocol ID	<p>Select the inner tag protocol ID:</p> <ul style="list-style-type: none"> • 0x88a8 • 0x8100 • 0x9100 <p>NOTE: You cannot specify the Inner Tag protocol ID if the Customer traffic type is Transport all traffic.</p>
Editable in Service Order	To allow the service provisioner to override the outer and inner tag protocol IDs, select the check boxes for those options.
MTU range for manual-config	<p>In the MTU range fields, type the lowest and highest values for MTU that the service provisioner can type, for each UNI</p> <p>NOTE: To allow the service provisioner to override the MTU setting, select Editable in Service Order and, in the MTU range fields, type the highest and lowest MTU values that the service provisioner can type.</p>
Default Interface MTU (Bytes)	The default MTU value is 1522 bytes. To allow the service provisioner to override the MTU setting, select the Editable in Service Order check box.
PE-CE Interface Rate-Limiting Settings	
Enable Interface Rate Limiting	<p>To enable a service provisioner to limit the available bandwidth, select this check box, and type a default bandwidth limit.</p> <p>NOTE: Bandwidth settings are available in the service definition when Manage CoS Profiles page is configured with CoS profiles.</p>
Default bandwidth (Mbps)	<p>Specify the default bandwidth value in Mbps.</p> <p>Default: 10 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps</p>
Min Bandwidth (Kbps)	<p>Specify the minimum bandwidth value in Kbps.</p> <p>Default: 1000 Kbps</p> <p>Range: 64 Kbps through 100,000 Kbps</p>
Max Bandwidth (Mbps)	<p>Specify the maximum bandwidth value in Mbps. For more information on maximum bandwidth see Table 79 on page 663</p> <p>Default: 100 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps</p>
Increment (Kbps)	<p>Specify a value that defines which values in the range is made available to the service provisioner.</p> <p>Default: 1000 Kbps</p> <p>Range: 64 Kbps through 100,000 Kbps</p>

Field	Action
Bandwidth – Burst Size Settings	
Burst Size Calculator	<p>Select the preferred option for calculating the burst size:</p> <ul style="list-style-type: none"> MTU Based If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902. The default value for MTU Factor is 10. Burst Period Based If you select the option Burst Period Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds. The default value for Burst Period is 1. <p>NOTE: The Burst Size Calculator list is enabled only when you select the Enable Interface Rate Limiting check box.</p>

- Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

After you complete reviewing the settings, click **Finish** to complete the service definition creation.

Reviewing the Configured Settings

The Review page of the service definition or service order creation and modification wizards enable you to view and evaluate the service parameters and components you configured in preceding steps or pages of the wizard. This page provides a comprehensive, single-page view of all the service elements configured in the different pages of the wizard. You can either click the buttons corresponding to the various settings at the top of the wizard page to directly traverse to the page you want to modify or click the navigation buttons at the bottom of the wizard page to go to the different pages of the wizard.



NOTE: On the Review page, in the Service Templates section, the names of the service templates with which the service definition is associated are displayed. The Default Service Template column indicates whether the attached template is the default template.

To examine and modify the configured service definition settings:

1. Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify.
2. Click **Edit** next to the section that contains the parameter you want to modify. You are navigated to the corresponding page of the wizard in which the parameter settings are defined.
3. Click **Finish** to save the service definition or service order.
4. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

The service order inventory window appears.

**Related
Documentation**

- [Creating a Multipoint-to-Multipoint VPLS Service Definition on page 653](#)
- [Creating a Service Definition for VPLS Access into Layer 3 Networks on page 705](#)

Creating a Service Definition for VPLS Access into Layer 3 Networks

You can configure an Integrated Routing and Bridging (IRB) interface to provide access from VPLS Layer 2 networks and services into Layer 3 networks. If the IRB interface configured as a Layer 3 interface is being used in a routing instance, that routing instance will specifically declare it as routing-interface rather than a regular VPLS interface (which acts like the interface on a specific VPLS site). This feature requires a normalized VLAN (vlan-id=xxx which is the same as the unit name on which the inet4 address is specified)

Junos Space uses the two peer subinterfaces of the IRB to create the link between an existing VLAN and the Layer 3 network. An extra VPLS node is required to support the IRB interface which allows the rest of the VPLS nodes to be able to access all Layer 3 networks reachable through that interface. Providing the VPLS access into Layer 3 networks enhances basic VPLS services. Because this feature requires a normalized VLAN, it is available only on the Juniper Networks MX 3D Router series.

Prerequisites for VPLS Access into Layer 3 Networks

- The PE device with the IRB must be a Juniper Networks MX 3D Series Router to accommodate the normalized VLAN requirement.
- In addition to the PE device used for the IRB, 2 or more PEs must exist on the VPLS network for a minimum of 3 PE devices.
- A VLAN must already exist to configure this feature.

To begin the configuration of the IRB interface, in the **Network Services > Connectivity** task pane, select **Service Design > Manage Service Definitions > Create VPLS Service Definition**.

Field	Action
Service Definition Name	Provide a name for the VPLS service definition you want to create.
Service Type	<p>Select the type of service from the menu list. To create the VPLS into Layer 3 service, use either of the following service type:</p> <ul style="list-style-type: none"> • Multipoint-to-Multipoint Ethernet (VPLS) • Point-to-Multipoint Ethernet (VPLS)
Description	Provide any comments or a description that will help explain the purpose of this definition.
Enable L3 Access	Check the box to create the link into Layer 3.
Route target	The Route target field is prepopulated with the Auto pick option.
Route distinguisher	The Route distinguisher field is prepopulated with the Auto pick option.
MAC Settings	
MAC learning	MAC learning is on by default for VPLS service definitions.
Interface MAC limit	The default value for Interface MAC limit is 1024. If you are using a different value, enter that value.
MAC table size	The table size is predetermined to correspond to the default MAC limit. If you are using a value other than the default, specify that value.

1. Click **Next** to display the next screen, **Site Settings**, and continue creating the service definition.

Specifying Site or UNI Settings

Site Settings Field	Action
PE-CE Interface Settings – Ethernet Encapsulation	
VLAN Tagging	Indicate the Ethernet option to use for this VPLS service definition. Choices are qinq or dot1q .
Customer VLANs	The only option for VPLS service definitions is Transport single VLAN .
VLAN normalization	All VPLS service definitions require VLAN normalization.
Auto Pick VLAN ID	The only option for VPLS service definitions is Select manually .
Physical Interface Encapsulation	The only option for VPLS service definitions is flexible-ethernet-services .
Logical Interface Encapsulation	The only option for VPLS service definitions is vlan-vpls .
Default MTU (Bytes)	This field is populated with the default MTU value of 1522. If you are not using the default value, enter the MTU value in bytes.
MTU range (Bytes)	If you are specifying a custom MTU value, indicate the range of values in bytes.

1. Click **Finish** to see the service definition inventory list.
2. Click on the unpublished service definition you just created.
3. Right-click on the selected service definition to choose publishing options.
4. Select the service definition and click **Publish** to save and publish the definition.
5. The next step is to create the service order. In the **Network Services > Connectivity** task pane, select **Service Provisioning**.

Related Documentation

- [Creating a Multipoint-to-Multipoint VPLS Service Definition on page 653](#)
- [Creating a Point-to-Multipoint VPLS Service Definition on page 678](#)

CHAPTER 27

Service Design: Managing Layer 3 VPN Service Definitions

- [Creating a Full-Mesh Layer 3 VPN Service Definition on page 709](#)
- [Creating a Hub-and-Spoke \(One Interface\) Layer 3 VPN Service Definition on page 719](#)
- [Creating a Service Definition for Point-to-Point Pseudowire Access into a Layer 3 VPN on page 730](#)
- [Creating a Multicast VPN Service Definition on page 732](#)

Creating a Full-Mesh Layer 3 VPN Service Definition

You can create a customized service definition—for example, to set a different VLAN ID range on the service than those offered in the standard service definitions. Network operators or service provisioners can use the service definition as a base for creating and then activating full-mesh ethernet services on the network.

You can use the tab panel at the top, or the **Back** and **Next** buttons to switch between the wizard pages.

You can create a Full-Mesh Layer 3 VPN Service Definition, by following the steps given in the procedure.

Creating a full mesh Layer 3 VPN service definition consists of the following steps:

1. [Specifying General Settings Information on page 709](#)
2. [Specifying Site or UNI Settings on page 712](#)
3. [Reviewing the Configured Settings on page 718](#)

Specifying General Settings Information

In the **Service View** pane, select **Network Services > Connectivity > L3 VPN Services**. In the **Tasks** pane, select **Service Design > Manage Service Definitions**.

Create L3VPN Service Definition

General | Site Settings | Review

You are here: General

General Settings

Service Definition Name*: TempSD

Description:

Service Type*: L3 VPN (Full Mesh)

Instance Type*: vrf

☒ Enable Distinct Instance Name

☒ Decouple Service From Port Status

Connectivity Settings

<input type="checkbox"/> Auto Pick Route Target	<input type="checkbox"/> Editable in Service Order
<input checked="" type="checkbox"/> Policy Based Route Target	<input type="checkbox"/> Editable in Service Order
<input type="checkbox"/> Auto Pick Route Distinguisher	<input type="checkbox"/> Editable in Service Order
<input checked="" type="checkbox"/> VRF Table Label	<input type="checkbox"/> Editable in Service Order
<input type="checkbox"/> Enable Auto Export Routes	<input type="checkbox"/> Editable in Service Order
<input type="checkbox"/> Export Direct Routes	
<input type="checkbox"/> Import Internal Routes	
<input type="checkbox"/> Import External Routes	
<input type="checkbox"/> Enable MVPN	

Service Templates

Back Next Done Cancel

1. In the **Manage Service Definitions** pane, click **New**.

The **Create L3 VPN Service Definition** wizard appears.

2. To specify the general settings or service attributes for a full mesh service definition, fill in the fields on the General page as indicated in [Table 81 on page 710](#).

Table 81: Layer 3 VPN Service Definition - General Settings

Field	Action
Service Definition Name	Type a unique name that identifies the full mesh Layer 3 VPN definition. Range: 3 through 50 characters.
Service Type	Select L3 VPN (Full Mesh) .
Instance Type	Select one of the following instance types: <ul style="list-style-type: none"> • vrf—To advertise routes from the CE router to the PE router and vice versa. • default—To add an IP Transit Service to the PE-CE router configuration. • virtual router—To divide a router into multiple independent virtual routers where each router has its own routing table. The Connectivity Settings sections appear only if the instance type is vrf.
Description (Optional)	Type a comment that identifies or describes the definition. Range: 1 through 200 characters.
Enable Distinct Instance Name	Select this check box to specify different routing instance name for each device selected in a Layer 3 VPN Service.

Table 81: Layer 3 VPN Service Definition - General Settings (continued)

Field	Action
Decouple Service Status From Port Status	<p>Select this check box to isolate the events related to an interface in the OpenNMS.</p> <p>NOTE: When you select this check box, only the MPLS traps are monitored, and not the interface-related traps (such as jnxVpnIfUp or jnxVpnIfDown).</p> <p>By default, all the events are saved in the OpenNMS database.</p>
Connectivity Settings	
Policy Based Route Target	<p>Select this check box to create a policy-based vrf instance.</p> <p>Deselect this check box to create a community-based vrf instance.</p> <p>Route Leak is supported when Policy Based Route Target check box is selected.</p> <p>For more information on creating policies for a Layer 3 VPN service, see “Creating Policies for a Layer 3 VPN Service” on page 998.</p>
Auto-pick Route Target	<p>Select a route target option:</p> <ul style="list-style-type: none"> • Select the Auto-pick Route Target check box and the Policy Based Route Target check box to auto generate route target policies. • Select the Auto-pick Route Target check box and deselect the Policy Based Route Target check box to auto generate a community. No policy will be used. • When you clear this check box and select the Policy Based Route Target check box: <ul style="list-style-type: none"> • You can create a route target policy and associate it with import and export policy. • The route target policy will be auto generated. <p>Note that, you cannot manually select or modify policy during the modification of service.</p> <p>To override this setting in the service order, you can select the Editable in Service Order check box.</p>
Enable Auto Export Routes	<p>Select this check box in the Create Layer 3 VPN Service Definition wizard to enable internal and external route leak as part of route target policy creation.</p>
Import Internal Routes	<p>Select this check box in the Create Layer 3 VPN Definition wizard to enable internal route leak feature as part of route target policy creation.</p> <p>Import Internal Route field is available only if Policy Based Route Target check box is selected.</p>
Import External Route	<p>Select this check box in the Create Layer 3 VPN Definition wizard to enable external route leak feature as part of route target policy creation.</p> <p>Import External Route field is available only if Policy Based Route Target check box is selected.</p>
Auto-pick Route Distinguisher	<p>Select a route distinguisher option:</p> <ul style="list-style-type: none"> • Deselect the check box to enable the service provider to specify the route distinguisher. • Select the check box to enable the route distinguisher to be selected automatically. <p>To override this setting in the service order, you can select the Editable in Service Order check box.</p>

Table 81: Layer 3 VPN Service Definition - General Settings (continued)

Field	Action
VRF Table label	<p>Select this check box to configure a separate label for each VRF to provide double lookup and egress filtering.</p> <p>To override this setting in the service order, you can select the Editable in Service Order check box.</p>
Export Direct Routes	Select this check box to export direct routes.
Enable MVPN	Select the check box to enable multicast virtual private network (MPVN).
Service Template	<p>(Optional) To include a service template for the service, click the Add icon or plus sign (+) to select a service template from the Service Template list. The list of available service templates is displayed. Select the check box beside the template you want and click OK. You are returned to the General Settings page.</p> <p>The selected service template appears in the Default Service Template field.</p> <p>You can select one or more service templates as the default service template. By default, the default service templates are attached to the endpoints.</p> <p>NOTE: Starting with Connectivity Services Director Release 2.1, you can add or delete a service template while creating a service order.</p> <p>The remaining service templates on the Service Template list are termed as optional service templates. You can attach the optional service templates to the endpoints on a need basis.</p> <p>In the View Service Definition Details window, the value for the default service template in the Default Service Template column is <i>True</i>.</p> <p>For instructions on creating a service template, see “Creating a Service Template” on page 1815.</p> <p>NOTE: To provision a Layer 3 VPN service for QinQ UNI type, you can create a service template with service variables as <i>interface name</i> and <i>unit name</i>.</p>

3. Click **Next** to save the General page information. Continue with [“Specifying Site or UNI Settings” on page 712](#).

Specifying Site or UNI Settings

To provide the site or UNI service attributes for this service definition:

1. Fill in the fields on the Site Settings page as indicated in [Table 82 on page 713](#).

Table 82: Layer 3 VPN Service Definition - PE-CE UNI Settings

Field	Action
PE-CE UNI Settings	
MTU Settings	
Interface MTU (Bytes)	<p>You can specify an MTU value in this field. The default value for MTU is 1522 bytes.</p> <p>To see the permitted range for the MTU value, select the Editable in Service Order check box. The MTU range is 1522 through 9192.</p>
MTU Range (Bytes)	<p>If you select the check box Editable in Service Order, you can specify a value range for MTU (in bytes). The permitted range for MTU is 1522 through 9192.</p> <p>NOTE: Ultimately, the system establishes the MTU by multiplying the value you specify in the Default MTU (Bytes) field by the value you specify for MTU Factor.</p>
Bandwidth Settings	

Table 82: Layer 3 VPN Service Definition - PE-CE UNI Settings (continued)

Field	Action
Enable QoS	<p>When you enable QoS in the service definition, you can specify a QoS profile in the service order to classify traffic into defined service groups to provide the special treatment of traffic across the network service. For example, voice traffic can be sent across certain links, and data traffic can use other links.</p> <p>If you enable the inclusion of QoS profile settings for the service in the service template or service definition, the list of CoS profiles that you defined using the Manage CoS Profiles page (by selecting CoS under Profile and Configuration Management in the Tasks pane) are displayed. Select the CoS profile you want to associate with the service from the drop-down list.</p>
Enable rate limiting (check box)	Select the check box to enable rate-limiting of traffic. Clear the check box to disable rate-limiting.
Bandwidth (Mbps)	<p>Specify the default bandwidth value, in Mbps.</p> <p>Default: 10 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps</p>
Min Bandwidth (Kbps)	<p>To override the default bandwidth value, select the Editable in Service Order check box.</p> <p>Specify the minimum bandwidth value in Kbps:</p> <p>Default: 1000 Kbps</p> <p>Range: 64 Kbps through 100,000 Kbps</p>
Max Bandwidth (Mbps)	<p>Specify the maximum bandwidth value, in Mbps.</p> <p>Default: 100 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps</p>

The following table lists the **Max Bandwidth (Mbps)** for the M Series, MX Series, and ACX Series Routers:

Table 83: Maximum Bandwidth for M Series, MX Series, and ACX Series Routers

M Series IQ2E PIC		M Series IQ2 PIC		MX Series 3D PIC		MX Series Non-3D PIC		ACX 2000	
GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)
32,000 Mbps or 32 Gbps	32,000 Mbps or 32 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps	100,000 Mbps or 100 Gbps	100,000 Mbps or 100 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps

Increment (Kbps)	Specify a value in the range that is made available to the service provisioner.
-------------------------	---

Table 82: Layer 3 VPN Service Definition - PE-CE UNI Settings (continued)

Field	Action
Burst Size	<p>You can choose one of the following as the Burst Size:</p> <ul style="list-style-type: none"> • MTU Based (default) • Line Rate Based <p>Burst Size is the number of bytes that can pass unrestricted through a policed interface when a burst of traffic pushes the average transmit rate or receive rate above the configured bandwidth limit.</p> <p>NOTE: This field is enabled only when you select the Enable Rate Limiting check box.</p>
MTU Factor	<p>You can specify a value for MTU Factor in the range 1 through 1087902. The default value for MTU Factor is 10.</p> <p>The value you configure for MTU Factor should not exceed one tenth of the value you configured for burst size.</p> <p>NOTE: This field is enabled only when you select MTU Based as the Burst Size.</p>
Burst Period	<p>Specify a value for Burst Period in the range 10 through 1000. The default value for Burst Period is 10.</p> <p>NOTE: This field is enabled only when you select Line Rate Based as the Burst Size.</p>
PE-CE Interface Encapsulation Settings	

Table 82: Layer 3 VPN Service Definition - PE-CE UNI Settings (continued)

Field	Action
Auto-pick VLAN ID	<p>Specify how the VLAN ID is determined:</p> <ul style="list-style-type: none"> To allow the service provider to specify the VLAN ID, clear this check box. Specify the range in VLAN ID Range for Manual Config. To allow the VLAN ID to be selected automatically from the VLAN ID pool, select Auto-pick VLAN ID check box. This option is used typically when VLAN normalization is applied. Specify the range in VLAN ID Range for Auto-pick <p>NOTE: Select the Editable in Service Order check box, if you want to override VLAN ID selection setting in the service order.</p> <p>NOTE: When the range of VLAN IDs that are automatically assigned by the system (with the auto-pick option enabled during the creation of a service definition) is less than or greater than the range of VLAN IDs that are manually specified (with the manual selection option enabled during the creation of a service definition), the following conditions apply during the creation of a service order with the Editable in Service Order check box selected during service definition creation:</p> <ul style="list-style-type: none"> If you create a service order with the Auto-pick VLAN ID option enabled, the VLAN ID is selected from the auto-pick range, and the value is displayed in the VLAN ID Range for Auto-Pick field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range. If you create a service order with the Auto-pick VLAN ID option disabled, the VLAN ID is selected from the manually configured range, and the value is displayed in the VLAN ID range for Manual Config field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range.
VLAN range for auto-pick	<p>Specify the range.</p> <p>Range: 1 through 4094.</p>
VLAN ID Range for Manual Config	<p>Specify the range.</p> <p>Range: 1 through 4094.</p> <p>NOTE: This parameter reserves a range of VLANs for provisioning Layer 3 VPNs. These VLANs are not used to transport data from one end of a connection to the other.</p>
PE-CE Routing	

Table 82: Layer 3 VPN Service Definition - PE-CE UNI Settings (continued)

Field	Action
Routing Protocols	<p>Select one of the following options to allow each PE router to distribute VPN-related routes to and from connected CE routers:</p> <ul style="list-style-type: none"> • BGP/Static Route • OSPF/Static Route • BGP/OSPF/Static Route
PE-CE Interface Address Settings	
Pool-based assignment	<p>Indicate the method to be used for assigning IP addresses to PE and CE interfaces. The address-assignment pool feature supports subscriber management and DHCP management functionality by enabling you to create centralized IPv4 address pools independently of the client applications that use the pools.</p> <p>Select the check box to enable allocation of PE-CE IP addresses from IP address pools. By default, this check box is deselected. Clear the check box to disable the address-assignment pools functionality.</p>
IP Pool Type	<p>Select an IP pool type option:</p> <ul style="list-style-type: none"> • Global—A Global IP address pool pertains to the service provider. There can be more than one global IPv4 address pool. However, each global pool must have its own unique name and its set of IPv4 addresses must not overlap with those of any other global pool. You can allocate addresses from global pools across multiple Layer 3 VPNs across multiple customers. The IP addresses allocated to services are unique across customers. • Customer—A Customer IP address pool pertains to an existing customer. These pools are associated with the corresponding customer. You can associate more than one customer IPv4 pool with each customer. However, each customer pool must have its own set of IPv4 addresses which must not overlap with those of any other pool belonging to the same customer. You can allocate addresses from customer pools across multiple Layer 3 VPNs for a particular customer. The IP addresses allocated to services are unique within specified customer services. <p>For more information on creation an IP pool, see <i>Creating an IP Address Pool</i>.</p>
Auto-pick PE Interface IP Address	<p>Select an option:</p> <ul style="list-style-type: none"> • Clear the check box to enable the service provider to specify the IP address of a provider edge (PE) interface. • Select the check box to cause the IP address of a provider edge (PE) interface to be selected automatically. <p>To override this setting in the service order, you can select the Editable in Service Order check box.</p>

Table 82: Layer 3 VPN Service Definition - PE-CE UNI Settings (continued)

Field	Action
IP Address Block Size	<p>Specify the size of the IPv4 IP addressee block allocated for each provider edge (PE) or customer edge (CE) link.</p> <p>Range: 1 through 32</p> <p>To override this setting in the service order, you can select the Editable in Service Order check box.</p>

2. Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

After you complete reviewing the settings, click **Finish** to complete the service definition creation.

Reviewing the Configured Settings

The Review page of the service definition or service order creation and modification wizards enable you to view and evaluate the service parameters and components you configured in preceding steps or pages of the wizard. This page provides a comprehensive, single-page view of all the service elements configured in the different pages of the wizard. You can either click the buttons corresponding to the various settings at the top of the wizard page to directly traverse to the page you want to modify or click the navigation buttons at the bottom of the wizard page to go to the different pages of the wizard.



NOTE: On the Review page, in the Service Templates section, the names of the service templates with which the service definition is associated are displayed. The Default Service Template column indicates whether the attached template is the default template.

To examine and modify the configured service definition settings:

1. Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertinent to the settings you want to modify.

Create L3VPN Service Definition

General Site Settings Review

You are here: Review

General Settings Edit

Service Definition Name:	TempSD
Service Type:	L3 VPN (Full Mesh)
Instance Type:	vrf
Enable Distinct Instance Type:	true
Decouple Service Status from Port Status:	true

Connectivity Settings

Route Target:	Select manually
Route Distinguisher:	Select manually
VRF Table Label:	true
Enable Auto Export Routes:	false
Policy Based Route Target:	true

Site Settings Edit

- PE-CE Interface Encapsulation Settings
- PE-CE Interface Address Settings
- PE-CE Routing
- MTU Settings
- Bandwidth

Back Next Done Cancel

2. Click **Edit** next to the section that contains the parameter you want to modify. You are navigated to the corresponding page of the wizard in which the parameter settings are defined.
3. Click **Done** to save the service definition or service order.
4. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

The service order inventory window appears.

Related Documentation

- [Creating a Hub-and-Spoke \(One Interface\) Layer 3 VPN Service Definition on page 719](#)
- [Creating a Service Definition for Point-to-Point Pseudowire Access into a Layer 3 VPN on page 730](#)
- [Creating a Multicast VPN Service Definition on page 732](#)

Creating a Hub-and-Spoke (One Interface) Layer 3 VPN Service Definition

You can create a one-interface hub-and-spoke BGP/Static or OSPF/Static Layer 3 VPN service definition, for the Connectivity Services Director application, using predefined service definitions.

In the **Service View** pane, click **Network Services > Connectivity > L3 VPN Services**. In the **Tasks** pane, click **Service Design > Manage Service Definitions**.

To create a new service definition, click **New** In the **Manage Service Definitions** pane. You can also choose a predefined service definition from the **Manage Service Definitions** pane.

In a one-interface hub-and-spoke topology, there is only one interface using a combination of static routes, BGP, and OSPF routes between CE hub and PE hub routers. You can use a one-interface hub-and-spoke Layer 3 VPN service definition to configure a service to advertise a default route from a hub to the spokes.

For more information about predefined one-interface hub-and-spoke BGP/Static or OSPF/Static Layer 3 VPN service definitions, see [“Predefined Hub-and Spoke Layer 3 VPN Service Definitions” on page 590](#). You can, however create a customized service definition—for example, to set different bandwidth limits on the service than those offered in the standard service definitions.

You must have a Service Designer user role to create Layer 3 VPN hub-and-spoke service definitions. When you create and publish a new service definition, network operators or service provisioners with a Service Activator role can use the completed service definition as a base for creating and then activating hub-and-spoke Ethernet services on the network.

Creating a hub-and-spoke (one interface) Layer 3 VPN service definition consists of the following steps:

1. [Specifying General Information on page 721](#)
2. [Specifying UNI or Site Settings on page 723](#)
3. [Reviewing the Configured Settings on page 729](#)

Specifying General Information

To specify general information for a hub-and-spoke service definition:

1. Fill in the fields on the General page as indicated in [Table 84](#) on page 721.

Table 84: Layer 3 VPN Service Definition - General Settings

Field	Action
Service Definition Name	Type a unique name that identifies the hub-and-spoke Layer 3 VPN definition. Range: 3 through 50 characters.
Service Type	Select L3 VPN (Hub-Spoke 1 Interface) .
Instance Type	Select one of the following instance types: <ul style="list-style-type: none"> • vrf—To advertise routes from the CE router to the PE router and vice versa. • default—To add an IP Transit Service to the PE-CE router configuration. • virtual router—To divide a router into multiple independent virtual routers where each router has its own routing table. The Connectivity Settings sections appear only if the instance type is vrf.
Description (Optional)	Type a comment that identifies or describes the definition. Range: 1 through 200 characters.
Enable Distinct Instance Name	Select this check box to specify different routing instance name for each device selected in a Layer 3 VPN service.

Table 84: Layer 3 VPN Service Definition - General Settings (continued)

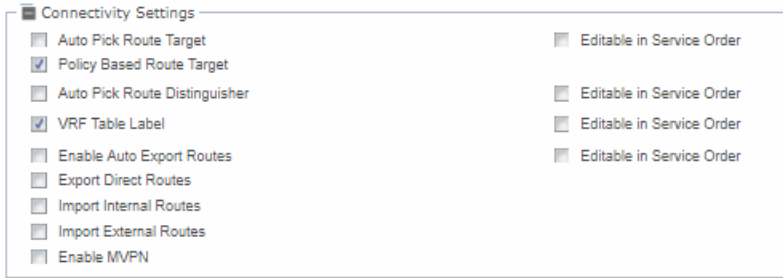
Field	Action
Decouple Service Status From Port Status	<p>Select this check box to isolate the events related to an interface in the OpenNMS.</p> <p>NOTE: When you select this check box, only the MPLS traps are monitored, and not the interface-related traps (such as jnxVpnIfUp or jnxVpnIfDown).</p> <p>By default, all the events are saved in the OpenNMS database.</p>
Connectivity Settings 	
Policy Based Route Target	<p>Select this check box to create a policy-based vrf instance.</p> <p>Deselect this check box to create a community-based vrf instance.</p> <p>Route Leak is supported when Policy Based Route Target check box is selected.</p> <p>For more information on creating policies for a Layer 3 VPN service, see “Creating Policies for a Layer 3 VPN Service” on page 998.</p>
Auto-pick Route Target	<p>Select a route target option:</p> <ul style="list-style-type: none"> • Select the Auto-pick Route Target check box and the Policy Based Route Target check box to auto generate route target policies. • Select the Auto-pick Route Target check box and deselect the Policy Based Route Target check box to auto generate a community. No policy will be used. • When you clear this check box and select the Policy Based Route Target check box: <ul style="list-style-type: none"> • You can create a route target policy and associate it with import and export policy. • The route target policy will be auto generated. <p>Note that, you cannot manually select or modify policy during the modification of service.</p> <p>To override this setting in the service order, you can select the Editable in Service Order check box.</p>
Enable Auto Export Routes	<p>Select this check box in the Create Layer 3 VPN Service Definition wizard to enable internal and external route leak as part of route target policy creation.</p>
Import Internal Routes	<p>Select this check box in the Create Layer 3 VPN Definition wizard to enable internal route leak feature as part of route target policy creation.</p> <p>Import Internal Route field is available only if Policy Based Route Target check box is selected.</p>
Import External Route	<p>Select this check box in the Create Layer 3 VPN Definition wizard to enable external route leak feature as part of route target policy creation.</p> <p>Import External Route field is available only if Policy Based Route Target check box is selected.</p>

Table 84: Layer 3 VPN Service Definition - General Settings (continued)

Field	Action
Auto-pick Route Distinguisher	<p>Select a route distinguisher option:</p> <ul style="list-style-type: none"> • Deselect the check box to enable the service provider to specify the route distinguisher. • Select the check box to enable the route distinguisher to be selected automatically. <p>To override this setting in the service order, you can select the Editable in Service Order check box.</p>
VRF Table Label	<p>Select this check box to configure a separate label for each VRF to provide double lookup and egress filtering.</p> <p>To override this setting in the service order, you can select the Editable in Service Order check box.</p>
Export Direct Routes	Select this check box to export direct routes.
Enable MVPN	Select this check box to enable MVPN settings in Layer 3 VPN service orders to be based on this service definition.
Service Template	<p>(Optional) To include a service template for the service, click the Add icon or plus sign (+) to select a service template from the Service Template list. The list of available service templates is displayed. Select the check box beside the template you want and click OK. You are returned to the General Settings page.</p> <p>The selected service template appears in the Default Service Template field.</p> <p>You can select one or more service templates as the default service template. By default, the default service templates are attached to the endpoints.</p> <p>NOTE: Starting with Connectivity Services Director Release 2.1, you can add or delete a service template while creating a service order.</p> <p>The remaining service templates on the Service Template list are termed as optional service templates. You can attach the optional service templates to the endpoints on a need basis.</p> <p>In the View Service Definition Details window, the value for the default service template in the Default Service Template column is <i>True</i>.</p> <p>For instructions on creating a service template, see “Creating a Service Template” on page 1815.</p> <p>NOTE: To provision a Layer 3 VPN service for QinQ UNI type, you can create a service template with service variables as <i>interface name</i> and <i>unit name</i>.</p>

2. Click **Next** to save the General information.

The **Site Settings-Create L3VPN Service Definition** page appears.

Specifying UNI or Site Settings

To specify UNI interface settings for the service definition:

Create L3VPN Service Definition

General | **Site Settings** | Review

You are here: Site Settings

PE-CE MTU Settings

Interface MTU (Bytes): 1522 ☐ Editable in service order

MTU Range (Bytes): 1522 - 9192

PE-CE QoS

☒ Enable QoS

PE-CE Bandwidth

☒ Enable Rate Limiting

Bandwidth (Mbps): 10 ☐ Editable in service order

Min. Bandwidth (Kbps): 1000

Max Bandwidth (Mbps): 100

Increment (Kbps): 1000

Burst Size: MTU Based

MTU Factor: 10 ☐ Editable in service order

Burst Period (ms): 10 ☒ Editable in service order

PE-CE Interface Encapsulation Settings

PE-CE Interface Address Settings

PE-CE Routing

Back Next Done Cancel

1. Fill in the fields on the Site Settings page as indicated in the table as indicated in [Table 85 on page 724](#).

Table 85: Layer 3 VPN Service Definition - PE-CE UNI Settings

Field	Action
PE-CE UNI Settings	
MTU Settings	
Interface MTU (Bytes)	<p>You can specify an MTU value in this field. The default value for MTU is 1522 bytes.</p> <p>To see the permitted range for the MTU value, select the Editable in Service Order check box. The MTU range is 1522 through 9192.</p>
MTU Range (Bytes)	<p>If you select the check box Editable in Service Order, you can specify a value range for MTU (in bytes). The permitted range for MTU is 1522 through 9192.</p> <p>NOTE: Ultimately, the system establishes the MTU by multiplying the value you specify in the Default MTU (Bytes) field by the value you specify for MTU Factor.</p>
Bandwidth Settings	

Table 85: Layer 3 VPN Service Definition - PE-CE UNI Settings (continued)

Field	Action
Enable QoS	<p>When you enable QoS in the service definition, you must specify a QoS profile in the service order to classify traffic into defined service groups to provide the special treatment of traffic across the network service. For example, voice traffic can be sent across certain links, and data traffic can use other links.</p> <p>If you enable the inclusion of QoS profile settings for the service in the service template or service definition, the list of CoS profiles that you defined using the Manage CoS Profiles page (by selecting CoS under Profile and Configuration Management in the Tasks pane) are displayed. Select the CoS profile you want to associate with the service from the drop-down list.</p>
Enable rate limiting (check box)	Select the check box to enable rate-limiting of traffic. Clear the check box to disable rate-limiting.
Bandwidth (Mbps)	<p>Specify the default bandwidth value, in Mbps.</p> <p>Default: 10 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps</p>
Min Bandwidth (Kbps)	<p>To override the default bandwidth value, select the Editable in Service Order check box.</p> <p>Specify the minimum bandwidth value in Kbps:</p> <p>Default: 1000 Kbps</p> <p>Range: 64 Kbps through 100,000 Kbps</p>
Max Bandwidth (Mbps)	<p>Specify the maximum bandwidth value, in Mbps.</p> <p>Default: 100 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps</p>

The following table lists the **Max Bandwidth (Mbps)** for the M Series, MX Series, and ACX Series Routers:

Table 86: Maximum Bandwidth for M Series, MX Series, and ACX Series Routers

M Series IQ2E PIC		M Series IQ2 PIC		MX Series 3D PIC		MX Series Non-3D PIC		ACX 2000	
GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)	GE Port (1G)	XE Port (10G)
32,000 Mbps or 32 Gbps	32,000 Mbps or 32 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps	100,000 Mbps or 100 Gbps	100,000 Mbps or 100 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps	50,000 Kbps or 50 Gbps

Table 85: Layer 3 VPN Service Definition - PE-CE UNI Settings (continued)

Field	Action
Burst Size	<p>You can choose one of the following as the Burst Size:</p> <ul style="list-style-type: none"> • MTU Based (default) • Line Rate Based <p>Burst Size is the number of bytes that can pass unrestricted through a policed interface when a burst of traffic pushes the average transmit rate or receive rate above the configured bandwidth limit.</p> <p>NOTE: This field is enabled only when you select the Enable Rate Limiting check box.</p>
MTU Factor	<p>You can specify a value for MTU Factor in the range 1 through 1087902. The default value for MTU Factor is 10.</p> <p>The value you configure for MTU Factor should not exceed one tenth of the value you configured for burst size.</p> <p>NOTE: This field is enabled only when you select MTU Based as the Burst Size.</p>
Burst Period	<p>Specify a value for Burst Period in the range 10 through 1000. The default value for Burst Period is 10.</p> <p>NOTE: This field is enabled only when you select Line Rate Based as the Burst Size.</p>
Increment (Kbps)	Specify a value in the range that is made available to the service provisioner.
PE-CE Interface Encapsulation Settings	

Table 85: Layer 3 VPN Service Definition - PE-CE UNI Settings (continued)

Field	Action
Auto-pick VLAN ID	<p>Specify how the VLAN ID is determined:</p> <ul style="list-style-type: none"> To allow the service provider to specify the VLAN ID, clear the check box. Specify the range in VLAN ID Range for Manual Config. To allow the VLAN ID to be selected automatically from the VLAN ID pool, select Auto-pick VLAN ID check box. This option is used typically when VLAN normalization is applied. Specify the range in VLAN ID Range for Auto-pick <p>NOTE: Select the Editable in Service Order check box, if you want to override VLAN ID selection setting in the service order.</p> <p>NOTE: When the range of VLAN IDs that are automatically assigned by the system (with the auto-pick option enabled during the creation of a service definition) is less than or greater than the range of VLAN IDs that are manually specified (with the manual selection option enabled during the creation of a service definition), the following conditions apply during the creation of a service order with the Editable in Service Order check box selected during service definition creation:</p> <ul style="list-style-type: none"> If you create a service order with the Auto-pick VLAN ID option enabled, the VLAN ID is selected from the auto-pick range, and the value is displayed in the VLAN ID Range for Manual Config field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range. If you create a service order with the auto-pick option disabled, the VLAN ID is selected from the manually configured range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range.
VLAN range for auto-pick	<p>Specify the range.</p> <p>Range: 1 through 4094.</p>
VLAN ID Range for Manual Config	<p>Specify the range.</p> <p>Range: 1 through 4094.</p> <p>NOTE: This parameter reserves a range of VLANs for provisioning Layer 3 VPNs. These VLANs are not used to transport data from one end of a connection to the other.</p>
PE-CE Routing	

Table 85: Layer 3 VPN Service Definition - PE-CE UNI Settings (continued)

Field	Action
Routing Protocols	<p>Select one of the following options to allow each PE router to distribute VPN-related routes to and from connected CE routers:</p> <ul style="list-style-type: none"> • BGP/Static Route • OSPF/Static Route • BGP/OSPF/Static Route
PE-CE Interface Address Settings	
Pool-based assignment	<p>Indicate the method to be used for assigning IP addresses to PE and CE interfaces. The address-assignment pool feature supports subscriber management and DHCP management functionality by enabling you to create centralized IPv4 address pools independently of the client applications that use the pools.</p> <p>Select the check box to enable allocation of PE-CE IP addresses from IP address pools. By default, this check box is deselected. Clear the check box to disable the address-assignment pools functionality.</p>
IP Pool Type	<p>Select an IP pool type option:</p> <ul style="list-style-type: none"> • Global—A Global IP address pool pertains to the service provider. There can be more than one global IPv4 address pool. However, each global pool must have its own unique name and its set of IPv4 addresses must not overlap with those of any other global pool. You can allocate addresses from global pools across multiple Layer 3 VPNs across multiple customers. The IP addresses allocated to services are unique across customers. • Customer—A Customer IP address pool pertains to an existing customer. These pools are associated with the corresponding customer. You can associate more than one customer IPv4 pool with each customer. However, each customer pool must have its own set of IPv4 addresses which must not overlap with those of any other pool belonging to the same customer. You can allocate addresses from customer pools across multiple Layer 3 VPNs for a particular customer. The IP addresses allocated to services are unique within specified customer services. <p>For more information on creation an IP pool, see “Creating an IP Address Pool” on page 389.</p>
Auto-pick PE Interface IP Address	<p>Select an option:</p> <ul style="list-style-type: none"> • Clear the check box to enable the service provider to specify the IP address of a provider edge (PE) interface. • Select the check box to cause the IP address of a provider edge (PE) interface to be selected automatically. <p>To override this setting in the service order, you can select the Editable in Service Order check box.</p>

Table 85: Layer 3 VPN Service Definition - PE-CE UNI Settings (continued)

Field	Action
IP Address Block Size	<p>Specify the size of the IPv4 IP addressee block allocated for each provider edge (PE) or customer edge (CE) link.</p> <p>Range: 1 through 32</p> <p>To override this setting in the service order, you can select the Editable in Service Order check box.</p>

2. Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

After you complete reviewing the settings, click **Finish** to complete the service definition creation.

Reviewing the Configured Settings

The Review page of the service definition or service order creation and modification wizards enable you to view and evaluate the service parameters and components you configured in preceding steps or pages of the wizard. This page provides a comprehensive, single-page view of all the service elements configured in the different pages of the wizard. You can either click the buttons corresponding to the various settings at the top of the wizard page to directly traverse to the page you want to modify or click the navigation buttons at the bottom of the wizard page to go to the different pages of the wizard.



NOTE: On the Review page, in the Service Templates section, the names of the service templates with which the service definition is associated are displayed. The Default Service Template column indicates whether the attached template is the default template.

To examine and modify the configured service definition settings:

1. Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify.
2. Click **Edit** next to the section that contains the parameter you want to modify. You are navigated to the corresponding page of the wizard in which the parameter settings are defined.

3. Click **Done** to save the service definition or service order.
4. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

The service order inventory window appears.

Related Documentation

- [Creating a Full-Mesh Layer 3 VPN Service Definition on page 709](#)
- [Creating a Service Definition for Point-to-Point Pseudowire Access into a Layer 3 VPN on page 730](#)
- [Creating a Multicast VPN Service Definition on page 732](#)

Creating a Service Definition for Point-to-Point Pseudowire Access into a Layer 3 VPN

Creating a pseudowire between two terminating PE devices allows you to encapsulate traffic from the Layer 2 VPN into a Layer 3 VPN, thereby providing access to Layer-3 services. Also known as *pseudowire stitching*, the benefit of this feature is that devices running older technologies will continue to function when networks are upgraded and Layer-3 technologies are in play.

To use this feature, the following prerequisites must be met:

- An existing Layer 3 VPN must be used as the target VPN.
- A device with an LT interface must be used to create the pseudowire.

To create the pseudowire, in the Network Services > Connectivity view pane, select **Service Design > New > P2P Service Definition**.

1. Define the general settings for the service definition.

Field	Action
Name	Provide a name for the service definition.
Service type	The service type is point-to-point pseudowire
Comments	Enter any comments that will help describe the service definition and its purpose.
Interface type	Specify the type of interface as Ethernet. Also check the box to enable pseudowire access into the Layer 3 VPN network.

2. Click **Next** to display the **Connectivity** window.

Field	Action
VC ID selection	Choose from Auto pick or Select Manually for VC ID assignment.

Field	Action
Default MTU (Bytes)	Indicate the MTU size or use the default that appears in the field.

- Click **Next** to display the **Site Settings** window.
- Define the UNI settings for the service definition. This definition can be created as a port-to-port or 802.1q link. This procedure shows the port-to-port Ethernet settings.

Site Settings Field	Action
Traffic Treatment Settings	
Ethernet option	Indicate the Ethernet option to use for this point-to-point service definition. Choices are port-port or dot1q .
Customer traffic type	This field can be left blank.
VLAN ID selection	This field can be left blank.
Interface Settings	
Physical IF encapsulation	The interface encapsulation for the port-to-port link must be specified as ethernet-ccc .
Logical IF encapsulation	This field is not used.
MTU Settings	
Default MTU (Bytes)	This field is populated with the default MTU value of 1522. If you are not using the default value, enter the MTU value in bytes.
MTU range (Bytes)	If you are specifying a custom MTU value, indicate the range of values in bytes.

If you are creating an 802.1q link, use the following settings:

- Click **Finish** and then create the service order.



NOTE: On the Review page, in the Service Templates section, the names of the service templates with which the service definition is associated are displayed. The Default Service Template column indicates whether the attached template is the default template.

- Related Documentation**
- [Creating a Full-Mesh Layer 3 VPN Service Definition on page 709](#)
 - [Creating a Hub-and-Spoke \(One Interface\) Layer 3 VPN Service Definition on page 719](#)

- [Creating a Multicast VPN Service Definition on page 732](#)

Creating a Multicast VPN Service Definition

This topic describes how the Connectivity Services Director application enables you to create an L3VPN service definition preliminary to creating a Multicast VPN (MVPN) service order.

Refer to the topic [“Creating a Full-Mesh Layer 3 VPN Service Definition” on page 709](#).



NOTE: Multicast VPN services are supported on LN2600 and MX devices only.

To create a L3VPN Service definition upon which to base a MVPN service order, in the Network Services > Connectivity view pane, select **Service Design > Manage Service Definitions > New > L3VPN Service Definition**.

1. Specify values for the parameters in the **General** and **Site Settings** windows as described in the following tables.

In the **General** settings window, add information in the relevant fields as described in the following table:

Field	Description
Service Definition Name	Type a name for this service definition.
Service type	Select L3VPN (Full Mesh)
Description	Type comments to describe the service definition.
Service Template	None
Enable MVPN	Select this check box to enable MVPN settings in L3VPN service orders to be based on this service definition.
Decouple Service Status from Port Status	Do not select this check box.

2. Click **Next**.

3. In the **Site Settings** window, add information in the relevant fields as described in the following table:

Field	Description
Ethernet	Select this check box.

Field	Description
Auto-pick VLAN ID	Select this check box.
VLAN range for auto-pick	N/A
VLAN range for manual input	N/A
Auto-pick Route Target	A site within a VPN that a PE router services and to which the PE router will distribute routes.
Auto-pick Router Distinguisher	<p>An identifier attached to a route that distinguishes the VPN to which the route belongs. Each routing instance must have a unique route distinguisher associated with it.</p> <p>Select Auto pick. JUNOS Space selects the route distinguisher automatically.</p>
VRF Table label	<p>A VRF table label distinguishes one VRF instance from another and enables double lookup and egress filtering.</p> <p>Select this check box.</p>
Export Direct Routes	Select this check box.
Allowed Routing Protocols	Select BGP/Static Route
PE Interface IP Address	<p>The IP address of the interface on the PE device.</p> <p>Select Auto pick.</p>
IP Pool Type	<p>Global—A Global IP address pertains to the service provider. There can be more than one global IPv4 address pool. However, each global pool must have its own unique name and its set of IPv4 addresses must not overlap with those of any other global pool. You can allocate addresses from global pools across multiple Layer 3 VPNs across multiple customers.</p> <p>Customer—A Customer IP address pool pertains to an existing customer. These pools are associated with the corresponding customer. You can associate more than one customer IPv4 pool with each customer. However, each customer pool must have its own set of IPv4 addresses which must not overlap with those of any other pool belonging to the same customer. You can allocate addresses from customer pools across multiple Layer 3 VPNs for a particular customer.</p>
IP Address Block Size	<p>The size of the IPv4 addresses block allocated for each PE/CE link.</p> <p>Range: 28–32</p>

4. Click **Review** to examine the settings and modify any attributes as required.



.....

NOTE: On the Review page, in the Service Templates section, the names of the service templates with which the service definition is associated are displayed. The Default Service Template column indicates whether the attached template is the default template.

.....

5. Click **Finish**.

**Related
Documentation**

- [Creating a Full-Mesh Layer 3 VPN Service Definition on page 709](#)
- [Creating a Hub-and-Spoke \(One Interface\) Layer 3 VPN Service Definition on page 719](#)
- [Creating a Service Definition for Point-to-Point Pseudowire Access into a Layer 3 VPN on page 730](#)

PART 8

Service Provisioning: Working with Customers

- [Service Provisioning: Managing Customers on page 737](#)

Service Provisioning: Managing Customers

- [Adding a New Customer on page 737](#)
- [Deleting Customers on page 738](#)
- [Modifying an Existing Customer on page 739](#)
- [Viewing Customer Details on page 740](#)

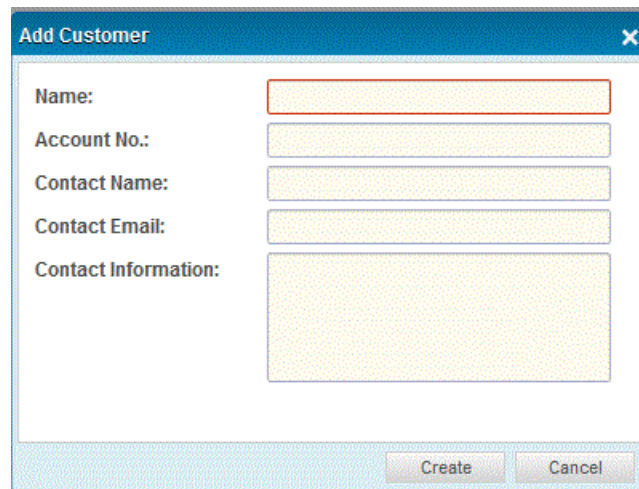
Adding a New Customer

New customers must be identified to the system before you can provision and activate a service order for them.

To add a customer to the database:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. In the **Network Services > Connectivity** task pane, select **Customer > Manage Customers**. The View Customers window is displayed.
4. Click the **Add** icon above the table of listed customers. The Add Customer dialog box is displayed.

Figure 38: Add Customer Dialog Box

A screenshot of the 'Add Customer' dialog box. The dialog has a blue title bar with the text 'Add Customer' and a close button (X). The main area contains five labels with corresponding input fields: 'Name:' with a single-line text box, 'Account No.:' with a single-line text box, 'Contact Name:' with a single-line text box, 'Contact Email:' with a single-line text box, and 'Contact Information:' with a multi-line text area. At the bottom right, there are two buttons: 'Create' and 'Cancel'.

5. On the **Create Customer** dialog box, provide the information requested for the customer, similar to the following example.

Fill out the fields in the form.

The **Name** and **Account number** fields are required. All other fields are optional.

6. Click **Create**.

The **View Customers** page shows the new customer.

Related Documentation

- [Deleting Customers on page 738](#)
- [Modifying an Existing Customer on page 739](#)
- [Viewing Customer Details on page 740](#)

Deleting Customers

You cannot delete a customer from the database if an active service exists for that customer. You must decommission all such services before you can delete the customer.

To delete a customer from the database:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. In the **Network Services > Connectivity** task pane, select **Customer > Manage Customers**. The View Customers window is displayed.

4. Select the customer you need to delete by clicking the row of the corresponding customer.

5. Click the **Delete** above the list of displayed customers.

If the **Delete** option is dimmed, it indicates that you have not selected a customer that must be cleared for the operation to succeed.

After successfully selecting the **Delete** action, a pop-up window appears requesting confirmation.

6. Click **Delete**.

The **View Customers** page no longer lists the deleted customer.

Related Documentation

- [Adding a New Customer on page 737](#)
- [Modifying an Existing Customer on page 739](#)
- [Viewing Customer Details on page 740](#)

Modifying an Existing Customer

To edit the information about an existing customer:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. In the **Network Services > Connectivity** task pane, select **Customer > Manage Customers**. The View Customers window is displayed, which shows the customers already added to the system.
4. Select the customer you need to modify by clicking the row of the corresponding customer.
5. Click the **Edit** icon above the table of displayed customers.
6. Make the required changes to the customer information.
7. Click **Modify**.

The **View Customers** page shows the modified information.

- Related Documentation**
- [Adding a New Customer on page 737](#)
 - [Deleting Customers on page 738](#)
 - [Viewing Customer Details on page 740](#)

Viewing Customer Details

To view your customers:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. In the **Network Services > Connectivity** task pane, select **Customer > Manage Customers**. The View Customers window is displayed, which shows the customers already added to the system.
4. Click the plus sign (+) next to the Customers tree in the Service View pane and select the customer for which you need to view detailed, extensive information.
5. From the View Customers page, click the **Details** icon above the table of displayed customers.

Alternatively, for details about a specific customer, double-click the listed customer.

Name	Account	Contact	Email
15_1Customer	1	-	-
Amazon	261456451	-	-
Orange	Orange	Orange	Orange@test.net
vpis_sanity	account_120251	-	-
vpis_sanity_idp	account_120252	-	-
vpis_sanity_idp_rerun	account_120253	-	-

The **Details** window displays the customer name, account number, contact name, contact e-mail address, and contact information in the upper half of the page. The

lower half of the page displays the **Services Provisioned for Customer** pane. This pane contains three tabs: P2P, VPLS, and L3VPN. The following fields are displayed in a table under each tab, depending on the type of service associated with a customer.

Field	Description
Name	Name of the service order assigned during service creation or edit.
Service Type	One of the following: <ul style="list-style-type: none"> Point-to-Point Ethernet (LDP) VPLS—Either a multipoint-to-multipoint service or a point-to-multipoint service
Customer	Name of the enterprise customer who placed an order for the service.
Order State	Status of the service order: <ul style="list-style-type: none"> Completed—Service order has been successfully deployed. Deploy failed—Device is down or the Connectivity Services Director application was unable to push the service configuration to a device configured for the service. In-progress—Connectivity Services Director application is in the process of deploying the service. Requested—Service provisioner has created the service order, but has not yet attempted to deploy it or schedule it for deployment. Scheduled—Service provisioner has scheduled the service order for deployment. Invalid—Service order contains invalid data.
FA Status	Status of functional audit of the service.
Fault Status	Fault management status of the service.
SLA Status	Service-level agreement status of the service. If data exceeds the threshold value specified in the Threshold Alarm Profile, the system generates a threshold alarm. The value in the SLA Status column changes to SLA Violated. If the data does not cross the threshold value specified in the Threshold Alarm Profile, the value in the SLA Status column changes to SLA Violation Cleared.
PM Status	Performance management status of the service.
Definition	Name of the service definition upon which the service order is based.
Activation Date	Date and time at which the service order was last activated.
Last Modified Time	Date and time at which the profile was last updated.
Image Name	Name of the image file to pictorially depict the customer.

Field	Description
Domain ID	Unique domain identifier associated with the customer.

6. To restrict the display of customers, enter a search criterion of one or more characters in the Search bar and press Enter. All customer names that match the search criterion are shown in the main display area.

**Related
Documentation**

- [Adding a New Customer on page 737](#)
- [Deleting Customers on page 738](#)
- [Modifying an Existing Customer on page 739](#)
- [Viewing Customer Details on page 740](#)

PART 9

Working in Deploy Mode

- [About Deploy Mode on page 745](#)
- [Deploying and Managing Device Configurations on page 751](#)
- [Deploying and Managing Software Images on page 789](#)

CHAPTER 29

About Deploy Mode

- [Understanding Deploy Mode in Views Other than Service View of Connectivity Services Director on page 745](#)
- [Understanding the Deploy Mode Tasks Pane in Views Other than Service View on page 748](#)

Understanding Deploy Mode in Views Other than Service View of Connectivity Services Director

The Deploy mode enables you to deploy configuration changes and software upgrades to devices and perform several device management and configuration file management tasks.

This topic describes:

- [Deploying Configuration Changes on page 745](#)
- [Managing Software Images on page 747](#)
- [Managing Devices on page 747](#)
- [Managing Device Configuration Files on page 747](#)
- [Managing Baseline Configuration on page 747](#)

Deploying Configuration Changes

When you make configuration changes in Build mode, the changes are not deployed to devices automatically. You must manually deploy the changes to devices in Deploy mode. Every time you make configuration changes in Build mode that affect a device, the device is automatically added to the list of devices with pending changes. Configuration changes are deployed to devices at the device level. When you deploy configuration changes to a device, all pending configuration changes for that device are deployed.

You can deploy the device configurations in the following two ways:

- **Auto Approval**—In this mode, the device configuration changes are approved automatically by the system and do not require explicit (manual) approval by a configuration approver before they can be deployed. This is the default approval mode.

- **Manual Approval**—In this mode, the device configuration changes are required to be explicitly approved by a configuration approver before the changes can be deployed to the device.



NOTE: Manual approval is not supported in Connectivity Services Director.

For more information about enabling these modes, see [“Setting Up User and System Preferences” on page 122](#).

An operator performs device configurations and creates a change request for that configuration and submits it for approval to an approver. The approvers are notified by e-mail whenever a change request is created. If a configuration or a change to it is approved by an approver, then the operator is able to deploy it. If a configuration is rejected then the operator must make the necessary changes, resubmit the change request, and procure an approval before the configuration can be deployed. For more information, see [“Approving Change Requests” on page 765](#)



NOTE: You can specify any number of approvers. If you specify more than one approver while configuring the Manual Approval mode, once an approver accepts or rejects the proposed change, the change request is not listed for the other approvers and they cannot approve or reject the same change request.

You can do the following configuration deployment tasks on devices that have pending changes:

- Run configuration deployment jobs immediately or schedule them for future times.
- Approve the change requests for pending configurations, if you have selected the Manual Approval mode.
- Preview pending configuration changes before deploying the changes.
- Validate that the pending changes are compatible with the device's configuration.
- Manage configuration deployment jobs.

Configuration changes are validated for each device both in Connectivity Services Director and on the device. If any part of a configuration change for a device fails validation, no configuration changes are deployed to the device. You can see the results of each validation phase separately.

Connectivity Services Director will not deploy configuration to a device with a configuration that is out of sync (meaning that the device's configuration differs from Connectivity Services Director's version of that device's configuration), or to a device that has uncommitted changes to its candidate configuration. Deployment to such devices will fail.

When you schedule a deployment job, that job and any profiles and devices assigned to that job are locked within Connectivity Services Director. You cannot edit the job or any

of its assigned profiles until the job runs or gets cancelled. This locking feature prevents you from deploying unintended configuration changes that could result from editing profiles and devices that are already scheduled to deploy. To change any properties of a scheduled job, cancel the job and create a new scheduled job with the desired properties. You cannot edit the profile assignments of a device that has scheduled pending configuration changes.

Managing Software Images

Connectivity Services Director can manage software images on the nodes it manages. You can do the following software image management tasks:

- Deploy a software image stored in an image repository on the Connectivity Services Director server to multiple devices with a single job.
- Track the status of software image management jobs.
- Stage and install software images as separate tasks.
- Schedule staging and installation to happen at independent future times.
- Perform several software image upgrade options, such as rebooting devices automatically after the upgrade finishes.



NOTE: Using nonstop software upgrade (NSSU) to upgrade EX Series switches is supported in Connectivity Services Director.

Managing Devices

In Deploy mode you can perform several device management tasks, including:

- View the device inventory.
- Show a device's current configuration.
- Resynchronize the device configuration maintained in Build mode with the configuration on the device. For more information about resynchronization of device configuration, see [“Understanding Resynchronization of Device Configuration” on page 773](#)

Managing Device Configuration Files

You can back up device configuration files to the Connectivity Services Director server. You can perform several actions on backed up configuration files, such as restoring configuration files to devices, and viewing and comparing configuration files.

Managing Baseline Configuration

You can baseline device configuration and the OS version to the Connectivity Services Director server. You can perform several actions on baseline configuration files, such as restoring configuration files to devices, and viewing and comparing configuration files.

Understanding the Deploy Mode Tasks Pane in Views Other than Service View

The Tasks pane in Deploy mode lists the available tasks. All Deploy mode tasks are always available, regardless of the scope selected in the View pane.

Deploy mode tasks are divided into the following categories:

- **Configuration Deployment**—These tasks enable you to deploy configuration changes to devices and manage configuration deployment jobs. [Table 87 on page 748](#) describes the configuration deployment tasks.
- **Image Management**—These tasks enable you to manage software images on devices. [Table 88 on page 749](#) describes the image management tasks.
- **Device Management**—These tasks enable you to view the device inventory, resynchronize the configuration of out-of-sync devices, manage the administrative state of ports, manage QFabric node groups, and convert QSFP+ port configuration. [Table 89 on page 749](#) describes the device management tasks.
- **Device Configuration File Management**—These tasks enable you manage configuration files on managed devices. [Table 90 on page 749](#) describes the device configuration file management tasks.
- **Baseline Management**—These tasks enable you manage baseline configuration of devices. [Table 91 on page 749](#) describes the baseline management tasks.
- **Key Tasks**—Connectivity Services Director enables you to group the tasks that you perform frequently and create a list of key tasks. You can add any task from the Tasks pane to the Key Tasks list by selecting a task and clicking the plus (+) sign that appears adjacent to the task. For some modes, you can see that Connectivity Services Director has predefined some key tasks for you. You can modify this set of tasks to suit your requirements. This feature is available in Task pane irrespective of your current mode, scope, or view.

[Table 87 on page 748](#) through [Table 90 on page 749](#) describe the tasks in each task category.

Table 87: Configuration Deployment Tasks

Task	Description
Deploy Configuration Changes	Deploys pending configuration changes to devices.
Approve Change Requests	Enables a configuration approver to approve or reject a change request, which has been submitted for approval by an operator.
Set SNMP Trap Configuration	Enables SNMP traps on Connectivity Services Devices so that Connectivity Services Director can collect and manage event and error information from these devices.
View Deployment Jobs	Manages configuration deployment jobs.

Table 88: Image Management Tasks

Task	Description
Manage Image Repository	Manages the software images repository on the server.
Deploy Images to Devices	Deploys software images from the repository to devices.
View Image Deployment Jobs	Manages software image deployment jobs.

Table 89: Device Management Tasks

Task	Description
Resynchronize Device Configuration	Resynchronizes the device configuration maintained in Build mode with the running configuration on the devices.
Show Current Configuration	Shows the selected device's current configuration.
View Inventory	Displays the device inventory of the selected node.

Table 90: Device Configuration File Management Tasks

Task	Description
Manage Device Configuration Files	Manages backup device configuration files.
View Configuration File Mgmt Jobs	Manages device configuration file management jobs.

Table 91: Baseline Management Tasks

Task	Description
Manage Baseline	Manages baseline configuration files.
View Baseline Mgmt Jobs	Manages baseline configuration file management jobs.

CHAPTER 30

Deploying and Managing Device Configurations

- [Deploying Configuration to Devices on page 751](#)
- [Managing Configuration Deployment Jobs on page 762](#)
- [Deploy Configuration Window on page 764](#)
- [Approving Change Requests on page 765](#)
- [Enabling SNMP Categories and Setting Trap Destinations on page 767](#)
- [Understanding Resynchronization of Device Configuration on page 773](#)
- [Resynchronizing Device Configuration on page 778](#)
- [Managing Device Configuration Files on page 783](#)
- [Enabling or Disabling Network Ports on Routers on page 787](#)

Deploying Configuration to Devices

When you make configuration changes in Build mode, the changes are not deployed to devices automatically. You must manually deploy the changes to devices in Deploy mode.

To start deploying configuration changes:

1. Click **Deploy** in the Connectivity Services Director banner.
2. Select a node in the View pane that contains the devices to which you want to deploy.
3. In the Tasks pane, select **Configuration Deployment > Deploy Configuration Changes**.

Depending upon the type of approval mode you select different windows are displayed.

If you select the Auto Approval mode, the Devices with Pending Changes page opens in the main window, listing the devices within the selected node that have pending configuration changes.

If you select the Manual Approval mode, the following two sections open in the main window:

- **Devices with recent configuration changes**—This section lists the devices with pending changes (along with the details of the change) performed by the user currently logged into the system.
- **Change Requests**—This section lists the change requests created by the user currently logged into the system.

This topic describes:

- [Selecting Configuration Deployment Options on page 752](#)
- [Using the Change Request Details Page on page 755](#)
- [Creating a Change Request on page 756](#)
- [Validating Configuration on page 756](#)
- [Discarding the Pending Configurations on page 757](#)
- [Viewing Pending Configuration Changes on page 757](#)
- [Using the Pending Changes Window on page 758](#)
- [Using the Configuration or Pending Configuration Window on page 758](#)
- [Using the Deploy Configuration Errors/Warnings Window on page 758](#)
- [Using the Configuration Validation Window on page 759](#)
- [Deploying Configuration Changes to Devices Immediately on page 759](#)
- [Scheduling Configuration Deployment on page 759](#)
- [Specifying Configuration Deployment Scheduling Options on page 760](#)
- [Editing Change Requests on page 760](#)
- [Deleting Change Request on page 761](#)
- [Resubmitting a Change Request on page 761](#)
- [Performing a Rollback on page 762](#)

Selecting Configuration Deployment Options

Based on the approval mode, you can choose to deploy the device configuration changes in the following ways:

- When you select the auto approval mode, the page **Devices with Pending Changes** open. From the **Devices with Pending Changes** page, you can:
 - Deploy configuration changes immediately by selecting one or more devices and clicking **Deploy Now**. For more information, see [“Deploying Configuration Changes to Devices Immediately” on page 759](#).
 - Schedule configuration deployment by selecting one or more devices and clicking **Schedule Deploy**. For more information, see [“Scheduling Configuration Deployment” on page 759](#).
 - View configuration changes that are pending on a device by clicking **View** in the **Configuration Changes** column. For more information, see [“Viewing Pending Configuration Changes” on page 757](#).

- Validate that the pending changes for a device are compatible with the device's configuration by selecting up to ten devices and clicking Validate Pending Configuration Changes. For more information, see [“Validating Configuration” on page 756](#).
- Discard the pending configuration changes. For more information, see [“Discarding the Pending Configurations” on page 757](#).

[Table 92 on page 753](#) describes the information provided in the table on the Devices with Pending Changes page. Only the subset of devices within the selected object that have pending configuration changes are listed in the table.

Table 92: Devices with Pending Changes Page

Table Column	Description
Check box	Select to perform an action on the device in that row
Name	Device name
IP Address	Device IP address
Model	Device Model
OS Version	Operating system version running on device
Connection State	State of the connection to the device: <ul style="list-style-type: none"> • Up—Connectivity Services Director can communicate with the device. • Down—Connectivity Services Director cannot communicate with the device. You cannot deploy configuration to devices that are down.
Configuration State	Indicates whether the device's configuration is in sync with Connectivity Services Director's version: <ul style="list-style-type: none"> • In Sync—The configuration on the device is in sync with the Connectivity Services Director configuration for the device. • Out Of Sync—The configuration on the device does not match the Connectivity Services Director configuration for the device. This state is usually the result of the device configuration being altered outside of Connectivity Services Director. You cannot deploy configuration on a device when the device is Out Of Sync. To resolve this state, use the Resynchronize Device Configuration task in Deploy mode. • Synchronizing—The device configuration is in the process of being resynchronized. • Sync failed—An attempt to resynchronize an Out Of Sync device failed.
Configuration Changes	Click to view pending configuration changes for a device. The Pending Changes window opens.

If you select the Manual Approval mode, the windows Devices with recent configuration changes and Change Requests opens.

From the Devices with recent configuration changes window, you can:

- Create a device configuration change request approval and submit it for approval. Upon submission, all device changes made by an operator are validated and all the approvers are notified of the details of the proposed change request by e-mail. For more information, see [“Creating a Change Request” on page 756](#).
- View configuration changes that are pending on a device by clicking View in the Configuration Changes column. For more information, see [“Viewing Pending Configuration Changes” on page 757](#).
- Validate that the pending changes for a device are compatible with the device's configuration. For more information, see [“Validating Configuration” on page 756](#).
- Discard the pending configuration changes. For more information, see [“Discarding the Pending Configurations” on page 757](#).



NOTE: You cannot delete a device from the Devices with Pending Changes list. To remove a device from the list, you must undo the Build mode configuration changes that placed the device on the list.

[Table 93 on page 754](#) describes the information provided in the table on the Devices with recent configuration changes page.

Table 93: Devices with recent configuration changes

Table Column	Description
Name	Indicates the name of the device and profile node. Below each device node, a profile node is listed.
Change Type	Indicates the type of the configuration change done to the device.
Associations Added	Lists the ports that are added to that profile.
Associations Deleted	Lists the ports that are deleted from that profile.
Configuration	Click to view pending configuration changes for a device. The Pending Changes window opens.
Deployment State	Indicates the deployment state of a change request.

From the Change Requests window, you can:

- Deploy configuration changes immediately by selecting one or more devices and clicking Deploy Now. For more information, see [“Deploying Configuration Changes to Devices Immediately” on page 759](#).
- Schedule configuration deployment by selecting one or more devices and clicking Schedule Deploy. For more information, see [“Scheduling Configuration Deployment” on page 759](#).

- Resubmit for the change request for approval after making the necessary modifications. For more information, see [“Resubmitting a Change Request” on page 761](#).
- Edit or delete the change requests by selecting one or more change requests and clicking Edit or Delete respectively. For more information, see [“Editing Change Requests” on page 760](#) and [“Deleting Change Request” on page 761](#).
- Roll back the device configuration that is already deployed. For more information, see [“Performing a Rollback” on page 762](#).
- View the details of the change request created. For more information, see [“Using the Change Request Details Page” on page 755](#)

[Table 94 on page 755](#) describes the information provided in the table on the change requests submitted for the devices for which configuration changes are sought.

Table 94: Change Requests

Table Column	Description
Check Box	Select to perform an action on the device in that row.
Change Request No	Indicates the change request number of the change request that is waiting to be deployed.
Title	Indicates the title name of the change request.
Created On	Indicates the change request creation date.
Approver	Indicates the username of the configuration approver.
Last Action On	Indicates the date on which the change request status is changed.
Approval Status	Indicates whether a change request is approved or rejected by the approver.
Deployment Status	Indicates whether a change request is deployed after the approval.
History Icon	Records the audit trail details of a change request, such as operation performed on a change request during a given period of time, username of the approver or operator, and so on.

Using the Change Request Details Page

Use the Change Request Details window to view the details of the change request before you either approve or reject a change request. This window provides you the details such as change request number, title, username of the user who created the change request, change request creation date and so on. A Devices table is also displayed showing the deployment status. [Table 95 on page 755](#) describes the fields in this table.

Table 95: Change Request Details

Column	Description
--------	-------------

Table 95: Change Request Details (continued)

Name	Indicates the name of the device and profile node. Below each device node, a profile node is listed.
Change Type	Indicates the type of the configuration change done to the device.
Associations Added	Lists the ports that are added to that profile.
Associations Deleted	Lists the ports that are deleted from that profile.
Configuration	Click to view pending configuration changes for a device. The Pending Changes window opens.
Deployment Status	Indicates the deployment state of a change request.

Creating a Change Request

To create a change request for device configurations approval:

1. Click **Create Change Request** in the Devices with recent configuration changes page.
The Create Change Request page opens.

2. Enter the change request number.

You can either enter a number or retain the autogenerated number in this field.

3. Enter an appropriate title name for the change request.
4. Optionally, you can enter comments for the device configuration changes.
5. Click **Submit**.

The Create Change Request page opens, listing the change request details such as change request number, title, and comment, along with the change request submission job details. A Devices table is also displayed showing the validation status of the device and configuration generated for that device.

6. Click **Close**.

A new change request entry with the status Pending Approval is added to the Change Request section.

Validating Configuration

When you deploy configuration changes to a device, validation checks are performed to validate that the pending changes are compatible with the device. You can also perform this validation without deploying.



NOTE: You can also verify the configuration from the Build mode by clicking **Tasks > Domain Management > Validate Pending Configuration**.

To validate that the pending changes for devices are compatible with the device configuration:

1. For Auto Approval mode, select up to ten devices in the Devices with Pending Changes page.



NOTE: For Manual Approval mode, you cannot choose the devices for which validation needs to be done. All the configuration changes for all the devices are validated.

2. Click **Validate Pending Configuration Changes**.

The Configuration Validation window opens. See [“Using the Configuration Validation Window” on page 759](#) for a description of the window.

Discarding the Pending Configurations

Use the Discard Local Configuration Changes Results window to discard all the pending configurations that were made on a device. Once you discard the local configuration changes on a device, the configuration state of the device changes to In Sync or Out of Sync based on the system of record (SOR) mode set for the Junos Space Network Management Platform. If the SOR mode is set to Network as system of record (NSOR), then the configuration state changes to In Sync and if the SOR mode is set to Junos Space as system of record (SSOR), then the configuration state changes to Out of Sync.

To discard the configuration changes:

1. For Auto Approval mode, select the devices for which you want to discard the pending configuration and click **Discard Pending Configuration**.

The Discard Local Configuration Changes Results window opens displaying the status of the discard pending configuration job.

2. Click **Close** to close the Discard Local Configuration Changes Results window.

Viewing Pending Configuration Changes

To view pending configuration changes for a device, click **View** in the Pending Changes column.

The Pending Changes window opens. See [“Using the Pending Changes Window” on page 758](#) for a description of the window.

Using the Pending Changes Window

Use the Pending Changes window to view the pending Connectivity Services Director changes for a device. [Table 96 on page 758](#) describes the fields in this window.

Table 96: Pending Changes Window

Field	Description
Name	Lists each selected device. Expand a device by Clicking its plus sign to see its pending changes. Each pending change to a profile or other configuration object for the device is listed.
State	Describes the nature of the pending change to the configuration object. These are the possible states: <ul style="list-style-type: none"> • Added—The profile or configuration object was added to this device. • Removed—The profile or configuration object was removed from the device • Updated—The profile or configuration object was updated.
Configuration	Click View to view the pending configuration changes for a device. The Pending Configuration window opens. See “Using the Configuration or Pending Configuration Window” on page 758 for information about the window. NOTE: The device configuration state must be In Sync for you to view the pending configuration changes.
Close	Click to close the window.

Using the Configuration or Pending Configuration Window

Use the Pending Configuration window to view the configuration changes that will be deployed to a device when a job runs. Use the Configuration window to see changes that were deployed to a device when a completed job ran. The configuration changes are shown in these formats:

- Select the **XML View** tab to view the configuration changes in XML format. This view shows the XML-formatted configuration that will be deployed to the device's Device Management Interface (DMI), which is used to remotely manage devices.
- Select the **CLI View** tab to view the configuration changes in CLI format. This view shows the Junos configuration statements that will be deployed to the device.

In both views, the content is color-coded for easier reading:

- Black text indicates configuration that is already active on the device, and will not be changed if you deploy.
- Green text indicates configuration that will be added if you deploy.
- Red text indicates configuration that will be removed if you deploy.

Using the Deploy Configuration Errors/Warnings Window

Use the Deploy Configuration Errors/Warnings window to view the results of deploying configuration to a device. The Errors/Warnings in validating the device configuration pane

shows the results of configuration validation by Connectivity Services Director. The Errors/Warnings in Updating Device configuration pane shows the results of configuration validation on the device.

Using the Configuration Validation Window

Use the Configuration Validation window to validate that the pending changes for a device are compatible with the device's configuration. [Table 97 on page 759](#) describes this window.

Table 97: Configuration Validation Window

Table Column	Description
Object name	Lists the devices you selected for validation. Click the arrow next to a device to expand it. If there are no errors or warnings, one item labeled No Validation warnings appears. If the device has errors or warnings, they appear under the device. The device contains a list of the profiles that caused errors or warnings. Expand a profile name to see the of errors and warnings it caused.
Errors/Warnings	Describes the error or warning.

Deploying Configuration Changes to Devices Immediately

To deploy configuration changes to devices immediately:

1. Select the device or devices in the Devices with Pending Changes page.
2. Click **Deploy Now**.

The Deploy Options window opens.

3. In the Deploy Options window, enter a job name in the Deployment Job Name field, then click **OK**.

The configuration deployment job runs. The Deploy Configuration window opens and shows the results of the deployment job. For a description of fields in this window, see *Deploy Configuration Window*.

Scheduling Configuration Deployment

To schedule configuration deployment to devices:

1. Select the device or devices in the Devices with Pending Changes page.
2. Click **Schedule Deploy**.

The Deploy Options window opens.

3. Use the Deploy Options window to schedule the configuration deployment. See [“Specifying Configuration Deployment Scheduling Options” on page 760](#) for a description of the window.

Specifying Configuration Deployment Scheduling Options

Use the Deploy Options window to schedule configuration deployment jobs.
[Table 98 on page 760](#) describes the actions for the fields in this window.

Table 98: Deploy Options Window

Field	Action
Deployment Job Name	Enter a job name.
Date and Time	Enter the job's start date and time.
OK	Click to accept changes and exit the window.
Cancel	Click to cancel changes and exit the window.

Editing Change Requests

You can edit a change request to change the profile that was added to a device or delete some of the profile associations. After editing a change request, you can resubmit the change request for approval. While editing a change request, if you try to delete all the profile associations in a given change request, the system prompts a message that a change request should have at least one valid association. Deleting all the associations in a change request makes it invalid. Hence, you cannot delete all the associations in a given change request. However, you can delete a change request itself to delete all the associations for that change request.



NOTE: You are unable to delete a change request or an association of a change request if an association is in pending removal state.

You are unable to edit a change request that is in Cancelled, Deployed, Rollback Success, or Rollback Failed state.

To change a profile or delete the profile associations of a change request:

1. Select the change request in the Change Requests pending action page to edit.
2. Click **Edit**.
The Edit Change Request window opens.
3. Click the call out symbol to change the profile and choose the new profile that you want to assign.. the change request.
4. To delete a profile association, click **Delete**
5. Click **Save**.

The Edit Change Request window opens, listing the change request details such as change request number, title, and comment, along with the change request submission job details. A Devices table is also displayed showing the validation status of the device and configuration generated for that device.

6. Click **Close**.

Deleting Change Request

Sometimes you might need to delete a change request from the change request list. A change request is assigned with profile associations. If you delete a change request, all the associations of that change request are also deleted.

To delete a change request:

1. Select the change request or change requests in the Change Requests pending action window.
2. Click **Delete**.

The Delete Change Request window opens, displaying the message: **Are you sure you want to delete Change Request?**

3. Click **Yes** to delete the change request; else click **No**.

If you clicked **Yes**, the message: **Change Request deleted successfully** appears.

4. Click **OK**.

Resubmitting a Change Request

You can resubmit only those change requests that are in Pending Approval, Pending Deployment, Deploy Failed, and Create Failed state. You are unable to resubmit change requests in Deployed, Cancelled, Rollback Success, or Rollback Failure state.

In certain situations, a device can go out of sync while a user is creating a change request for that device. The change request is created, but the configuration changes for that change request are not generated. You can select the change request and resubmit it after the device is in sync again, which generates the configuration for this change request. You can resubmit change requests only for devices that have pending configuration changes.

To resubmit a change request:

1. Select the change request in the Change Requests pending action window to edit.
2. Click **Resubmit**.

A warning message pops up indicating if you want to resubmit the change request.

3. Click **Yes**.

The Resubmit Change Request window opens, listing the change request details such as change request number, title, and comment, along with the change request submission job details. A Devices table is also displayed showing the validation status of the device and configuration generated for that device.

4. Click **Close**.

Performing a Rollback

In case of any misconfigurations, you can choose to roll back a configuration that has already been deployed to the device. The following conditions apply for a rollback operation:

- The maximum number of change requests that you can roll back is the rollback limit specified in Preferences.
- Change requests are rolled back in reverse chronological order; the later change requests are rolled back first. If there are any conflicting change requests, roll back is not supported. For example, assume that a user assigns port profile P1 to ge-0/0/1 and creates a change request CR1 and deploys the profile. After this, if the user edits P1, creates another change request CR2 and deploys and removes P1 from the port by assigning some other port profile and deploys device changes or configurations as part of CR3. If the user now tries to roll back CR1, an error message about the conflicting change requests CR2 and CR3 is shown. To roll back CR1, the user must roll back CR3, then CR2, and then CR1.

Managing Configuration Deployment Jobs

When you deploy configuration changes or schedule a configuration deployment, a configuration deployment job is created.

To start managing configuration deployment jobs:

1. Click **Deploy** in the Connectivity Services Director banner.
2. In the Tasks pane, select **Device Management > View Deployment Jobs**.

The Deploy Configuration page opens in the main window. The table on that page lists configuration deployment jobs.

This topic describes:

- [Selecting Configuration Deployment Job Options on page 763](#)
- [Viewing Configuration Deployment Job Details on page 764](#)
- [Canceling Configuration Deployment Jobs on page 764](#)

Selecting Configuration Deployment Job Options

From the Deploy Configuration page, you can:

- View the details of a configuration deployment job by clicking Show Details. See [“Viewing Configuration Deployment Job Details” on page 764](#) for more information.
- Cancel a scheduled configuration deployment job by clicking Cancel Job. See [“Canceling Configuration Deployment Jobs” on page 764](#) for more information.

[Table 99 on page 763](#) describes the information provided on the Deploy Configuration page

Table 99: Deploy Configuration Table Description

Table Column	Description
Check box	Select to perform an action on the job in that row.
Job Id	An identifier assigned to the job.
Job Name	Job name (user-created).
Percent	Percentage of the job that is complete.
Status	Job status. The possible states are: <ul style="list-style-type: none"> • CANCELLED—The job was cancelled by a user. • FAILURE—The job failed. This state is applied if any of the devices in the job failed. But some of the devices might have completed successfully. View the job details for the status of each device. • INPROGRESS—The job is running. • SCHEDULED—The job is scheduled but has not run yet. • SUCCESS—The job completed successfully. This state is applied if all of the devices in the job completed successfully.
Summary	Job summary.
Scheduled Start Time	Job's scheduled start time
Actual Start Time	Time when the job started.
End Time	Time when the job ended
User	User who created the job
Recurrence	This field is not used for configuration deployment jobs.

Viewing Configuration Deployment Job Details

To view the details of a configuration deployment job:

1. Select the job in the table.
2. Click **Show Details**. The Deploy Configuration window opens. See *Deploy Configuration Window* for a description of the window.

Canceling Configuration Deployment Jobs

To cancel a configuration deployment job:

1. Select the job in the table.
2. Click **Cancel Job**.
3. Click **Yes** in the confirmation window that opens.

Deploy Configuration Window

The Deploy Configuration window shows the results of a completed deployment job or information about a scheduled job. See [Table 100 on page 764](#) for a description of the fields in this window.

Table 100: Deploy Configuration Window

Field	Description
Job Name	Job name.
Job Start Time	Time when job started or will start.
Job End Time	Time when job ended.
Percentage Completed	Percentage of the job that is complete.
Number of Devices	Number of devices in the deployment job.
Deployed Devices table	
Name	Device name.
IP Address	Device IP address.

Table 100: Deploy Configuration Window (continued)

Field	Description
Deployment Status	<p>Status of configuration deployment on device:</p> <ul style="list-style-type: none"> • Scheduled—Job is scheduled for future deployment. • In Progress—Deployment is in progress. • Success—Deployment completed successfully. • Failed—Deployment failed.
Configuration	<p>Click View to see the configuration changes that were deployed to the device. See “Deploying Services Configuration to Devices” on page 758 for more information.</p> <p>For a scheduled job, this column does not contain a link. See “Deploying Services Configuration to Devices” on page 1005 for information about viewing pending configuration changes for a device.</p>
Result Details	Click View to see the results of configuration deployment for the device.
Close	Click to close the window.

Approving Change Requests



NOTE: This option is available only for the users who are assigned a Configuration Approver role.

When you select the Approve Change Request option, the page Change request(s) pending approval and the page approved/declined change request(s) open in the top and bottom panels respectively.

The [Table 101 on page 765](#) shows details of the change requests that are pending for approval by the approver.

Table 101: Change request(s) pending approval

Table Column	Description
Change Request No	Indicates the change request number that was either approved or rejected by the approver.
Title	Indicates the title of the change request.
Created By	Indicates the operator name who created the change request and submitted it for approval.
Created On	Indicates the date on which the change request was created.
Age	Indicates the age of the change request, time since the change request was created.
Deployment Status	Indicates the deployment state of the change request.

Table 101: Change request(s) pending approval (continued)

Table Column	Description
History Icon	Records the audit trail details of a change request, such as operation performed on a change request during a given period of time, username of the operator, and so on.

The [Table 102 on page 766](#) shows the change requests that were approved or rejected by the currently logged in approver. The approver can also provide comments

Table 102: approved/declined change request(s)

Table Column	Description
Change Request No	Indicates the change request number that was either approved or rejected by the approver.
Title	Indicates the title of the change request.
Created By	Indicates the operator name who created the change request and submitted it for approval.
Created On	Indicates the date on which the change request was created.
Age	Indicates the age of the change request, time since the change request was created.
Approval Status	Indicates the approval state of the change request.
Deployment Status	Indicates the deployment state of the change request.
History Icon	Records the audit trail details of a change request, such as operation performed on a change request during a given period of time, username of the approver, and so on.

To approve or reject the change requests submitted by an operator:

1. Select **Approve Change Requests** under Configuration Deployment.
2. Select the check box against the change request and click on a change request in the change request(s) pending approval page.
The Change Request Details page opens.
3. Review details of the profile and its associations.
4. Click on the **View** link.
The Pending Configuration device name page opens.
5. Click **Close**.

6. Click **Approve** or **Reject** to approve or reject the device configuration changes respectively.

The Change Request Details page opens.

7. Type your comments and click **Approve** to approve; else click **Reject**.

After the successful approval, you can deploy the device configurations immediately or schedule the deployment for a later period.

Enabling SNMP Categories and Setting Trap Destinations

SNMP traps must be enabled on network devices for Connectivity Services Director to collect and manage event and error information from these devices.

Connectivity Services Director organizes switch and controller traps by categories. These categories must be enabled and deployed in order to forward trap information to Connectivity Services Director.



NOTE: Connectivity Services Director uses protocol port 10162 for receiving traps from devices. This port must be open on the devices.

This topic describes:

- [Viewing Eligible Devices for Trap Forwarding on page 767](#)
- [Enabling Trap Forwarding on page 768](#)
- [Deploying SNMP Trap Configurations on page 769](#)

Viewing Eligible Devices for Trap Forwarding

Traps are enabled on the Devices page in Deploy mode. To locate this page:

1. Select **Deploy** in the Connectivity Services Director banner.
2. Select **Set SNMP Trap Configuration** in the Tasks pane. The Devices page opens. For a description of fields in the Devices page, view [Table 103 on page 767](#).

Table 103: Device Page Fields

Field	Description
Name	Either the hostname or the IP address of the device.
IP Address	Device IP address.
Model	Device model number.
OS Version	Version and release level of the operating system running on the device.

Table 103: Device Page Fields (continued)

Field	Description
Connection State	<p>State of connection to the device. Valid states are:</p> <ul style="list-style-type: none"> • Up—Connectivity Services Director is in communication with the device. • Down—Connectivity Services Director cannot communicate with the device. You cannot enable traps on devices that are in this state.
Configuration State	<p>Either the device's configuration is in sync or out-of-sync with Connectivity Services Director's version:</p> <ul style="list-style-type: none"> • IN_SYNC—The configuration is in-sync with the database. • OUT_OF_SYNC—The configuration is out-of-sync with the database.

Enabling Trap Forwarding

Select **Set SNMP Trap Configuration** in Deploy mode to enable your network devices to pass SNMP traps and events to Connectivity Services Director. Connectivity Services Director creates a target group called *networkdirector_trap_group* using target port 10162. The Community name is *public* and the access is *read-write-notify*.

Before enabling trap forwarding, complete device discovery for all the devices and ensure they are in the up state. Down devices cannot be enabled for trap forwarding.

Selecting Set SNMP Trap Configuration displays the Devices page which contains a table of all discovered switches and controllers in the network. To enable SNMP traps on switches and controllers:

1. Either select individual check boxes for devices, or select the check box next to the Name heading to select all devices. These devices must be up and in the same device family.
2. Click **Deploy Trap Configuration**. The Deploy Options window opens.
3. Fill in a new deployment job name or accept the default name of Deploy SNMP Targets.
4. Either select check boxes for individual traps, or select the check box next to the Trap Name heading to select all traps. These traps are discussed further in [“Deploying SNMP Trap Configurations”](#) on page 769.



TIP: To clear an existing configuration, do not select any of the check boxes.

5. Click **Ok**. The Deploy Configuration window opens, which shows the status of deploying the configuration change.
6. Review the outcome of the deployment.

After enabling the traps, enable the alarms and establish the alarm retention period. These tasks are located in Preferences in the Connectivity Services Director banner.

Deploying SNMP Trap Configurations

The Deploy Options for trap forwarding enable you to select individual traps or all traps for the selected device family.

The device family determines which traps are displayed in the Deploy Options window. The following tables map the trap to one or more MIBs being used.

- EX Series switches traps and related MIBs are shown in [Table 104 on page 769](#).
- Controllers traps and related MIBs are shown in [Table 105 on page 770](#).

Table 104: EX Series Switches Traps

Trap	MIB
Chassis	jnxExMibRoot.mib
Link	snmpTraps.mib
Configuration	jnxCfgMgmt.mib
Authentication	jnxJsAuth.mib
Remote operations	jnxPing.mib
Routing	jnx-ipv6.mib
Startup	snmpTraps.mib
Rmon-alarm	jnxRmon.mib
Vrrp-events	rfc2787a.mib
Services	jnxServices.mib
Sonet-alarms	jnx-sonetaps.mib
Otn-alarms	jnxMibs.mib

Table 105: Controllers Traps

Trap	MIB
LinkDown	snmpTraps.mib
LlinkUp	snmpTraps.mib
Authentication	snmpTraps.mib
DeviceFail	trpzTrapsV2.mib
DeviceOkay	trpzTrapsV2.mib
PoEFail	trpzTrapsV2.mib
MobilityDomainJoin	trpzTrapsV2.mib
MobilityDomainTimeout	trpzTrapsV2.mib
RFDetectAdhocUser	trpzTrapsV2.mib
ClientAuthenticationFailure	trpzTrapsV2.mib
ClientAuthorizationFailure	trpzTrapsV2.mib
ClientAssociationFailure	trpzTrapsV2.mib
ClientDeAssociation	trpzTrapsV2.mib
ClientRoaming	trpzTrapsV2.mib
AutoTuneRadioPowerChange	trpzTrapsV2.mib
AutoTuneRadioChannelChange	trpzTrapsV2.mib
CounterMeasureStart	trpzTrapsV2.mib
CounterMeasureStop	trpzTrapsV2.mib
ClientDot1xFailure	trpzTrapsV2.mib
RFDetectDoS	trpzTrapsV2.mib
RFDetectDoSPort	trpzTrapsV2.mib
ClientIpAddrChange	trpzTrapsV2.mib
ClientAssociationSuccess	trpzTrapsV2.mib
ClientAuthenticationSuccess	trpzTrapsV2.mib

Table 105: Controllers Traps (continued)

Trap	MIB
ClientDeAuthentication	trpzTrapsV2.mib
RFDetectBlacklisted	trpzTrapsV2.mib
RFDetectAdhocUserDisappear	trpzTrapsV2.mib
ApRejectLicenseExceeded	trpzTrapsV2.mib
ClientDynAuthorChangeSuccess	trpzTrapsV2.mib
ClientDynAuthorChangeFailure	trpzTrapsV2.mib
ClientDisconnect	trpzTrapsV2.mib
MobilityDomainFailOver	trpzTrapsV2.mib
MobilityDomainFailBack	trpzTrapsV2.mib
RFDetectRogueDeviceDisappear	trpzTrapsV2.mib
RFDetectSuspectDeviceDisappear	trpzTrapsV2.mib
RFDetectedClientViaRogueWiredAP	trpzTrapsV2.mib
RFDetectedClassificationChange	trpzTrapsV2.mib
ConfigurationSaved	trpzTrapsV2.mib
APNonOperStatus	trpzTrapsV2.mib
MichaelMICFailure	trpzTrapsV2.mib
ApManagerChange	trpzTrapsV2.mib
ClientCleared	trpzTrapsV2.mib
MobilityDomainResiliencyStatus	trpzTrapsV2.mib
ApOperRadioStatus	trpzTrapsV2.mib
ClientAuthorizationSuccess	trpzTrapsV2.mib
RFDetectRogueDevice	trpzTrapsV2.mib
RFDetectSuspectDevice	trpzTrapsV2.mib
ClusterFailure	trpzTrapsV2.mib

Table 105: Controllers Traps (continued)

Trap	MIB
MultimediaCallFailure	trpzTrapsV2.mib
ApTunnelLimitExceeded	trpzTrapsV2.mib
WsTunnelLimitExceeded	trpzTrapsV2.mib
RFNoiseSource	trpzTrapsV2.mib
M2UConvNotPossibleTrap	trpzTrapsV2.mib
M2UConvAvailabilityRestored	trpzTrapsV2.mib

Understanding Resynchronization of Device Configuration

In a network managed by Connectivity Services Director, three separate repositories about device configuration are maintained:

- The configuration information on the devices themselves. Each device maintains its own configuration record.
- The configuration information maintained by the Junos Space Network Management Platform. When a device is discovered, either by Junos Space or Connectivity Services Director, Junos Space stores a record of the configuration on that device.

Connectivity Services Director uses the configuration record maintained by Junos Space to determine what configuration commands need to be sent to the device when you deploy configuration on the device in Deploy mode.

- The configuration information maintained by Connectivity Services Director in Build mode. This information takes the form of the profiles assigned to the device, plus the additional configuration, such as LAG and access point configuration, that you can do under device management.

In Connectivity Services Director, the configuration state of a device is shown as In Sync when the configuration information in all three repositories match. If there is a conflict between the configuration information in one or more of the repositories, Connectivity Services Director shows the device configuration state as Out of Sync.

An Out of Sync state is usually the result of out-of-band configuration changes—that is, configuration changes made to a device using a management tool other than Connectivity Services Director. Examples of such changes include changes made by:

- Using the device CLI.
- Using the device Web-based management interface (the J-Web interface or Web View).
- Using the Junos Space Network Management Platform configuration editor.
- Using RingMaster software.
- Restoring or replacing device configuration files.

You cannot deploy configuration on a device when the device configuration state is Out of Sync.

This topic describes how Connectivity Services Director enables you to resynchronize the device configuration state. It covers:

- [The Resynchronize Device Configuration Task on page 774](#)
- [How Resynchronization Works in NSOR Mode on page 774](#)
- [How Resynchronization Works in SSOR Mode on page 776](#)
- [How Connectivity Services Director Resynchronizes the Build Mode Configuration on page 778](#)

The Resynchronize Device Configuration Task

Connectivity Services Director provides a task in Deploy mode that enables you to resynchronize the repositories of configuration information. When an out-of-band configuration change is made, you can use this task to resynchronize both the Junos Space configuration record and the Build mode configuration with the configuration on the device.

How Connectivity Services Director performs resynchronization depends on the system of record (SOR) mode set for the Junos Space Network Management Platform. There are two possible modes:

- Network as system of record (NSOR). This is the default mode.
- Junos Space as system of record (SSOR).

You set the mode in Junos Space under Administration > Applications > Network Management Platform > Modify Application Settings.

How Resynchronization Works in NSOR Mode

In NSOR mode, the network device is considered the system of record for device configuration, which means the configuration maintained by the device takes precedence over the configuration maintained by Junos Space and Connectivity Services Director. Thus when you perform a resynchronization, the Junos Space configuration record and the Connectivity Services Director Build mode configuration are updated to match the device configuration.

When an out-of-band change is made on a managed device when Junos Space is in NSOR mode:

1. Junos Space detects that a configuration change has occurred on the device and informs Connectivity Services Director about the change.
2. Both Junos Space and Connectivity Services Director set the device configuration state to Out of Sync.
3. Junos Space and Connectivity Services Director automatically resynchronizes its configuration record to match the device configuration and sets the device configuration state to In Sync when the synchronization completes. Connectivity Services Director performs auto-synchronization when it is operating in the Network as System Of Record (NSOR) mode. The auto-resynchronization parameters are defined in the Preferences page. These parameters enables auto-resynchronization after the interval specified in this page. For more information see, *Setting Up User and System Preferences*.
4. When the device out-of-band changes does not conflict with Connectivity Services Director, Connectivity Services Director automatically resynchronizes the network changes and retains the local changes in Connectivity Services Directory. The configuration state of the device and the profile associated with that device remains

unaffected. For example, if you modify the MTU value of the port ge-0/0/1 in Connectivity Services Director and another user modifies the MTU value of port ge-0/0/2 on the same device, Connectivity Services Director automatically resynchronizes the changes on ge-0/0/2 into Connectivity Services Director and retains the local changes on ge-0/0/1. The profile corresponding to ge-0/0/1 continues to remain in Pending Deployment state and the profile corresponding to port ge-0/0/2 is in Deployed state.

5. When the device out-of-band changes conflict with the changes made in Connectivity Services Director, Connectivity Services Director does not automatically resynchronize the device changes into Connectivity Services Director. The device is marked as Out Of Sync, and you must manually resynchronize the changes by using the Resynchronize Configuration task. After this, the local changes are discarded and are replaced by the latest network configuration. For example, if you modify MTU of ge-0/0/1 from Connectivity Services Director and another user modifies MTU of the same port on the device, Connectivity Services Director does not automatically synchronize and marks this device as Out Of Sync.
6. When a profile associated with a device is either added or removed from that device while another user tries to change the attributes corresponding to that profile, Connectivity Services Director does not automatically synchronize the device and marks the device as Out Of Sync, and you must manually resynchronize the changes by using the Resynchronize Configuration task.
7. When you make local changes to profiles, the changes are merged with the new profiles if there is no conflicting configuration. If there are conflicting changes, Connectivity Services Director receives an Out Of Sync message from Junos Space and you need to manually choose the appropriate profile value.

When you do not make any local changes on a profile, the device association with the profile is deleted and a new device association is created. However, when a profile has local changes, the device association of the profile is not deleted.

8. If the configuration change does not affect configuration that you can perform in Build mode (for example, routing configuration), Connectivity Services Director also sets the device configuration state to In Sync after the Junos Space resynchronization completes. All three configuration repositories are now in sync.

If the configuration change affects configuration that you can perform in Build mode, Connectivity Services Director does not set the device configuration state to In Sync. Instead, it continues to show the device configuration state as Out of Sync because the Build mode configuration does not match the device configuration.

9. To resolve the Out of Sync state in Connectivity Services Director, use the Resynchronize Device Configuration task in Deploy mode. Connectivity Services Director updates the Build mode configuration to match the out-of-band changes.
10. Connectivity Services Director sets the device configuration state to In Sync.



.....

NOTE: Automatic resynchronization, as described in Step 3 above, is a default setting for the Junos Space Network Management Platform. If automatic resynchronization is disabled, you must manually resynchronize the Junos Space configuration with the device configuration. You can do so in two ways:

- Use the Resynchronize with Network action in Junos Space. The Junos Space configuration is synchronized with the device configuration. However, the Build mode configuration is not synchronized, so the device state in Connectivity Services Director remains Out of Sync. You must use the Resynchronize Device Configuration task in Deploy mode to resynchronize the Build mode configuration.
 - Use the Resynchronize Device Configuration task in Deploy mode. In this case, Connectivity Services Director resynchronizes both the Junos Space configuration and the Build mode configuration with the device configuration.
-

How Resynchronization Works in SSOR Mode

When Junos Space is in SSOR mode, Junos Space is considered the system of record for device configuration. In this mode, when an out-of-band configuration change occurs on a device, you can choose whether to accept the change or to overwrite the change with the configuration maintained by Junos Space.

When an out-of-band change is made on a managed device when Junos Space is in SSOR mode:

1. Junos Space detects that a configuration change has occurred on the device and informs Connectivity Services Director about the change.
2. Junos Space sets the device configuration state as Device Changed, and Connectivity Services Director sets the device configuration state to Out of Sync.

Connectivity Services Director sets the device configuration state to Out of Sync even if the configuration change does not affect configuration you can perform in Build mode. This allows you to resolve the Device Changed configuration state for Junos Space from Connectivity Services Director.

3. In Connectivity Services Director, use the Resynchronize Device Configuration task to accept or reject the out-of-band changes:
 - If you accept the out-of-band changes, both the Junos Space configuration record and the Connectivity Services Director Build mode configuration are resynchronized to reflect the out-of-band configuration changes.

- If you reject the out-of-band changes, the configuration on the device is overwritten by the configuration record maintained by Junos Space. The Connectivity Services Director Build mode configuration remains unchanged.
4. Both Junos Space and Connectivity Services Director set the device configuration state to In Sync.

The above process differs somewhat when out-of-band configuration changes are made through the Junos Space configuration editor. In this case:

1. Junos Space sets the device configuration state as Space Changed after the configuration change is saved.

At this point, the changes have been made only in the Junos Space configuration record and the changes have not yet been deployed to the device. Connectivity Services Director shows the device configuration state as In Sync.



NOTE: Because the device configuration state is In Sync in Connectivity Services Director, you can deploy configuration on the device from Connectivity Services Director at this point. If you do so, the Connectivity Services Director changes are deployed on the device, but the Junos Space changes are not. The device state in Junos Space remains Space Changed.

2. When the changes are deployed to the device from Junos Space, Junos Space changes the device state to In Sync, while Connectivity Services Director changes the device state to Out of Sync.
3. In Connectivity Services Director, use the Resynchronize Device Configuration task to resolve the Out of Sync state. In this case, because the Junos Space configuration record and the device configuration are in sync, you cannot reject the changes. When you resynchronize the device in Connectivity Services Director, the Build mode configuration is updated to reflect the configuration changes.
4. Connectivity Services Director sets the device configuration state to In Sync.

If you use Junos Space instead of Connectivity Services Director to resolve out-of-band configuration changes in SSOR mode, note the following:

- If you reject an out-of-band change, the device state becomes In Sync in both Connectivity Services Director and Junos Space.
- If you accept an out-of-band change that does not affect the Build mode configuration, the device state becomes In Sync in both Connectivity Services Director and Junos Space.
- If you accept an out-of-band change that affects the Build mode configuration, the device state becomes In Sync in Junos Space but remains Out Of Sync in Connectivity

Services Director. You must use the Resynchronize Device Configuration task to resolve the Out of Sync state.



NOTE: When Junos Space is in SSOR mode, we recommend that you do not make out-of-band changes to the cluster configuration on the secondary seeds and member controllers of a mobility domain, such as disabling the cluster on these devices. Use Connectivity Services Director to modify the cluster configuration on these devices.

How Connectivity Services Director Resynchronizes the Build Mode Configuration

When you use the Resynchronize Device Configuration task to resynchronize the Build mode configuration to the device configuration, Connectivity Services Director launches a resynchronization job. This job deletes all profile assignments configured for the device. The profiles themselves are not deleted—just the assignments of the profiles to the device are deleted. It then reimports the device configuration, as if the device were a newly discovered device. It reassigns existing profiles and creates new profiles as necessary. Profiles that were originally assigned to the device will be reassigned to the device if the profiles were unaffected by the out-of-band changes. All profiles assigned to the device are in a deployed state at the end of the process. Any profile that is not reassigned to the device and is not assigned to any other device will be in a unassigned state.

Resynchronizing Device Configuration

A network managed by Connectivity Services Director has three repositories of information about the configuration of a network device—the configuration stored on the device itself, the device configuration record maintained by Junos Space, and the Build mode configuration maintained by Connectivity Services Director.

When the configuration contained in all three repositories match, the device configuration state is shown as In Sync in Connectivity Services Director. When the repositories do not match, the configuration state is shown as Out of Sync. A common cause for this state is out-of-band configuration changes—that is, configuration changes made to a device outside of Connectivity Services Director.

When a device state is Out of Sync, you cannot deploy configuration changes on the device in Deploy mode. Use the Resynchronize Device Configuration task to resynchronize the three configuration repositories and change the device configuration state back to In Sync.

How the Resynchronize Device Configuration task performs the resynchronization depends on the system of record (SOR) mode setting for the Junos Space Network Management Platform:

- When Junos Space is in network as system of record (NSOR) mode, the device is considered the system of record for configuration. When you resynchronize a device when Junos Space is in NSOR mode, both the Junos Space configuration record and the Connectivity Services Director Build mode configuration are updated to reflect the

device configuration—in other words, the out-of-band configuration changes are incorporated into both the Junos Space and the Connectivity Services Director configuration repositories.

- When Junos Space is in Junos Space as system of record (SSOR) mode, you can choose whether accept or reject the out-of-band changes reflected in the device configuration. If you accept the changes, both the Junos Space configuration record and the Connectivity Services Director Build mode configuration are updated to reflect the device configuration. If you reject the changes, the out-of-band changes are rolled back on the device so that the device configuration matches the Junos Space configuration record and the Connectivity Services Director Build mode configuration.

For more information about out-of-band configuration changes, Junos Space SOR modes, and how Connectivity Services Director resynchronizes device configuration, see *Understanding Resynchronization of Device Configuration*.

This topic covers:

- [The Resynchronize Device Configuration List of Devices on page 779](#)
- [Resynchronizing Devices When Junos Space Is in NSOR Mode on page 780](#)
- [Resynchronizing Devices When Junos Space Is in SSOR Mode on page 781](#)
- [Resynchronizing Devices in Manual Approval Mode on page 782](#)
- [Viewing the Network Changes on page 782](#)
- [Viewing Resynchronization Job Status on page 782](#)

The Resynchronize Device Configuration List of Devices

The Resynchronize Device Configuration page displays a list of all devices in the selected scope whose configuration was successfully imported during device discovery and whose configuration state is now Out Of Sync. You can select devices from this list and resynchronize them.

[Table 106 on page 779](#) describes the fields in the list of devices.

Table 106: Resynchronize Device Configuration Fields

Field	Description
Name	Device hostname or device IP address.
IP address	IP address of device.
Model	Model number of the device.
OS Version	Operating system version currently running on the device.
Connection State	Connection state: <ul style="list-style-type: none"> • UP—Connectivity Services Director is connected to the device • DOWN—Connectivity Services Director cannot connect to the device

Table 106: Resynchronize Device Configuration Fields (continued)

Field	Description
Configuration State	<p>Shows the configuration state of the device:</p> <ul style="list-style-type: none"> • Out Of Sync—The device configuration is out of sync with either the Connectivity Services Director Build mode configuration or the Junos Space configuration record or both. • Resynchronizing—The device configuration is in the process of being resynchronized. • Sync Failed—The resynchronization attempt failed. <p>If the resynchronization is successful, the device is removed from the table.</p>
Local Changes	<p>Specifies whether configuration changes have been made in Build mode and are pending deployment on the device.</p> <ul style="list-style-type: none"> • None—There are no configuration changes pending deployment. • View—There are configuration changes that are pending deployment. Click View to view the changes. These changes will be lost if you resynchronize the Build mode configuration to match the device configuration. <p>NOTE: The Pending Changes window that appears when you click View allows you to see what profiles have been added, modified, or changed. However, because the device is not in sync, you cannot view the specific changes in CLI or XML format.</p>
Network Changes	<p>Indicates whether you can view the out-of-band changes:</p> <ul style="list-style-type: none"> • None—The out-of-band changes are not available for viewing. You cannot view out-of-band changes in NSOR mode. In SSOR mode, you cannot view the out-of-band changes if they are already resolved in Junos Space—that is, the device configuration state in Junos Space is In Sync. • View—You can view the out-of-band changes made on the device. Click View to view the changes presented in XML format.

Resynchronizing Devices When Junos Space Is in NSOR Mode

To resynchronize devices when the Junos Space Network Application Platform is in NSOR mode:

1. On the Resynchronization Device Configuration page, select the device or devices that you want to resynchronize.
2. (Optional) View any pending changes to a device's configuration in Connectivity Services Director by clicking **View** in the Local Changes column. These pending changes are deleted when you resynchronize the device.
3. Click **Resynchronize Configuration**.

The Resynchronize Device Configuration Results window appears. This window will be updated with status of the resynchronization when the resynchronization completes.

Resynchronizing Devices When Junos Space Is in SSOR Mode

To resynchronize devices when the Junos Space Network Management Platform is in SSOR mode:

1. On the Resynchronization Device Configuration page, select the device or devices that you want to resynchronize.
2. (Optional) View any pending changes to a device's configuration in Connectivity Services Director by clicking **View** in the Local Changes column. These pending changes are deleted if you accept the out-of-band changes when you resynchronize the device.
3. (Optional) View the out-of-band configuration changes by selecting **View** in the Network Changes column. If you accept the out-of-band changes when you resynchronize the device, these changes will be reflected in the Build mode configuration. If you reject the out-of-band changes when you resynchronize the devices, these changes will be deleted from the device. For more information about viewing the out-of-band changes, see [“Viewing the Network Changes” on page 782](#).



NOTE: Out-of-band changes that were made with the Junos Space configuration editor or that were already accepted in Junos Space are not shown. Such changes also cannot be rejected.

4. Click **Resynchronize Configuration**.
5. In the Confirm dialog box:
 - Click **Accept device changes** if you want to accept the out-of-band changes.
 - Click **Reject device changes** if you want to reject the out-of-band changes and have the configuration that existed on the device before the out-of-band changes were made be reinstated.

click **Submit**.

The Resynchronize Device Configuration Results window appears. This window will be updated with status of the resynchronization when the resynchronization completes.



NOTE: Device changes made by the Junos Space configuration editor or device changes that have been accepted in Junos Space cannot be rejected. Even if you select Reject device changes, these changes will not be rejected and instead will be incorporated into the Build mode configuration.

Resynchronizing Devices in Manual Approval Mode

When out-of-band changes exist, device resynchronization merges the changes done by using the CLI with the local changes provided that there are no conflicts. If there are conflicting changes, the changes made using the CLI take precedence over the local changes. Therefore, configuration changes that are part of a change request might be lost. The configuration change requests that are lost are marked as Cancelled against the corresponding device. When device resynchronization is initiated for a device, a message is displayed that lists the change requests that will be lost because of conflicting CLI and local changes. All other changes remain unaffected.

Viewing the Network Changes

The Network Changes window shows the out-of-band configuration changes made to a device when Junos Space is in SSOR mode.

Not all out-of-band configuration changes are shown in this window. Configuration changes are shown only when the device configuration differs from the Junos Space configuration record—that is, when the device configuration state in Junos Space is not In Sync. For example, if the out-of-band changes were deployed from the Junos Space configuration editor or if the out-of-band changes were already accepted in Junos Space, the configuration changes will not appear in this window.

The configuration changes are shown in XML format. If there have been multiple out-of-band changes—that is, there has been more than one configuration commit, or save, on the device—the changes are grouped by each commit.

The following information is provided for each configuration commit:

- `junos:commit-seconds`—Specifies the time when the configuration was committed as the number of seconds since midnight on 1 January 1970.
- `junos:commit-localtime`—Specifies the time when the configuration was committed as the date and time in the device's local time zone.
- `xmlns:junos`—Specifies the URL for the DTD that defines the XML namespace for the tag elements.
- `junos:commit-user`—Specifies the username of the user who requested the commit operation.

Viewing Resynchronization Job Status

The Resynchronize Device Configuration Results window appears after you start a resynchronization job. This window is automatically updated with the resynchronization status for each device when the job completes.

You can also view the status of the resynchronization jobs using the Manage Jobs task in System mode. The following jobs are associated with resynchronization:

- **Resynch Network Elements**—This job runs in NSOR mode and resynchronizes the Junos Space configuration record with the device configuration.

- **Resolve OOB Changes**—This job runs in SSOR mode and resolves the out-of-band changes for Junos Space—either accepting the changes and updating the Junos Space configuration or rejecting the changes and rolling back the changes on the device.
- **Resynchronize devices**—This job runs in both NSOR and SSOR mode and resynchronizes the Build mode configuration with the device configuration.

Managing Device Configuration Files

You can back up device configuration files to the Connectivity Services Director server. You can perform several actions on backed up configuration files, such as restoring configuration files to devices, and viewing and comparing configuration files.

To start managing device configuration files:

1. Click **Deploy** in the Connectivity Services Director banner.
2. In the Tasks pane, select **Device Configuration Files > Manage Device Configuration Files**.

The Manage Device Configuration page opens in the main window. The table lists the devices that have configuration files backed up.

This topic describes:

- [Selecting Device Configuration File Management Options on page 783](#)
- [Backing Up Device Configuration Files on page 784](#)
- [Restoring Device Configuration Files on page 785](#)
- [Viewing Device Configuration Files on page 785](#)
- [Comparing Device Configuration Files on page 786](#)
- [Deleting Device Configuration Files on page 786](#)
- [Managing Device Configuration File Management Jobs on page 786](#)

Selecting Device Configuration File Management Options

From the Manage Device Configuration page, you can:

- Back up device configuration files by clicking Backup. See [“Backing Up Device Configuration Files” on page 784](#) for more information.
- Restore backup device configuration files to devices by selecting devices and clicking Restore. See [“Restoring Device Configuration Files” on page 785](#) for more information.
- View backed up configuration files by selecting a device and clicking View Configuration File. See [“Viewing Device Configuration Files” on page 785](#) for more information.

- Compare backed up device configuration files by selecting devices and clicking Compare Config Files. See “[Comparing Device Configuration Files](#)” on page 786 for more information.
- Delete backup device configuration files by selecting devices and clicking Delete. See “[Deleting Device Configuration Files](#)” on page 786 for more information.

Table 107 on page 784 describes the information provided in the Manage Device Configuration table.

Table 107: Manage Device Configuration Table

Table Column	Description
Device Name	Device name.
Config File Version	Version number of the backup configuration file.
First Backup on	Date when the oldest version of the backup configuration file was created.
Most Recent Backup on	Date when the configuration file was backed up most recently.

Backing Up Device Configuration Files

To back up device configuration files:

1. Click **Backup**.

The Backup Devices Configuration page opens in the main window.

2. Select the devices to back up from the device tree.

3. To back up configuration files immediately, click **Backup Now**.

The backup job runs. When it finishes, the Manage Device Configuration table shows updated information for the devices you backed up.

4. To schedule the backup to run later, click **Schedule Backup**.

The Schedule Backup window opens.

- a. Select the **Schedule at a later time** check box.
- b. Specify when the backup will run using the **Date and Time** fields.
- c. Optionally, configure the backup job to repeat by selecting the **Repeat** check box, then specifying the backup schedule using the provided fields.

Optionally, you can specify when repeated backups will stop by selecting the **End Time** check box, then specifying the last date on which the repeated backup job will run using the **Date and Time** fields.

- d. Click **Schedule Backup**.

Restoring Device Configuration Files

You can restore a backed up configuration file to the device from which it was backed up.



CAUTION: Restoring a configuration file to a device is considered an out-of-band configuration change, which can cause some unexpected results. For more information, see [“Out-of-Band Configuration Changes” on page 173](#).

To restore backed up configuration files to devices:

1. Select the devices to restore from the Manage Device Configuration list.
2. Click **Restore**.

The Restore Device Configuration File(s) window opens.

3. To restore a configuration file that is older than the most recent version, click in the **Latest Version** cell and select the version to restore.
4. Click **Restore**.

Viewing Device Configuration Files

To view the backed up configuration files for a device:

1. Select the device from the Manage Device Configuration list.
2. Click **View Configuration File**.

The Device Configuration Summary window opens, displaying the most recently backed up configuration file.

3. To view an older stored configuration file version, select a version number from the **Config File Version** list.

Comparing Device Configuration Files

To compare backed up device configuration files:

1. Select the configuration files to compare from the Manage Device Configuration list.
2. Click **Compare Configuration Files**.

The Compare Configuration Files window opens.

3. Select a source device from the **Source Device** list and a configuration file version from the **Config File Version** list.
4. Select a target device from the **Target Device** list and a configuration file version from the **Config File Version** list.
5. The configuration file versions you selected are displayed in the window. The file name and version appears at the top of each file. The differences between the configuration files are color-coded. The color-coding legend appears at the top of the window.

Deleting Device Configuration Files

When you delete a device's backed up configuration, all of the configuration file versions for the device are deleted.

To delete device configuration files:

1. Select the configuration files to delete from the Manage Device Configuration list.
2. Click **Delete**.

The Delete Device Configuration File(s) window opens.

3. Verify that the correct devices are listed, then click **Delete**.

Managing Device Configuration File Management Jobs

Each time you back up or restore device configuration files, a device configuration file management job is created.

To manage device configuration file management jobs:

1. Click **Deploy** in the Connectivity Services Director banner.
2. In the Tasks pane, select **Device Configuration Files > View Configuration File Mgmt Jobs**.

The Device Configuration Jobs page opens in the main window, listing the device configuration file management jobs.

Managing these jobs is similar to managing other types of jobs using the System mode. The advantage of accessing the jobs this way is that the jobs list show only configuration file management jobs. See [“Managing Jobs” on page 118](#) for more information.

Enabling or Disabling Network Ports on Routers

Network ports connect Routers to the network and carry network traffic. You can enable or disable network ports of Routers that are part of your network. When you enable or disable a port, the administrative status of the port changes to UP or DOWN respectively. When you disable a port, the system marks that port as administratively down, without removing the port configurations.

You can enable or disable one or more ports at a time using the Manage Port Admin State page. The status of the port is indicated by the Admin State and the Link State fields. The administrative status of a port is indicated by the Admin State field.

To enable or disable a network interface:

1. Do one of the following:
 - In the topology view, locate the device for which you want to enable or disable ports and click **Device Management > Manage Port Admin State** from the Tasks pane.
 - While in the Deploy mode, select the device for which you want to enable or disable ports in the View pane and click **Device Management > Manage Port Admin State** from the Tasks pane.

The Manage Port Admin State page appears displaying all the physical ports available on the selected device and the current status of each port. This page also displays the port mode of each interface, if any. Port mode can be access, tagged-access, or trunk mode.

2. Do one of the following:
 - Select the check box adjacent to the ports that you want to enable and click **Change Admin State UP**.
 - Select the check box adjacent to the interfaces that you want to disable and click **Change Admin State DOWN**.
3. Click **Done**. Connectivity Services Director changes the administrative status of the ports and displays a confirmation message confirming the changes.

Deploying and Managing Software Images

- [Managing Software Images on page 789](#)
- [Deploying Software Images on page 791](#)
- [Managing Software Image Deployment Jobs on page 795](#)

Managing Software Images

This topic describes how to manage software images for managed devices.

To start managing software images:

1. Click **Deploy** in the Connectivity Services Director banner.
2. In the Tasks pane, select **Image Management > Manage Image Repository**.

The Device Image Repository page opens in the main window. The table lists the software images in the repository.

3. In the Tasks pane, select **Device Configuration File Management > Manage Device Configuration**.

The Manage Device Configuration page opens in the main window. The table lists the devices that have configuration files backed up software images in the repository.

This topic describes:

- [Selecting Software Image Management Options on page 789](#)
- [Adding Software Images to the Repository on page 790](#)
- [Using the Device Image Upload Window on page 790](#)
- [Viewing Software Image Details on page 791](#)
- [Using the Device Image Summary Window on page 791](#)
- [Deleting Software Images on page 791](#)

Selecting Software Image Management Options

From the Device Image Repository page, you can:

- Add a software image to the repository by clicking **Add**.
- View details about a software image by selecting it and clicking **Details**.
- Delete software images from the repository by selecting them and clicking **Delete**.

[Table 108 on page 790](#) describes the information provided in the Device Image Repository table.

Table 108: Device Image Repository Table

Table Column	Description
Check box	Select to perform an action on the software image in that row.
Name	Software image name.
Version	Software version.
Series	Device series that uses the software image.
Uploaded By	User who uploaded the software image.
Created On	Time when the software image was uploaded to the server.
Size(MB)	Size of the software image in megabytes.

Adding Software Images to the Repository

Software images are stored in a repository on the Connectivity Services Director server.

To add a software image to the repository:

1. Click **Add**.

The Device Image Upload window opens.

2. Use the Device Image Upload window to upload a device software image. See [“Using the Device Image Upload Window” on page 790](#) for a description of the window.

Using the Device Image Upload Window

To use the Device Image Upload window to add a software image to the repository:

1. Click **Browse** and browse to the software image file.
2. Click **Upload** to add the file to the repository.

Viewing Software Image Details

To view details about a software image:

1. Select the software image file in the table.
2. Click **Details**.

The Device Image Summary window opens. See [“Using the Device Image Summary Window” on page 791](#) for information about this window.

Using the Device Image Summary Window

Use the Device Image Summary window to view detailed information about a software image. [Table 109 on page 791](#) describes the fields in this window.

Table 109: Device Image Summary Window

Field	Description
Name	Software image filename.
Version	Software version (release number).
Series	Device series on which the software is supported.
Supported Platforms	Platforms on which the software is supported.
Uploaded By	User who uploaded the image to the server.
Created On	Date and time when the software image was uploaded.
Size (MB)	Size of the software image file, in megabytes.
OK	Click to close the window.

Deleting Software Images

To delete software image files:

1. Select the check box in the rows of the software image files that you want to delete.
2. Click **Delete**.

Deploying Software Images

This topic describes how to deploy software images to managed devices. You must upload software images to the Connectivity Services Director server before you can deploy them to devices. See [“Managing Software Images” on page 789](#) for more information.

To start deploying software images:

1. Click **Deploy** in the Connectivity Services Director banner.
2. Select a node in the View pane that contains the devices to which you want to deploy software images.
3. In the Tasks pane, select **Image Management > Deploy Images to Devices**.

The Select Devices page of the Deploy Images to Devices wizard opens in the main window.

This topic describes:

- [Specifying Software Deployment Job Options on page 792](#)
- [Selecting Software Images To Deploy on page 793](#)
- [Selecting Options for Software Deployment on page 794](#)
- [Summary of Software Deployment on page 795](#)

Specifying Software Deployment Job Options

To specify software deployment job options in the Select Devices page:

1. In the Job name field, enter a job name.
2. From the Device and deployment options list, select an option:
 - Select **Staging only (Download image to the device)** to download the software image to the device but not install it.
 - Select **Upgrade only (Install previously staged image on device)** to upgrade the device to a software image that was previously staged on the device.
 - Select **Staging and Upgrade (Download and Install image on device)** to download the software image and install it on the device.

Devices are not automatically rebooted after upgrade to make the device begin running the new software version. You can select the option to reboot the device automatically after the upgrade in a later wizard page.

3. Click **Next** to continue to the next page.

The Select Images page opens. Select a software image as described in [“Selecting Software Images To Deploy” on page 793](#).

Selecting Software Images To Deploy

The Select Images page includes a table listing each device group and device that you selected for deployment. See [Table 110 on page 793](#) for a description of the table columns.

If you selected the Upgrade only (Install previously staged image on device) option, only devices that contain a previously staged software image appear in the table. You cannot select a different image to install on these devices.

To select the software images to deploy, perform the following steps on the table row for each device group or individual device that you want to upgrade:

1. In the Proposed Image Version/Profile column, click **Select Image/Profile**.

The Select Image/Profile list is displayed.

2. From the Select Image/Profile list, select a software image.



TIP: To clear this field, select **Select Image/Profile** from the list.

3. After you finish selecting software images, click **Next** to continue to the next page.

The Select Options page opens.



TIP: A pop-up message notifies you if you do not select a software image for all the listed devices. This is just for your information. No action will be taken on devices for which you do not select a software image. In effect, this removes those devices from the job.

Select options for software deployment as described in [“Selecting Options for Software Deployment” on page 794](#).

Table 110: Select images for devices Table

Table Column	Description
Device Family	Device family to which the device belongs. Devices are grouped by family. To display the devices within a device family, click the arrow next to the device family name.
Count	Number of devices contained within a device family.
IP Address	Device's IP address.
Device Name	Device's name.

Table 110: Select images for devices Table (continued)

Table Column	Description
State	Device's state: <ul style="list-style-type: none"> • UP—Connectivity Services Director can communicate with the device. • DOWN—Connectivity Services Director cannot communicate with the device.
Running Image Version	Software version the device is running.
Proposed Image Version/Profile	Software version that will be installed on the device when the job runs successfully.

Selecting Options for Software Deployment

The options that you can configure in the Select Options page are described in [Table 111 on page 794](#). The options that are available depend on the job flow you chose in the Select Images page.

After you finish selecting options, click **Next** to continue to the next page. The Summary page opens. Review the job summary as described in “[Summary of Software Deployment](#)” on page 795.

Table 111: Image Management Job Options

Option	Action
Select Options	
All Device Types	
Delete any existing image before download	Select to delete any existing software images on devices before downloading the new software image.
Reboot device after successful installation	Select to reboot the device after the software image is installed. A reboot is required to begin running the new software version on the device. NOTE: This option may get disabled based on your details that you specify in the remaining fields. This indicates that for the options that you specified, the system will automatically reboot the device as per the requirement during or after the image upgrade.
Wired Devices	
Check compatibility with current configuration	Select to validate the software package or bundle against the current configuration as a prerequisite to adding the software package or bundle.
ISSU/NSSU	Select if you want to perform a Nonstop software upgrade (NSSU) or lin-service software upgrade (ISSU). ISSU enables you to upgrade between two different Junos OS releases with minimal disruption on the control plane and with minimal disruption of traffic. NSSU enables you to upgrade the software running on an MX Series router with redundant Routing Engines or on most MX Series Virtual Chassis configuration by using a single command and with minimal disruption to network traffic

Table 111: Image Management Job Options (continued)

Option	Action
Archive data (Snapshot)	Select to take an archive snapshot of the files currently used to run the switch and copy them to an external USB storage device connected to the switch.
Copy to alternate slice	Select to copy the new Junos OS image into the alternate root partition. This ensures that the resilient dual-root partitions feature operates correctly. This option is available only if you select Reboot device after successful installation .
Select Schedule	
Stage now	Select Stage now to start staging software images to devices as soon as the job runs.
Stage later time	Select Stage later time to schedule the staging for a later time.
Staging Schedule	If you selected Stage later time, enter the date and time for staging to start.
Upgrade now	Select Upgrade now to start upgrading software images on devices as soon as staging finishes.
Upgrade later time	Select Upgrade later time to schedule the software upgrade for a later time.
Deployment Schedule	If you selected Upgrade later time, enter the date and time for upgrade to start. If you scheduled staging, you must schedule the upgrade for at least 10 minutes after staging, to ensure that staging completes before upgrade starts.

Summary of Software Deployment

On the Summary page, review the selections you made for the job. To change selections, click **Edit** in the area that you want to change. You can also click the boxes in the process flowchart above the wizard page to navigate between pages. When you are done making selections, click **Finish** on the Summary page to save the job, and run it if you configured the job to run immediately.

- Related Documentation**
- *Managing Software Image Deployment Jobs*
 - *Managing Software Images*

Managing Software Image Deployment Jobs

This topic describes how to manage software image jobs. A software image job is created each time you deploy software images to devices or schedule a software image deployment. You can check the status of jobs, see job details, and cancel scheduled jobs.

To start managing software image jobs:

1. Click **Deploy** in the Connectivity Services Director banner.
2. In the Tasks pane, select **Image Management > View Image Deployment Jobs**.

The Image Deployment Jobs page opens in the main window.

This topic describes:

- [Selecting Software Image Management Options on page 796](#)
- [Viewing Software Image Job Details on page 797](#)
- [Using the Device Image Staging Window on page 797](#)
- [Canceling Software Image Jobs on page 798](#)

Selecting Software Image Management Options

From the Image Deployment Jobs page, you can:

- Show deployment job details by selecting a job and clicking Show Details. See [“Viewing Software Image Job Details” on page 797](#) for more information.
- Cancel a pending job by selecting the job and clicking Cancel Job. See [“Canceling Software Image Jobs” on page 798](#) for more information.

[Table 112 on page 796](#) describes the information provided in the of the Image Deployment Jobs table.

Table 112: Image Deployment Jobs Table

Table Column	Description
Job Id	An identifier assigned to the job.
Check box	Select to perform an action on the job in that row.
Job Name	Job name.
Percent	Percentage of the job that is complete.
Status	Job status. The possible states are: <ul style="list-style-type: none"> • CANCELLED—The job was cancelled by a user. • SCHEDULED—The job is scheduled but has not run yet. • INPROGRESS—The job is running. • SUCCESS—The job completed successfully. This state is applied if all of the devices in the job completed successfully. • FAILURE—The job failed. This state is applied if any of the devices in the job failed. But some of the devices might have completed successfully. View the job details for the status of each device.
Summary	Job summary.
Scheduled Start Time	Job's scheduled start time.
Actual Start Time	Time when the job started.
End Time	Time when the job ended.

Table 112: Image Deployment Jobs Table (continued)

Table Column	Description
User	User who created the job.
Recurrence	This field is not used for software image management jobs.

Viewing Software Image Job Details

To view the details of a software image job:

1. Select the job in the table.
2. Click **Show Details**.

The Device Image Staging window opens. See [“Using the Device Image Staging Window” on page 797](#) for a description of the window.

Using the Device Image Staging Window

Use the Device Image Staging window to view information about software image jobs. [Table 113 on page 797](#) describes this window.

Table 113: Device Image Staging Window Description

Field	Description
Job Name	Job name.
Start Time	Job's scheduled start time.
End Time	Time when the job ended.
% Complete	Percentage of the job that is complete.
Status	Job status. The possible statuses are: <ul style="list-style-type: none"> • CANCELLED—The job was cancelled by a user. • SCHEDULED—The job is scheduled but has not run yet. • INPROGRESS—The job is running. • SUCCESS—The job completed successfully. • FAILURE—The job failed.
Host Name	Host name of device.
Status	Device status. The possible statuses are: <ul style="list-style-type: none"> • INPROGRESS—The job is running. • SUCCESS—The job completed successfully. • FAILURE—The job failed.

Table 113: Device Image Staging Window Description (continued)

Field	Description
% Complete	Percentage of the job that is complete on the device.
Start Time	Time when the job started on the device.
End Time	Time when the job ended on the device.
Description	Description of the job on the device. Can include error messages for failed devices.
Close	Click to close the window.

Canceling Software Image Jobs

To cancel a software image job:

1. Select the job in the table.
2. Click **Cancel**.

PART 10

Service Provisioning: Working with Service Orders

- [Service Provisioning: Viewing the Configured Services and Service Orders on page 801](#)
- [Service Provisioning: Managing Point-to-Point Service Orders on page 815](#)
- [Service Provisioning: Managing VPLS Service Orders on page 881](#)
- [Service Provisioning: Managing Layer 3 VPN Service Orders on page 939](#)

CHAPTER 32

Service Provisioning: Viewing the Configured Services and Service Orders

- [Viewing Service Orders on page 801](#)
- [Viewing Service Order and Service Details on page 803](#)
- [Viewing Services on page 807](#)
- [Viewing the Configured Point-to-Point, L3VPN, and VPLS Services on page 809](#)
- [Viewing the Configuration Details of VPN Services on page 812](#)

Viewing Service Orders

The following topic describes how you can view service orders.

- [Viewing Service Orders in a Table on page 801](#)

Viewing Service Orders in a Table

To view and determine the status of service orders in a tabular form:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the View pane, click the plus sign (+) to expand the Network Services > Connectivity tree and select the type of service.
4. In the Network Services > Connectivity view pane, select **Service Provisioning > Deploy Services**.

The Manage Service Deployment page is displayed in the lower half of the window.

Manage Service Orders							
Deploy Now Schedule Deploy View Pending Configuration Action Modify							
<input type="checkbox"/>	Name	Customer	State	Service Type	Signaling	Latest Job	Created Date
<input type="checkbox"/>	VPLS_LDP_451_audit_2015-09...	test	Completed	VPLS	LDP	822651	September 3, 20...
<input type="checkbox"/>	VPLS_LDP_451	test	Completed	VPLS	LDP	822647 ALL	September 3, 20... super

Page 1 of 1 Displaying 1 - 2 of 2 Show 3 items

A table of service orders on the system appears in the main display area. The following fields are displayed on this page:

- Name—Unique name assigned to the service.
- Customer—Name of the customer for which the service is provided.
- State:
 - Completed—Service order has been successfully deployed.
 - Failed—Device is down or the Connectivity Services Director application was unable to push the service configuration to a device configured for the service.
 - In-progress—Connectivity Services Director application is in the process of deploying the service.
 - Invalid—Service order contains invalid data.
 - Requested—Service provisioner has created the service order, but has not yet attempted to deploy it or schedule it for deployment.
 - Scheduled—Service provisioner has scheduled the service order for deployment.
- Service Type:
 - Point-to-point pseudowire (LDP)
 - Point-to-point pseudowire (BGP)
 - VPLS (MultiPoint-to-MultiPoint)
 - VPLS (Point-to-MultiPoint)
 - L3VPN (Full Mesh)
 - L3VPN (Hub-Spoke 1 Interface)
- Latest Job—Unique identifier assigned by the system for a deployment job. Click the link in the job ID to open the CSD Deployment Jobs. The table on that page lists configuration deployment jobs.
- Signaling Type:
 - BGP
 - LDP
- Created By—The screen name of the user who created the service order
- Created Date—The date and when you created the service order.

From this page, you can create a service order, modify the properties of the service order, conduct a functional or configuration audit, deploy or deactivate the service order, and view alarms associated with a particular service order for debugging and corrective action.

5. To view details of a specific service order, double-click the table row that summarizes the service order.

- Related Documentation**
- [Viewing Service Order and Service Details on page 803](#)
 - [Modifying a Saved Service Order on page 1107](#)
 - [Viewing Services on page 807](#)

Viewing Service Order and Service Details

In your network environment, it might be necessary to quickly view the list of deployed services for different protocols that you have defined, such as L3VPN or P2P, and obtain a high-level, comprehensive view of the different parameters defined for a service order. Based on the currently defined service attributes, you can modify them accordingly to suit your deployment needs. The service orders associated with customers that are shown also enable you to view the customer information and update the user-related details for a service order. The details for the service selected are displayed in a popup window such as the general settings, PE devices, UNI settings, the mapped service definition, and the corresponding service customer details. All the values shown in the details view are read-only fields.

You can launch the Service Detail window in two ways— by double-clicking a service order from the Manage Services page in Deploy Mode of Service View, and by selecting a service from the View pane and selecting Manage Services > View Details from the task pane in Deploy Mode of Service View to display detailed information for deployed services.

To view the consolidated details of a service:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.

- Select **L3VPN Services** to manage Layer 3 VPN Ethernet service orders.
- Select **P2P Services** to manage point-to-point service orders.
- Select **VPLS Services** to create and manage VPLS service orders.

Alternatively, you can drill-down the tree of each of the services, such as VPLS or L3VPN services, to view the previously configured service orders and modify their attributes.

- From the task pane, which is the middle pane in the window, select **Manage Services > View Details**. The Service Details window is displayed. The service details are grouped into various sections and only the applicable attributes are displayed for the selected service, based on the service type.

Alternatively, select **Deploy Services** from the task pane, and from the Manage Network Services window, select a service. The corresponding service order details are displayed in the Manage Service Orders window at the bottom of the right pane. Double-click a service order to view the service order details.

Figure 39: View Service Details Window

The screenshot shows the 'View Service Details' window. The 'Basic Details' section includes fields for Name, Customer, Service Definition, Service Order, Service Type, Signalling, State, Comments, Last Updated Date, Functional Audit, Fault Status, Configuration Audit, SLA Status, and Status. Below this is a 'View More' link. The 'End Points' section contains a table with columns: End Point, Device Name, Interface, Tagging, UnitId, VlanId, Template, and CoS Profiles. Two endpoints are listed: 'A' and 'Z'.

End Point	Device Name	Interface	Tagging	UnitId	VlanId	Template	CoS Profiles
A	960R1_EP...	ge-0/0/2.3	Ethernet	3	3	Interface_po...	
Traffic Type: DOT1Q Transport single vlan MTU: 1522 Logical Encapsulation: vlan-ccc Physical Encapsulation: flexible-ethernet-services							
Z	480R4_EP...	ge-0/0/2.3	Ethernet	3	3	P2P_LDP_L2...	
Traffic Type: DOT1Q Transport single vlan							

The Service Details window is divided into three sections—Basic Details, Advanced Details, and Endpoint Details. The service tree contains the service name as the root node. The device node is the child of the service node and it contains the provisioned UNIs as the child nodes. The details panel in the Endpoint Details table displays configuration parameters and their corresponding values for the service in the tree and based on the service type.

Under the Basic Details section, the general details about the node details are shown. Also, the device configuration parameters are displayed. Under the Advanced Details section, which you can open or close by clicking the View Less or View More toggle links, the advanced connectivity settings between sites in the service provider network are shown, such as route distinguisher and VRF route label details. Under the Endpoint

Details table, the configuration parameters of the UNI are displayed. The right pane displays the details corresponding to the node or element you selected on the left pane.

Under the Device Details section, the service details displayed on the right pane are organized under the following sections:

Basic Details

This section is applicable for all types of services and displays the following details.

- Name—Name of the selected service
- Customer—Name of the customer associated with the service.
- Service Definition—Name of the service definition that is used to create the service.
- Service Order—Unique identifier assigned by the system to denote the service order.
- Service Type—Selected service type, such as P2P, L3VPN, or VPLS
- State—State of the selected service. Possible values are:



NOTE: These states apply only for a service and not a service order

- Active—Denotes a service that has been deployed and is in an active state (enabled).
- Inactive—Denotes a service that has been deployed and is in a deactivated state (disabled).
- Pending—Denotes a service for which deployment of the service to a device is pending to be performed.
- Deploy—An attempt to modify the service failed.
- State—State of the selected service order. Possible values are:



NOTE: These states apply only for a service order and not a service.

- Completed—Service order has been successfully deployed.
- Deploy failed—Device is down or the Connectivity Services Director application was unable to push the service configuration to a device configured for the service.
- In-progress—Connectivity Services Director application is in the process of deploying the service.
- Requested—Service provisioner has created the service order, but has not yet attempted to deploy it or schedule it for deployment.
- Scheduled—Service provisioner has scheduled the service order for deployment.

- Invalid—Service order contains invalid data.
- Validated—When all the information in the service order is successfully validated, the service order transitions to the Validated state.
- Last Updated Date—Date and time at which the service was last modified.
- Functional Audit Status—Status of the functional audit for the selected service
- Configuration Audit Status—Status of the configuration audit for the selected service
- Fault Status—Fault status of the audit performed for the selected service
- SLA Status—SLA status of the audit performed for the selected service.

Advanced Details

This section displays the advanced, fine-grained connectivity settings between sites, such as the configured route distinguisher, VRF route label. The parameters displayed under this section are similar to the advanced parameters displayed in the wizard for service order creation.

Endpoint Details

A tabular view is displayed of the configured device and UNI Details that are part for the service. Each row in the table displays the basic, salient parameters, such as Device Name, Interface Name, Unit ID, Encapsulation and Description. You can use the paging controls to navigate across multiple pages of endpoints as necessary. A minimum of 20 endpoints per page are displayed.

The following fields are displayed in the End Points table:

- End Point—Name of the device configured as the source or origin (A) endpoint and the destination or target (Z) endpoint. This field is displayed for point-to-point services. Click the plus sign beside the device name for P2P services to expand the device-related parameters and view the detailed settings.
- Device Name—Name of the device for which the service is created. Click the plus sign beside the device name for VPLS and L3VPN services to expand the device-related parameters and view the detailed settings.
- Interface—Name of the physical interface associated with the service.
- Tagging—Type of packet tagging for the interface, such as Ethernet, dot1Q, or Q-in-Q.
- UnitId—Logical unit identifier of the interface.
- VlanId—VLAN identifier of the interface.
- Is Hub—Indicates whether the node is a hub or a spoke.
- Template—Name of the service template that is used to create the service order.
- CoS Profiles—Name of the COS profile associated with the service.

Device Details

Click the plus sign beside the device name shown under the Endpoint (for P2P services) or Device Name (for VPLS or L3VPN services) row of the table. The configured parameters on the device for the service are expanded and displayed after selecting a device in the navigation tree. The parameters to be shown are based on the service type. The parameters displayed under this section are similar to the node parameters and UNI parameters displayed in the wizard for service order creation, such as route distinguisher and MVPN status of the service (shown only for MVPN-enabled L3VPN services)).

Related Documentation

- [Viewing Service Orders on page 801](#)
- [Modifying a Saved Service Order on page 1107](#)
- [Viewing Services on page 807](#)

Viewing Services

The following topic describes how to view services:

- [Viewing Services in a Table on page 807](#)

Viewing Services in a Table

To view the services inventory in a table:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the View pane, click the plus sign (+) to expand the tree and select the type of service.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
5. In the **Network Services > Connectivity** task pane, select **Service Provisioning > Deploy Services**.

In the top half of the window on the right pane, the Manage Network Services page presents information on existing services in a table.

The **Manage Network Services** page provides the following information about each service:

[Table 114 on page 808](#) describes the fields in the service orders table.

Table 114: Fields in the Services Table

Field	Description
Name	Name of the service order assigned during service creation or edit.
Service Type	One of the following: <ul style="list-style-type: none"> Point-to-point pseudowire (LDP) Point-to-point pseudowire (BGP) VPLS (MultiPoint-to-MultiPoint) VPLS (Point-to-MultiPoint) L3VPN (Full Mesh) L3VPN (Hub-Spoke 1 Interface)
Customer	Name of the enterprise customer who placed an order for the service.
Deployment State	State of the service: <ul style="list-style-type: none"> Active—Denotes a service that has been deployed and is in an active state (enabled). Inactive—Denotes a service that has been deployed and is in a deactivated state (disabled). Pending—Denotes a service for which deployment of the service to a device is pending to be performed. Failed—An attempt to modify the service failed.
FA Status	Status of functional audit of the service.
Fault Status	Fault management status of the service.
SLA Status	Service-level agreement status of the service. If data exceeds the threshold value specified in the Threshold Alarm Profile, the system generates a threshold alarm. The value in the SLA Status column changes to SLA Violated. If the data does not cross the threshold value specified in the Threshold Alarm Profile, the value in the SLA Status column changes to SLA Violation Cleared.
PM Status	Performance management status of the service.
Definition	Name of the service definition upon which the service order is based.
Activation Date	Date and time at which the service order was last activated.
Last Modified Time	Date and time at which the profile was last updated.

6. To restrict the display of services, enter a search criterion of one or more characters in the search bar and press Enter. All services that match the search criterion are shown in the main display area.

7. To view details of a specific service, double-click the table row that summarizes the service.

For a VPLS service (point-to-multipoint or multipoint-to-multipoint), a table of service details appears.

8. Select the check box beside a service to launch the Manage Service Orders page in the lower half of the pane. The service orders associated with the selected service are displayed. You can perform different actions, such as validating or discarding configuration.

- See Also**
- [Viewing Service Orders on page 801](#)
 - [Viewing Service Order and Service Details on page 803](#)

- Related Documentation**
- [Understanding Service Validation on page 1063](#)
 - [Managing Jobs on page 118](#)
 - [Deleting a Partial Configuration of an LSP Service Order on page 1014](#)
 - [Deleting a Service Order on page 1015](#)
 - [Deploying a Service on page 1016](#)
 - [Validating the Pending Configuration of a Service Order on page 1018](#)
 - [Viewing the Configuration of a Pending Service Order on page 1020](#)

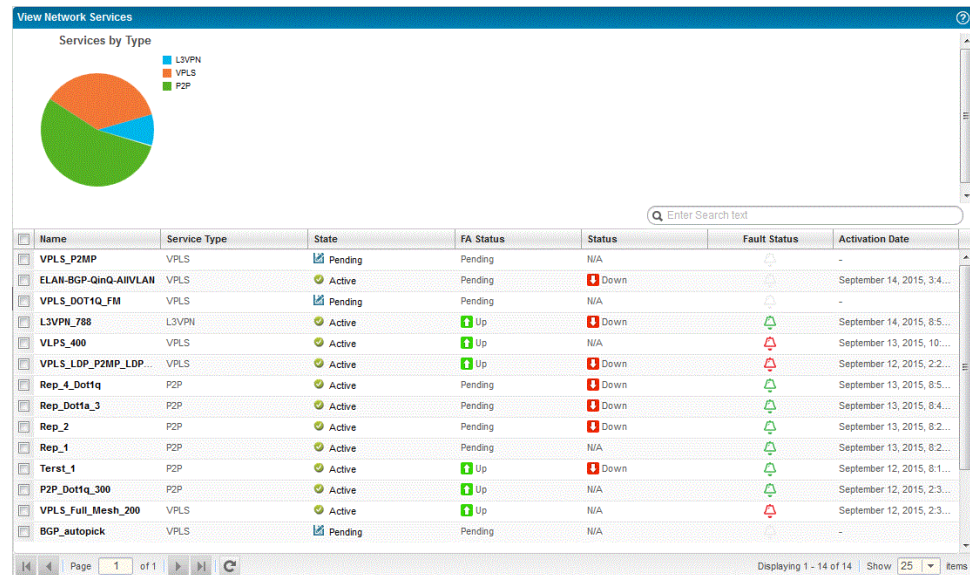
Viewing the Configured Point-to-Point, L3VPN, and VPLS Services

To view the services inventory in a table:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Build** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the View pane, click the plus sign (+) to expand the tree and select the type of service.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
5. With the Connectivity item selected in the View pane, from the **Network Services > Connectivity** task pane, select **Service Provisioning > View Services**.

The View Network Services page is divided into two panes. The top pane provides a pictorial representation of the types of services, statuses of services, and audit-related information.

Figure 40: View Network Services Page



In the View pane, if you select the Connectivity item in the tree under Network Services, without expanding the tree and selecting a specific service type, such as P2P Services, L3VPN Services, or VPLS Services, the top pane displays a set of five pie charts that enable you to view the different service orders configured, and their associated audit and monitoring statuses. The FA Status chart displays the functional audit status for the service orders. The Device State graph displays the statuses of devices on which services are being provisioned and commissioned. The Fault Status chart displays the connectivity fault management details for the service orders. The SLA Status chart displays the service-level agreement details for the service orders. The PM Status chart displays the performance management details for the service orders. The count or percentage of service orders in the pie chart segments sum up to the total number of configured service orders. Mouse over each segment of the pie to view the number corresponding to the percentage of service orders for each of the charts. These charts provide a visual overview of customers and service orders on your network, and enables you to quickly access related and commonly needed information. For example, you can check for failed service orders and then access a list of failed requests so you can begin to take restoration measure.

In the View pane, if you do not expand the Network Services tree, and select the Network Services node in the View pane, the top pane displays a pie chart that enables you to view and examine the different services configured for devices, and the types of service protocols configured. The Services by Type graph displays the count of services for each type of service definition. Mouse over each segment of the pie to view the number of services corresponding to the percentage of service types. This chart provides a visual overview of customers and service orders on your network, and enables you to quickly access related and commonly needed information.

The View Network Services page provides the following information about each service in the bottom pane:

[Table 114 on page 808](#) describes the fields in the View Network Services table.

Table 115: Fields in the Services Table

Field	Description
Name	Name of the service order assigned during service creation or edit.
Service Type	One of the following: <ul style="list-style-type: none"> Point-to-point pseudowire (LDP) Point-to-point pseudowire (BGP) VPLS (MultiPoint-to-MultiPoint) VPLS (Point-to-MultiPoint) L3VPN (Full Mesh) L3VPN (Hub-Spoke 1 Interface)
Customer	Name of the enterprise customer who placed an order for the service.
Deployment State	State of the service: <ul style="list-style-type: none"> Active—Denotes a service that has been deployed and is in an active state (enabled). Inactive—Denotes a service that has been deployed and is in a deactivated state (disabled). Pending—Denotes a service for which deployment of the service to a device is pending to be performed. Failed—An attempt to modify the service failed.
FA Status	Status of functional audit of the service.
Fault Status	Fault management status of the service.
SLA Status	Service-level agreement status of the service. If data exceeds the threshold value specified in the Threshold Alarm Profile, the system generates a threshold alarm. The value in the SLA Status column changes to SLA Violated. If the data does not cross the threshold value specified in the Threshold Alarm Profile, the value in the SLA Status column changes to SLA Violation Cleared.
PM Status	Performance management status of the service.
Definition	Name of the service definition upon which the service order is based.
Activation Date	Date and time at which the service order was last activated.
Last Modified Time	Date and time at which the profile was last updated.

6. To restrict the display of services, enter a search criterion of one or more characters in the search bar and press Enter. All services that match the search criterion are shown in the main display area.
7. To view details of a specific service, double-click the table row that summarizes the service.

For a VPLS service (point-to-multipoint or multipoint-to-multipoint), a table of service details appears.

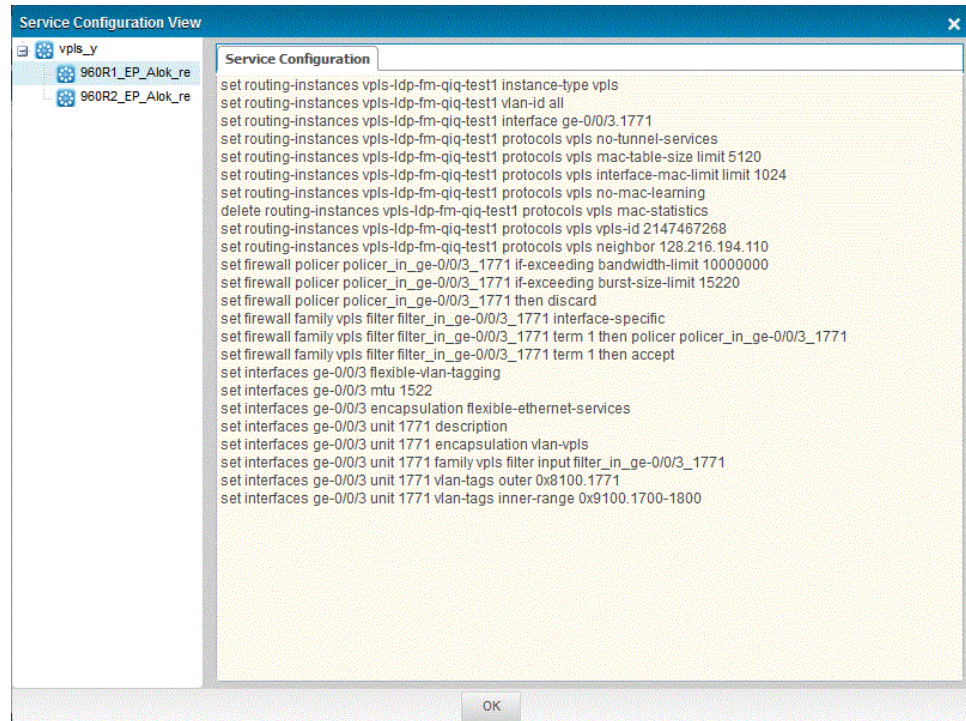
- Related Documentation**
- [Viewing Service Orders on page 801](#)
 - [Viewing Service Order and Service Details on page 803](#)

Viewing the Configuration Details of VPN Services

You can view the configuration of a point-to-point, L3VPN, or a VPLS service, which enables you to see the parameters and attributes configured for a service on the associated devices in the form of configuration statements and commands that are displayed in the Junos OS CLI interface. You can use these settings to examine the existing service configuration and modify it as necessary to correct any traffic-handling problems or system discrepancies.

To view the configuration of services:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
4. From the **Network Services > Connectivity** task pane, select **Service Provisioning > Deploy Services**. The Manage Network Services page is displayed on the top part of the right pane.
5. Select the check box next to a service for which you want to view the configuration details.
6. Click the **View Configuration** option. The Service Configuration View dialog box is displayed. The configuration is displayed in the CLI interface structure and in the form of configuration stanzas.



The left pane displays a tree of devices associated with the specified service. You can select a Service-name > Device-name in the left pane of the window to view the configuration parameters of the corresponding device on the right pane. The right pane contains two tabs— Service Configuration and Template Configuration. The Service Configuration tab displays the settings specified for the service on the device in CLI format. This tab displays the elements or components specified for a service template in the form of configuration stanzas and hierarchy levels. This display is similar to the show command that you can use at a certain [edit] hierarchy level to view the defined settings. The Template Configuration tab displays the service attributes and options defined in the service template, if any, that is associated with the service.

7. Click **OK** to close the dialog box after you complete viewing the configuration attributes and settings.

Related Documentation

- [Deleting a Partial Configuration of an LSP Service Order on page 1014](#)
- [Deleting a Service Order on page 1015](#)
- [Deploying a Service on page 1016](#)
- [Validating the Pending Configuration of a Service Order on page 1018](#)

CHAPTER 33

Service Provisioning: Managing Point-to-Point Service Orders

- [Creating a Service Order on page 815](#)
- [Creating a Point-to-Point ATM or TDM Pseudowire Service Order on page 816](#)
- [Creating a Point-to-Point Service Order on page 829](#)
- [Creating a Bulk-Provisioning Service Order for Pseudowire Services on page 845](#)
- [Creating an Inverse Multiplexing for ATM Service Order on page 849](#)
- [Provisioning a Single-Ended Point-to-Point Service on page 853](#)
- [Selecting Specific LSPs for Connectivity Services on page 855](#)
- [Stitching Two Point-to-Point Pseudowires on page 858](#)
- [Deactivating a Service on page 860](#)
- [Reactivating a Service on page 862](#)
- [Force-Deploying a Service on page 864](#)
- [Recovering a Service Definition through Force Upload on page 867](#)
- [Decommissioning a Service on page 868](#)
- [Viewing Alarms for a Service on page 871](#)
- [Inline Editing of VPLS and Layer 3 VPN Service Orders on page 872](#)
- [Interconnecting a Layer 3 VPN Service with a VPLS Service on page 876](#)
- [Changing the Logical Loopback Interface for Provisioning on page 878](#)

Creating a Service Order

A service order is an instance of the service definition that completes the definition for a specific customer's use. The service order always specifies the customer and the endpoints that link the customer sites through the MPLS network. For each endpoint, the service provisioner specifies the N-PE device and the UNI on that device that connects the customer site to the N-PE device. The service order can also specify any additional attributes that are configured in the service definition as editable in the service order. These attributes might include the VCID, MTU for the UNI, MTU for the connection across the network, VLAN-ID, rate limiting bandwidth, and so forth.

To create a point-to-point Ethernet service order, see [“Creating a Point-to-Point Service Order” on page 829](#)

To create a VPLS service order, see [“Creating a Multipoint-to-Multipoint VPLS Service Order” on page 881](#) or [“Creating a Point-to-Multipoint VPLS Service Order” on page 905](#).

Creating a Point-to-Point ATM or TDM Pseudowire Service Order

To create a point-to-point Ethernet service order, complete the following tasks in order:

1. [Selecting the Service Definition on page 816](#)
2. [Entering General/Connectivity Settings Information on page 818](#)
3. [Specifying Endpoint Information on page 820](#)
4. [Specifying Template Settings on page 826](#)
5. [Reviewing the Configured Settings on page 828](#)
6. [Deploying the New Service on page 828](#)

Selecting the Service Definition

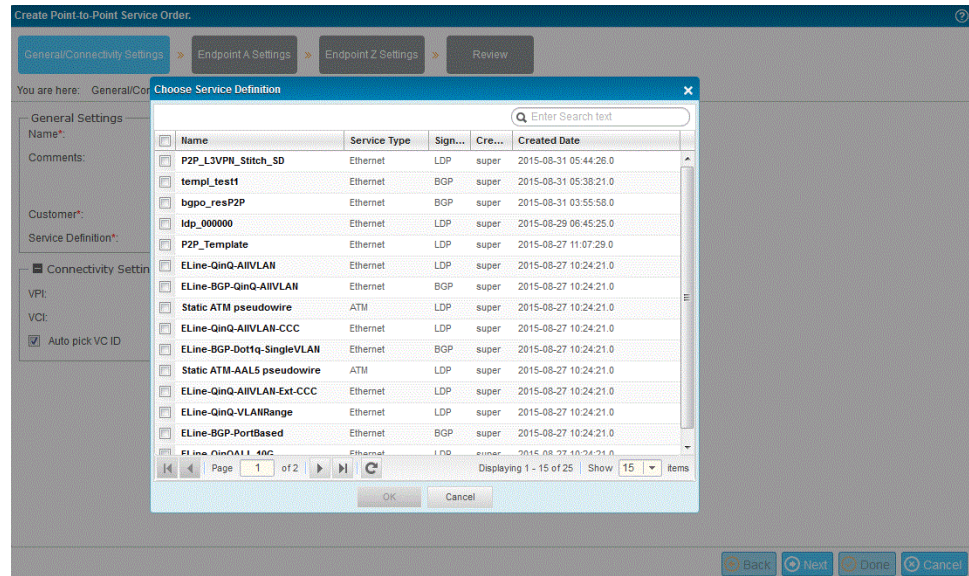
To select a service definition on which to base the new service order:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the View pane, click the plus sign (+) to expand the tree and select the type of service.
4. From the Tasks pane, select **Service Provisioning > Deploy Services**.

The Manage Network Services page is displayed in the top half of the right pane, which displays all of the configured services. The Manage Service Orders page is displayed in the bottom half of the right pane, which displays all of the service orders corresponding to a service.

From the **Manage Network Services** page, select **New > P2P Service Order**.

The **Create P2P Service Order** page displays an inventory of all available point-to-point service definitions.



The **General/Connectivity Settings** panel appears initially in the right panel, as shown in the example.



NOTE: In the service order creation wizard for point-to-point services, the search function has been enhanced to enable you to easily sort and filter the parameters that are of interest and relevance for the services you want to configure. The Choose Customer dialog box that is displayed when you click **Select** beside the Customer field contains the Search box, which enables you to perform a search on all of the columns. The search utility that is present in the Choose Service Definition dialog box that is displayed when you click **Select** beside the Service Definition field enables you to search by Name, Created by, and Signaling columns; search utility is not supported for other columns in the dialog box. The search box that is present in the Choose Endpoints dialog box when you click **Select** beside the PE Device and UNI Interface fields enables search across all the columns displayed in the dialog box. For any string-based search (which shows strings that match any part of the text you enter in the search box), only the Name, Platform, and OS Version columns are supported. For exact string-based search (which shows strings that exactly match the text you enter in the search box), the IPAddress, State, and Manage State columns are supported.

- From the Service Definition field, click **Select** to choose the service definition you want to base your service order on. The Choose Service Definition inventory page displays a view of only those published service definitions designed to work with the type of services you need.

Based on the fields or parameters that you defined in the service definition to be enabled for modification in the service order, the corresponding fields are available

for editing. The fields that are disabled for modification in the service order can only be edited in the service definition.

6. Select the check box beside the service definition that you want to associate with the service order, and click **OK**.
7. Click **View** to open a popup dialog box that displays the details of the selected service definition. The service definition properties, such as the name, signaling type (LDP or BGP), service type (point-to-point pseudowire, ATM, or TDM), are displayed. The interface-specific attributes, such as rate-limiting details, encapsulation, and VLAN tags, are also displayed in the dialog box. Close the dialog box to return to the service order creation wizard.

If a template is attached to the service definition on which the service order is based, you can invoke the template editor from the Template page of the wizard.

Entering General/Connectivity Settings Information

The **General Settings** panel is displayed on the right side of the service order window.

The screenshot shows the 'Create Point-to-Point Service Order' wizard. The top navigation bar includes 'General/Connectivity Settings' (active), 'Endpoint A Settings', 'Endpoint Z Settings', and 'Review'. Below the navigation bar, a breadcrumb trail reads 'You are here: General/Connectivity Settings'. The main panel is divided into two sections: 'General Settings' and 'Connectivity Settings'.

General Settings:

- Name*:** P2P_ATM_SO
- Comments:** (Empty text area)
- Customer*:** (Empty text field with 'Select' and 'Clear' buttons)
- Service Definition*:** ATM pseudowire (with 'Select' and 'View' buttons)

Connectivity Settings:

- VPt:** (Dropdown menu)
- VCt:** (Dropdown menu)
- ☒ Auto pick VC ID

At the bottom right of the wizard, there are four buttons: 'Back', 'Next', 'Done', and 'Cancel'.

To configure general settings in the **General Settings/Connectivity Settings** panel, provide the following information:

1. In the **Name** box, enter a unique name for the service.

The service order name can consist of only letters, numbers, and underscores.



NOTE: The name you specify for a service order becomes the routing-instance name in the device configuration when you deploy the service. Consequently, you cannot use any Juniper Networks keywords, for example, “bgp” or “vpls”, as the name of a service order.

2. In the **Customer** box, select the customer requesting the service.

If the customer is not in the list, you must add the customer to the database before proceeding. See [“Adding a New Customer” on page 737](#).

3. In the **Description** box, enter a description of the service. This description appears in information windows about the request or service instance created from the request.

4. In the **Connectivity Settings** box, specify the MTU for the connection across the network.

The service definition can constrain the MTU to a specific value or allow the service provisioner to override it in the service order. In this example, the service definition sets the MTU, but allows the service provisioner to change the value.

When you advance to the next step in creating your service order, your new connectivity settings appear under the Connectivity image in the main graphic and new general information is added to the text above the cloud. If you have incomplete or invalid information in the **General/Connectivity Settings** panel, a warning icon appears next to the cloud image.

5. Specify the virtual path identifier (VPI). This field is available only if you have selected an ATM point-to-point service definition.

The combination of the VPI and VCID defines the next destination for a cell in the ATM network.

Range: 0 through 255

6. Specify the virtual channel identifier (VCI). This field is available only if you have selected an ATM point-to-point service definition.

Range: 0 through 65535

7. Enter the virtual circuit identifier (VCID). This integer uniquely identifies the virtual circuit that the service uses.

The VCID can be set either automatically by the Junos Space software, or the service provisioner can set it manually in the service order. The service definition can force the system to pick the VCID, force the service provisioner to pick the VCID, or allow the service provisioner to override the settings in the service definition.

We recommend allocating the VCID automatically; however, service providers with their own systems for allocating VCIDs can choose the manual setting.

By default, the system picks a VCID from its pool automatically, but allows the service provisioner to override this value in the service order. The form expands to include an additional field for typing the VCID manually.

This field is displayed only if the selected definition's signaling type is **LDP**. You cannot edit this field if you have not selected the **Editable in Service Order** in the service definition.

8. Select the **MC APS** check box to add the **run show aps extensive** command.



NOTE: This check box is available only in an LDP-based point-to-point service order with PW Resiliency enabled. The **Interface type** must be ATM/TDM.

For more information on MC-APS, see [“Multi-Chassis Automatic Protection Switching Overview” on page 99](#).

9. Enter the **Route Distinguisher** value.

Range: 1.1.1.1 through 255.255.255.254:65535, or 1:1 through 65535:4294967295

This field is displayed only if the selected definition's signaling type is **BGP**. You cannot edit this field if you have not selected the **Editable in Service Order** in the service definition.

10. Specify the **Route Target**.

1. Clear the **Auto pick Route Target** check box.
2. Enter the **Route Target** value.

Range: 1.1.1.1 through 255.255.255.254:65535, or 1:1 through 65535:4294967295

This field is displayed only if the selected definition's signaling type is **BGP**. You cannot edit this field if you have not selected the **Editable in Service Order** in the service definition.

11. Provide endpoint information for the first endpoint: click the **Endpoint A** graphic element or click **Next**.

The **Endpoint Settings** form appears in the right panel.

Specifying Endpoint Information

On M Series, MX Series, and ACX routers:

- The ATM interfaces always appear as an AT interface.

- The TDM interfaces with SAToP encapsulation always appear as a T1 interface; TDM interfaces with CESoPSN encapsulation always appear as a DS interfaces.

To configure the endpoint settings:

Create Point-to-Point Service Order. ⓘ

Select Service Definition > General/Connectivity Settings > **Endpoint A Settings** > Endpoint Z Settings > Review

You are here: Endpoint A Settings

Endpoint: A

PE Device*: A116 Select Clear

UNI Interface*: ge-0/0/3 Select Clear

UNI Description:

Physical IF encapsulation: atm-ccc-cell-relay

Cell Bundle Size: 1

LSP Name: Select LSP Tunnel

Back Next Done Cancel

1. In the **PE Device** box, select the N-PE device you want to use for the first endpoint. From the Choose Endpoints dialog box that appears, select the devices that you want to participate in the service. Use the multiple selection feature to select one or more devices. The lower part of the dialog box refreshes to display the interfaces associated with the selected device. Select the check boxes next to the interfaces you want to associate with the service order.

Name	IP Address	State	Managed State	Platform	OS Version	Roles
<input checked="" type="checkbox"/> 960R2_EP_Alok_re	10.216.194.110	up	In Sync	MX960	14.2-20140916.0	N_PE
<input type="checkbox"/> 480R4_EP_Alok_re	10.216.194.105	up	In Sync	MX480	14.2-20140916.0	N_PE
<input type="checkbox"/> 480R3_EP_Alok_re	10.216.194.108	up	In Sync	MX480	14.2-20140916.0	N_PE
<input type="checkbox"/> 960R1_EP_Alok_re	10.216.194.118	up	In Sync	MX960	14.2-20140916.0	N_PE
<input type="checkbox"/> RouterZ-re	10.92.35.185	down	In Sync	MX960	15.1-20141022_1...	N_PE
<input type="checkbox"/> RouterY-re	10.92.35.187	up	In Sync	MX960	15.1-20141022_1...	N_PE
<input type="checkbox"/> RouterX-re	10.92.35.189	up	In Sync	MX960	15.1-20141022_1...	N_PE
<input type="checkbox"/> RouterXCore-re	10.92.35.183	down	In Sync	MX960	15.1-20141022_1...	-
<input type="checkbox"/> Merg1_006_re	10.92.37.13	up	In Sync	MX960	15.1-20150727_...	N_PE

Page 1 of 3 Displaying 1 - 9 of 25 Show 9 items

Name	Status	Encapsulation	Index
<input type="checkbox"/> ae0	down	none	508
<input type="checkbox"/> ae1	down	none	509
<input type="checkbox"/> em1	up	none	23
<input type="checkbox"/> em2	up	none	116
<input type="checkbox"/> ge-0/0/2	up	flexible-ethernet-services	533
<input type="checkbox"/> ge-0/0/3	up	flexible-ethernet-services	539
<input type="checkbox"/> ge-0/0/4	up	flexible-ethernet-services	542
<input type="checkbox"/> ge-0/0/5	up	none	550
<input type="checkbox"/> ge-0/0/6	up	none	551
<input type="checkbox"/> ge-0/0/7	up	none	552
<input type="checkbox"/> ge-0/0/8	up	none	553
<input type="checkbox"/> ge-0/0/9	up	none	554



NOTE: In the Choose Endpoints dialog box, you can sort and segregate the devices and their corresponding interfaces based on the roles of the devices to easily and quickly view only the devices of interest. Click the down arrow on the Filter Role menu, and select P2E to view only the provider edge devices, P to view only the provider devices, and L2E to view only Layer 2 Ethernet devices.

If you are unsure about which PE device to choose, go to the Prestaging Devices workspace landing page, which shows capacity information about UNIs on PE devices. You must pick a device that has available UNIs.

This step is required for all service orders.

2. In the **UNI interface** box, select a UNI. The list includes all UNIs available on the selected device.

You can enter the description of the UNI interface in the **UNI description** field.

If you have selected the **Enable Multi Segment Pseudowire** check box in the service definition, the **UNI interface** of the second endpoint lists the interworking (iw) interfaces only.

For more information on point-to-point pseudowire stitching, see [“Stitching Two Point-to-Point Pseudowires” on page 858](#).

This step is required for all service orders.

You cannot change the type of **Physical IF encapsulation**. This value is set in the service definition.

Based on the type of **Physical IF encapsulation**, the corresponding fields are displayed. For example, if the **Physical IF encapsulation** is CESoPSN, the following fields are displayed:

- Jitter buffer
- Idle pattern
- Excessive packet loss rate



NOTE: These fields are editable if you have selected the **Editable in Service Order** check box in the service definition.

3. Specify the stitching unit.

Default: 0

Range: 0 through 255



NOTE: This field is displayed only in the second endpoint. You must have selected the **Enable Multi Segment Pseudowire** check box in the service definition.

4. If the **Physical IF encapsulation** type is CESoPSN, specify the **Packetization Latency**. Packetization latency is the time required to create packets.

Range: 1000 through 8000 microseconds



NOTE: Based on the number of time slots, the default Packetization Latency value is as follows:

- If the number of time slots is equal to 1, the default value is either 5000 microseconds or 8000 microseconds.
- If the number of time slots is 2, 3, or 4, the default value is 4000 microseconds.
- If the number of time slots is greater than 4, the default value is 1000 microseconds.

5. In the **LSP tunnel name** box, select the LSP tunnel you want to use for this device.

You must supply an LSP tunnel name for the interface on BX devices. If one is not defined, you must first use the Transport Activate application to create an LSP on the BX7000 Gateway.

On the M Series router, the LSP tunnel is chosen automatically.

This field is displayed only if the selected definition's signaling type is **LDP**.

6. Specify the cell bundle size. The value of the cell bundle size can be from 1 through 34.
7. If you have enabled the **Enable PW Resiliency** check box in the selected service definition, fill in the following fields in the Backup settings and Resiliency settings:

- **Enable**
- **PE device**
- **UNI interface**
- **MTU (Bytes)**
- **LSP tunnel name**
- **Revert time (sec)**
- **Switch Over Delay (sec)**

For more information of pseudowire redundancy, see [“Redundant Pseudowires for Layer 2 Circuits and VPLS” on page 94](#).

8. If you selected the **Static pseudowire** check box in the selected service definition, you need to specify the **Outgoing label** for the static pseudowire.

Range: 1000000 through 1048575

In case of multi-segment pseudowire, you have to specify a new outgoing label for the second segment. The outgoing label for the second segment is not prepopulated from the first segment.



NOTE: You must manually compare the encapsulation, TDM bit rate, and control word of the router with the remote peer router and ensure that these parameters match; otherwise the static pseudowire might not work.

9. Select the **Enable send-oam config** check box to enable the **send-oam** command. You can select or clear this check box even in the Modify Service page.
10. Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

The service order that you have created is listed in the Manage Service Orders page.

Specifying Template Settings

The Template Settings page of the service order creation and modification wizards enables you to associate service templates with a point-to-point, VPLS, and Layer 3 VPN service order. You can apply only the templates that are previously configured in a service definition with the corresponding service order. The Template Settings page is available in the service order wizard only if the service definition that you selected to apply to the service order contains a service template. Otherwise, the Template Settings page is not displayed in the service order wizard. You can perform template operations for all endpoints in a service order.

If you defined a service template as the default service template, it is attached to the endpoint by default. You have the flexibility to create and provision a dynamic attribute

in a service template. You can mark an attribute of a service template as dynamic, and you can obtain the values for these dynamic attributes from a specific device. To create a dynamic attribute, you must first mark an attribute of a service template as dynamic and then specify the device XPath for the dynamic attribute.

The Template Settings page is displayed before the Review page, which is the final step of the service order wizard.

In the Service Settings page, from the Select Service Definition field of the service order creation wizard, you can double-click a service definition name displayed in the table to view the details of the definition in a popup dialog box. You can use this information to determine if the service definition is appropriate for your deployment needs. To filter and sort the display of service templates, enter the name of the template as a match criterion in the Search box and click the Search icon. The page refreshes to display only the template names that match with the search term. You can use the paging controls to navigate across multiple pages of templates as necessary.

All the tasks that you can perform with service templates are presented in the Template Settings page. The page is divided into three panes. The top half of the page displays a table of selected endpoints. All the endpoints or UNIs that you selected in the preceding pages of the service order wizard are displayed in this table. You can configure the template pertaining to only one endpoint at a point in time. If the selected endpoints (in previous pages of the wizard) contained a manually-entered unit number, that number is displayed in the table of selected endpoints. Otherwise, the Auto-pick label is displayed.

The lower half of the page is divided into two panes. The left pane displays the template selection table for the endpoint you selected. All the templates associated with the service definition are displayed. You can add and delete templates using the template selection table. The right pane displays all the parameters that you can modify for a selected service template. All such editable parameters are displayed in a consolidated form of a configuration page. This pane is displayed after you select a template. If any configuration parameter in template is set as a service-specific value, such attributes are not displayed in this pane.

To associate a service template with a service order:

1. Click **Add** to include a service template for the endpoint. A dialog box is displayed with the list of service templates associated with the service definition that is used to create the service order. The templates selected in this dialog box are displayed in the Template Selection table for the specified endpoint. Such templates are considered to be attached to that endpoint.

If you specified a template as a default template during the service definition creation, the template is displayed by default in the template selection table. You can associate non-default templates with the service order by clicking the **Add** button.

2. Click the link in the template name to open the Template Details dialog box. The template settings are displayed in the popup dialog box. For the selected template, the Configuration Page is displayed in the lower-right pane of the Template Settings page.

3. Modify any template-specific service components as necessary.
4. Click **Save** to submit the changes.
5. Select a template from the Template Selection table, and click Delete to remove the template from being associated with the service order for a particular endpoint.

Reviewing the Configured Settings

The Review page of the service definition or service order creation and modification wizards enable you to view and evaluate the service parameters and components you configured in preceding steps or pages of the wizard. This page provides a comprehensive, single-page view of all the service elements configured in the different pages of the wizard. You can either click the buttons corresponding to the various settings at the top of the wizard page to directly traverse to the page you want to modify or click the navigation buttons at the bottom of the wizard page to go to the different pages of the wizard.



NOTE: On the Review page, in the Service Templates section, the names of the service templates with which the service definition is associated are displayed. The Default Service Template column indicates whether the attached template is the default template.

1. Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify.
2. Click **Edit** next to the section that contains the parameter you want to modify. You are navigated to the corresponding page of the wizard in which the parameter settings are defined.
3. Click **Finish** to save the service definition or service order.
4. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

The service order inventory window appears.

Deploying the New Service

To deploy the new service:

1. Perform one of the following actions from the Deploy mode of the Service View of Connectivity Services Director:
 - To deploy the service immediately, select **Deploy now**, then click **OK**.

- To deploy the service later, select **Schedule deployment**, select a date and time, then click **OK**.

The time field specifies the time kept by the server, but in the time zone of the client.

2. To monitor the progress and status of the deployment, use the Jobs workspace.

**Related
Documentation**

- [Creating a Service Order on page 815](#)
- [Creating a Point-to-Point Service Order on page 829](#)
- [Cloning Deployed Point-to-Point Services](#)
- [Creating a Bulk-Provisioning Service Order for Pseudowire Services on page 845](#)
- [Creating an Inverse Multiplexing for ATM Service Order on page 849](#)
- [Provisioning a Single-Ended Point-to-Point Service on page 853](#)
- [Selecting Specific LSPs for Connectivity Services on page 855](#)

Creating a Point-to-Point Service Order

To create a point-to-point service order, complete the following tasks in order:

1. [Selecting the Service Type on page 830](#)
2. [Entering General Settings Information on page 832](#)
3. [Specifying the Connectivity on page 833](#)
4. [Specifying QoS Settings on page 835](#)
5. [Specifying OAM Settings on page 835](#)
6. [Specifying Endpoint Information on page 836](#)
7. [Specifying Template Settings on page 841](#)
8. [Reviewing the Configured Settings on page 843](#)
9. [Specifying Connectivity and Endpoint Information for Managing VLANs on page 844](#)
10. [Deploying and Monitoring the Progress of the New Service on page 844](#)

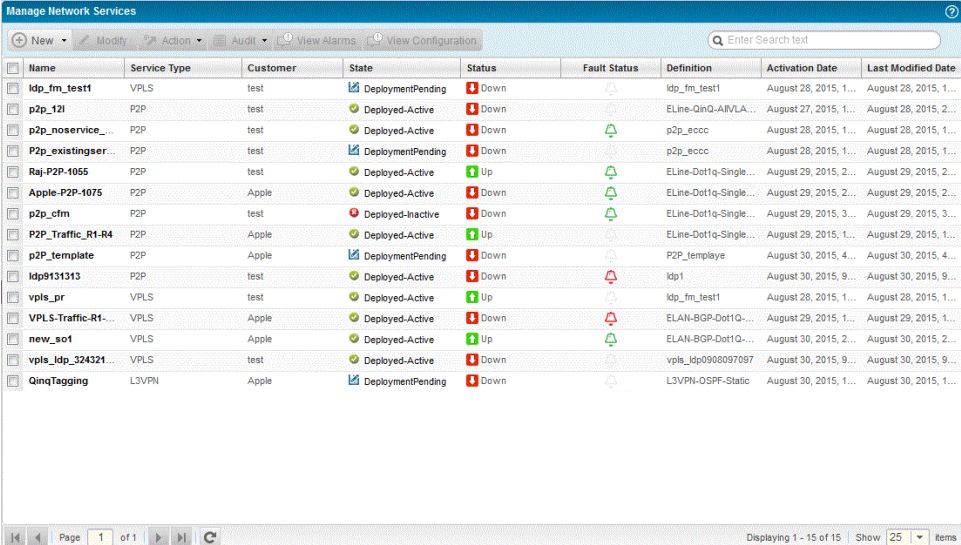
Selecting the Service Type

A wizard is available to create a service order in an intuitive and easily-navigable format. The settings that you can configure in the service order are organized in separate pages of the wizard, which you can launch by clicking the appropriate buttons at the top of the Create a Service Order page. Alternatively, you can proceed to the corresponding setting-related pages by clicking the **Back** and **Next** buttons at any point in the wizard during the creation of the service order.

To select the service type as point-to-point to base the new service order:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the View pane, click the plus sign (+) to expand the tree and select the type of service.
4. From the Tasks pane, select **Service Provisioning > Deploy Services**.

The Manage Network Services page is displayed in the top half of the right pane, which displays all of the configured services. The Manage Service Orders page is displayed in the bottom half of the right pane, which displays all of the service orders corresponding to a service.



Name	Service Type	Customer	State	Status	Fault Status	Definition	Activation Date	Last Modified Date
ldp_fm_test1	VPLS	test	DeploymentPending	Down		ldp_fm_test1	August 28, 2015, 1...	August 28, 2015, 1...
p2p_121	P2P	test	Deployed-Active	Down		ELINE-QinQ-AIRLA...	August 27, 2015, 1...	August 28, 2015, 2...
p2p_noservice...	P2P	test	Deployed-Active	Down		p2p_eccc	August 28, 2015, 1...	August 28, 2015, 1...
p2p_existingser...	P2P	test	DeploymentPending	Down		p2p_eccc	August 28, 2015, 1...	August 28, 2015, 1...
Raj-P2P-1055	P2P	test	Deployed-Active	Up		ELINE-Dot1q-Single...	August 29, 2015, 2...	August 29, 2015, 2...
Apple-P2P-1075	P2P	Apple	Deployed-Active	Down		ELINE-Dot1q-Single...	August 29, 2015, 2...	August 29, 2015, 2...
p2p_cfm	P2P	test	Deployed-Inactive	Down		ELINE-Dot1q-Single...	August 29, 2015, 3...	August 29, 2015, 3...
P2P_Traffic_R1-R4	P2P	Apple	Deployed-Active	Up		ELINE-Dot1q-Single...	August 29, 2015, 1...	August 29, 2015, 1...
p2p_template	P2P	Apple	DeploymentPending	Down		P2P_Template	August 30, 2015, 4...	August 30, 2015, 4...
ldp9131313	P2P	test	Deployed-Active	Down		ldp1	August 30, 2015, 9...	August 30, 2015, 9...
vpls_pr	VPLS	test	Deployed-Active	Up		ldp_fm_test1	August 28, 2015, 1...	August 28, 2015, 1...
VPLS-Traffic-R1...	VPLS	Apple	Deployed-Active	Down		ELAN-BGP-Dot1Q...	August 29, 2015, 1...	August 29, 2015, 1...
new_so1	VPLS	Apple	Deployed-Active	Up		ELAN-BGP-Dot1Q...	August 30, 2015, 2...	August 30, 2015, 2...
vpls_ldp_324321...	VPLS	test	Deployed-Active	Down		vpls_ldp0908097097	August 30, 2015, 9...	August 30, 2015, 9...
QinQTagging	L3VPN	Apple	DeploymentPending	Down		L3VPN-OSPF-Static	August 30, 2015, 1...	August 30, 2015, 1...

5. From the **Manage Network Services** page, click the **New** icon at the top of the lower half of the page that displays previously created service orders. The Select Service Type dialog box appears.
6. Select **Point-to-Point** to create a point-to-point service order.

The General/Connectivity Settings panel appears initially in the right panel, as shown in the example.



NOTE: In the service order creation wizard for point-to-point services, the search function has been enhanced to enable you to easily sort and filter the parameters that are of interest and relevance for the services you want to configure. The Choose Customer dialog box that is displayed when you click Select beside the Customer field contains the Search box, which enables you to perform a search on all of the columns. The search utility that is present in the Choose Service Definition dialog box that is displayed when you click Select beside the Service Definition field enables you to search by Name, Created by, and Signaling columns; search utility is not supported for other columns in the dialog box. The search box that is present in the Choose Endpoints dialog box when you click Select beside the PE Device and UNI Interface fields enables search across all the columns displayed in the dialog box. For any string-based search (which shows strings that match any part of the text you enter in the search box), only the Name, Platform, and OS Version columns are supported. For exact string-based search (which shows strings that exactly match the text you enter in the search box), the IPAddress, State, and Manage State columns are supported.

Entering General Settings Information

To enter general parameters related to a service order in the **General Settings** box of the General/Connectivity Settings page of the wizard:

The screenshot shows the 'Create Point-to-Point Service Order' wizard. The 'General/Connectivity Settings' tab is active. The 'General Settings' section includes fields for 'Name*' (containing 'P2P_SO'), 'Comments', 'Customer*' (containing 'Amazon'), and 'Service Definition*' (containing 'P2P_Template'). There are 'Select' and 'Clear' buttons for the Customer field, and 'Select' and 'View' buttons for the Service Definition field. The 'Connectivity Settings' section has a checked 'Auto pick VC ID' checkbox, an 'MTU' field (containing '1522'), and a 'VLAN normalization' dropdown (set to 'Normalize to None'). The 'CFM Settings' section has an 'OAM Profile' dropdown (set to 'Please select...') and a 'View' button. At the bottom right are 'Back', 'Next', 'Done', and 'Cancel' buttons.

1. In the **Name** field, enter a unique name for the service.

The service order name can consist of only letters, numbers, and underscores.



NOTE: The name you specify for a point-to-point service order becomes the routing-instance name in the device configuration when you deploy the service. Consequently, you cannot use any Juniper Networks keywords, for example, “bgp” or “vpls”, as the name of a service order.

2. From the Service Definition field, click **Select** to choose the service definition you want to base your service order on. The Choose Service Definition inventory page displays a view of only those published service definitions designed to work with the type of services you need.

Based on the fields or parameters that you defined in the service definition to be enabled for modification in the service order, the corresponding fields are available for editing. The fields that are disabled for modification in the service order can only be edited in the service definition.

3. Select the check box beside the service definition that you want to associate with the service order, and click **OK**.
4. Click **View** to open a popup dialog box that displays the details of the selected service definition. The service definition properties, such as the name, signaling type (LDP or

BGP), service type (point-to-point pseudowire, ATM, or TDM), are displayed. The interface-specific attributes, such as rate-limiting details, encapsulation, and VLAN tags, are also displayed in the dialog box. Close the dialog box to return to the service order creation wizard.

If a template is attached to the service definition on which the service order is based, you can invoke the template editor from the Template page of the wizard.

5. In the **Customer** field, select the customer requesting the service.

If the customer is not in the list, you must add the customer to the database before proceeding. See [“Adding a New Customer” on page 737](#).

6. In the **Description** field, enter a description of the service that you want to appear in the request or in a service instance created from the request.

This description is displayed in the Manage Service Order page.

7. Configure connectivity settings. See [“Specifying the Connectivity” on page 833](#).

Specifying the Connectivity

In the **Connectivity Settings** box of the General/Connectivity Settings page of the wizard, specify VCID and MTU information.

1. Specify the VCID. This is an integer that uniquely identifies the virtual circuit that the service will use.

The VCID can be either set automatically by the Junos Space software, or it can be set manually by the service provisioner in the service order. The service definition can force the system to pick the VCID, force the service provisioner to pick the VCID, or allow the service provisioner to override the settings in the service definition.

This field is displayed only if the selected definition's signaling type is **LDP**. You cannot edit this field if you have not selected **Editable in Service Order** in the service definition.

We recommend allocating the VCID automatically; however, service providers with their own systems for allocating VCIDs can choose the manual setting.

In the previous example, by default, the system picks a VCID from its pool automatically, but allows the service provisioner to override this value in the service order. Clear the check box to override the service definition setting. The form expands to include an additional field for entering the VCID manually.

2. Specify the MTU for the connection across the network.

The service definition can constrain the MTU to a specific value or allow the service provisioner to override it in the service order. In this example, the service definition sets the MTU, but allows the service provisioner to change the value.

When you advance to the next step in creating your service order, your new connectivity settings appear under the Connectivity image in the main graphic and new general information is added to the text above the cloud. If you have incomplete or invalid

information in the General/Connectivity Settings panel, a warning icon appears next to the cloud image.

3. Select the **Enable MC LAG** check box if you want the following configuration to be pushed to the selected endpoint.

```
set protocols l2circuit neighbor x.x.x.x interface interface name
pseudowire-status-tlv
```



NOTE: This check box is available only for an LDP-based point-to-point service order with PW Resiliency enabled. The Interface type must be Ethernet.

4. Specify the **Route Distinguisher** value.

Range: 1.1.1.1 through 255.255.255.254:65535, or 1:1 through 65535:4294967295

This field is displayed only if the selected definition's signaling type is **BGP**. You cannot edit this field if you have not selected the **Editable in Service Order** check box in the service definition.

5. To specify the **Route Target**, clear the **Auto pick Route Target** check box.

Range: 1.1.1.1 through 255.255.255.254:65535, or 1:1 through 65535:4294967295

This field is displayed only if the selected definition's signaling type is **BGP**. You cannot edit this field if you have not selected the **Editable in Service Order** check box in the service definition.

6. The **VLAN normalization** displays the information based on the option you have selected in the service definition.

7. If **VLAN normalization** is *Normalize to Dot1q tag*, specify the **VLAN Tag to stack**.

Default: 1

Range: 1 through 4094

8. If **VLAN normalization** is *Normalize to QinQ tags*, specify the **Normalize – Outer VLAN Tag** and **Normalize – Inner VLAN Tag** fields.

Default: 1

Range: 1 through 4094

9. To provide endpoint information for the first endpoint, click the **Endpoint A** button or click **Next**.

The Endpoint Settings form appears.

10. If you have enabled QoS, configure QoS settings. See [“Specifying QoS Settings” on page 835](#).

If QoS is not enabled, configure endpoint settings. See [“Specifying Endpoint Information” on page 836](#).

Specifying QoS Settings



NOTE: You can specify QoS parameters for a point-to-point service only in the service definition. This section explains the QoS attributes that can be defined or modified in a service definition. These settings cannot be modified in the service order.

If QoS is enabled on the service definition, configure the QoS Settings of the General/Connectivity Settings panel.

1. In the **QoS profile** field, select a profile from the list.

The **QoS profile** list displays the QoS profiles that are currently configured in the Manage CoS Profiles page of the Connectivity Services Director application.

A QoS profile classifies traffic into defined service groups to provide the special treatment of traffic across the network service.

2. Configure endpoint information. See [“Specifying Endpoint Information” on page 836](#).

Specifying OAM Settings

By default, OAM is enabled on the service definition. Enter the following information in the OAM Settings of the General Settings panel:

1. In the **OAM Profile** field, select a profile from the list.



NOTE: For OAM Settings, if you specify a CFM profile (for example, a CFM action profile with remote MEP), or an SLA-Iterator profile, first you must ensure that the profile is attached to the same device upon which you intend to deploy the P2P service order. If the profile is not previously attached (using the OAM Insight application), it is not on the device to support the service order.

To remove a previously associated CFM definition or OAM profile from a service definition, click the **Detach** button next to the OAM Profile field to remove the association. To associate a new OAM profile, you must dissociate the existing OAM profile and attach a fresh OAM profile. Detaching an OAM profile is enabled when you modify a service or service order.



NOTE: For Juniper Networks PTX3000 Packet Transport Routers, if you attach a CFM Definition to the service order, the CFM session operates for MEPs in either the Up or Down direction when the service is deployed.

2. Click **CFM Details** beside the OAM Profile field to view the profile configuration details in a dialog box.
3. Configure endpoint information. See [“Specifying Endpoint Information” on page 836](#).

Specifying Endpoint Information

If a service template is attached to the service definition, a link to that template is listed in the Template page of the creation of service order wizard. The service templates settings are same for both the endpoints. For instructions on working with service templates in service orders, see [“Creating a Service Order Based on a Service Definition with a Template” on page 990](#).

Some of the fields differ from one interface type to another and also differ depending on permissions assigned in the service definition.

Create Point-to-Point Service Order.

General/Connectivity Settings > **Endpoint A Settings** > Endpoint Z Settings > Template Settings > Review

You are here: Endpoint A Settings

Endpoint A

PE Device*: 960R1_EP_Alok_re Select Clear

UNI Interface*: ge-0/0/2 Select Clear

UNI Description:

Physical IF encapsulation: flexible-ethernet-services

Logical IF encapsulation: vlan-ccc

Traffic Type: DOT1Q Transport single vlan

☒ Auto pick Unit ID

☒ Auto pick VLAN ID

LSP Name: R1-to-R4

Back Next Done Cancel

To specify endpoint information:

1. In the **PE device** field, select the N-PE device you want to use for the first endpoint.

If you are unsure about which PE device to choose, go to the Prestaging Devices workspace landing page, which shows capacity information about UNIs on PE devices. You must pick a device that has available UNIs.

This step is required for all service orders.

You can configure the primary endpoint device as an unmanaged device. With the primary endpoint as an unmanaged device, the following combinations of primary and backup endpoints are supported:

- Primary (endpoint Z) as an unmanaged device and no backup (endpoint Z) device.
- Primary (endpoint Z) as an unmanaged device and backup (endpoint Z) as a managed device.

The following combinations are not supported:

- Primary (endpoint Z) as an unmanaged device and backup (endpoint Z) as an unmanaged device.
- Primary (endpoint Z) as a managed device and backup (endpoint Z) as an unmanaged device.

You cannot configure the backup endpoint Z as an unmanaged device using Connectivity Services Director. P2P Resiliency cannot be configured if any one of the endpoints is unmanaged. A validation is performed for the supported combinations of endpoints.



NOTE: If this endpoint is a third-party device, select **Unmanaged device** from the PE Device field list. You need to specify only the IP Address and Unmanaged Interface. For more information, see *Provisioning a Single-Ended Point-to-Point Service*.

2. In the UNI interface field, select a UNI.

The list includes all UNIs available on the selected device.

This step is mandatory for all service orders.

If you have selected the **Enable Multi Segment Pseudowire** check box in the service definition, the **UNI interface** of the second endpoint lists the interworking (iw) interfaces only.

For more information on point-to-point pseudowire stitching, see [“Stitching Two Point-to-Point Pseudowires” on page 858](#).

You can enter the description of the UNI interface in the **UNI description** field.

3. Specify the stitching unit.

Default: 0

Range: 0 through 255



NOTE: This field is displayed only in the second endpoint. You must have selected the **Enable Multi Segment Pseudowire** check box in the service definition.

4. In the **Traffic type** field, designate whether you want the service to transport all traffic, a single VLAN, or multiple VLANs.

Although this field is present for all service orders, the value is predetermined for some types of interfaces. For example, a port-to-port interface always transports all traffic. Moreover, for interface types that do support multiple traffic types, you can select this value only if the service definition allows you to do so.

If you are allowed to select this field, depending on the interface type, you can choose from the following values:

- Transport single VLAN
- Transport VLAN range
- Transport all traffic



NOTE: The **Physical IF encapsulation** and **Logical IF encapsulation** fields are not selectable. These values are set in the service definition.

The **Vlan Range for manual input** field displays the VLAN range that is specified in the service definition.

If the **Ethernet option** is *do1q* or *qinq*, and the **VLAN selection** is *Transport single vlan* type, the **Vlan Range for manual input** range is used for validation of manually entered VLAN.

If the **Ethernet option** is *qinq*, and the **VLAN selection** is *Transport vlan range* type, the **Vlan Range for manual input** range is used for validation of manually entered outer VLAN.

If the **Ethernet option** is *do1q*, and the **VLAN selection** is *Transport vlan range* type, the **Vlan Range for manual input** range is used for validation of manually entered customer's VLAN start and VLAN end.

5. In the **C-VLAN ID** field (or **VLAN ID** field), enter the customer's VLAN ID.

This field is mandatory for service orders that transport a single customer VLAN. The ID is provided by the customer.

6. In the **C-Vlan Start** and **C-Vlan End** fields, specify the beginning and end of the range of customer VLANs that you want the service to transport.

This field is mandatory for all services that transport a specific range of customer VLANs. These VLAN IDs are provided by the customer.

7. Select the **Auto pick VLAN ID** check box to have the system choose a service VLAN ID automatically.

This field is present only for interface types that provide double tagging; that is, only for Q-in-Q endpoint interface types. If this field is not set, then you must enter a service VLAN ID manually.

8. In the **VLAN ID** field, specify the service VLAN ID that you want be used to provide the outer tag for the service.

This field is present only for interface types that provide double tagging, and only if the **Auto pick VLAN ID** check box is not selected.

9. Specify whether the **Autopick UNIT ID** can be selected automatically or manually.

- To assign the **UNIT ID** automatically, select the **Autopick UNIT ID** check box.
- To assign the **UNIT ID** manually, clear the **Autopick UNIT ID** check box.

The window expands to include the **UNIT ID** field. In the **UNIT ID** field, type a value.

Range: 1 through 1073741823



NOTE: You can edit this field only if you have selected the **Editable in Service Order** check box for the **VLAN ID** selection in the service definition.

10. In the **MTU (Bytes)** field, specify the maximum transmission unit size for the UNI.

This field is present in all service orders. However, you can set this field only if the service definition allows you to do so.

11. If you selected the **Static pseudowire** check box in the selected service definition, you need to specify the **Outgoing label** for the static pseudowire.

Range: 1000000 through 1048575

In case of multi-segment pseudowire, you have to specify a new outgoing label for the second segment. The outgoing label for the second segment is not prepopulated from the first segment.



NOTE: You must manually compare the encapsulation, TDM bit rate, and control word of the router with the remote peer router and ensure that these parameters match; otherwise the static pseudowire might not work.

12. In the **Bandwidth (Mbps)** field, select a value from the list to limit the bandwidth of the service you are creating.

This field is present only if bandwidth limiting is allowed by the service definition, and is configurable in the service order only if the service definition allows you to do so.

When you click another graphic element in the main graphic area, the selected device name and interface name appear beneath the endpoint image in the main graphic.

13. If you have enabled the **Enable PW access to L3 VPN network** check box in the selected service definition, fill in the following fields in PW Stitching:

- **L3 routing instance name**—Specify the name of the Layer 3 routing instance.
- **Autopick interface IP**—If this field is enabled, specify **IP block size** and **IP address pool**; otherwise specify the **Interface IP address**.
- **Autopick peer unit**—To select the logical system unit number automatically, select the check box; otherwise specify the **Peer unit name**.



NOTE: These fields are available only if you have selected an LT interface in the UNI interface.

14. If you have enabled the **Enable PW Resiliency** check box in the selected service definition, fill in the following fields in the Backup settings and Resiliency settings:

- **Enable**
- **PE device**
- **UNI interface**
- **MTU (Bytes)**
- **LSP tunnel name**
- **Revert time (sec)**
- **Switch Over Delay (sec)**

For more information of pseudowire redundancy, see [“Redundant Pseudowires for Layer 2 Circuits and VPLS” on page 94](#).

15. Select the **Enable send-oam config** check box to enable the **send-oam** command. You can enable or disable this check box even in the Modify Service page.
16. To provide endpoint information for the second endpoint, click the **Endpoint Z** button (or click **Next**).

The Endpoint Settings form appears in the right panel for the second endpoint. Complete this form as for the first endpoint (repeat Step 1 through Step 18).

17. Click **Next** to proceed to the last step of the wizard, which is to examine the specified service attributes and submit the changes. Alternatively, click **Back** to navigate to the previous step of the wizard.

Specifying Template Settings

The Template Settings page of the service order creation and modification wizards enables you to associate service templates with a point-to-point, VPLS, and Layer 3 VPN service order. You can apply only the templates that are previously configured in a service definition with the corresponding service order. The Template Settings page is available in the service order wizard only if the service definition that you selected to apply to the service order contains a service template. Otherwise, the Template Settings page is not displayed in the service order wizard. You can perform template operations for all endpoints in a service order.

If you defined a service template as the default service template, it is attached to the endpoint by default. You have the flexibility to create and provision a dynamic attribute in a service template. You can mark an attribute of a service template as dynamic, and you can obtain the values for these dynamic attributes from a specific device. To create a dynamic attribute, you must first mark an attribute of a service template as dynamic and then specify the device XPath for the dynamic attribute.

The Template Settings page is displayed before the Review page, which is the final step of the service order wizard.

In the Service Settings page of the Select Service Definition field of the service order creation wizard, you can double-click a service definition name displayed in the table to view the details of the definition in a popup dialog box. You can use this information to determine if the service definition is appropriate for your deployment needs. To filter and sort the display of service templates, enter the name of the template as a match criterion in the Search box and click the Search icon. The page refreshes to display only the template names that match with the search term. You can use the paging controls to navigate across multiple pages of templates as necessary.

All the tasks that you can perform with service templates are presented in the Template Settings page. The page is divided into three panes. The top half of the page displays a table of selected endpoints. All the endpoints or UNIs that you selected in the preceding pages of the service order wizard are displayed in this table. You can configure the template pertaining to only one endpoint at a point in time. If the selected endpoints (in previous pages of the wizard) contained a manually-entered unit number, that number is displayed in the table of selected endpoints. Otherwise, the Auto-pick label is displayed.

The lower half of the page is divided into two panes. The left pane displays the template selection table for the endpoint you selected. All the templates associated with the service definition are displayed. You can add and delete templates using the template selection table. The right pane displays all the parameters that you can modify for a selected service template. All such editable parameters are displayed in a consolidated

form of a configuration page. This pane is displayed after you select a template. If any configuration parameter in template is set as a service-specific value, such attributes are not displayed in this pane.

Create Point-to-Point Service Order.

General/Connectivity Settings > Endpoint A Settings > Endpoint Z Settings > **Template Settings** > Review

You are here: Template Settings

Select End Points

Device	Interface	Unit
960R1_EP_Alok_re	ge-0/0/2	auto-pick
<input checked="" type="checkbox"/> 960R2_EP_Alok_re	ge-0/0/5	auto-pick

Page 1 of 1 | Displaying 1 - 2 of 2 | Show 10 items

Select Templates

Add Delete | Enter:

Name
<input checked="" type="checkbox"/> P2P_LDP_L2circuitOptions

Page 1 of 1 | Show 10

Configuration Page for the selected template P2P_LDP_L2circuitOptions Save

Config Page : cp1

policy-options

community

Members[@rowid="1"] 69-100

Back Next Done Cancel

To associate a service template with a service order:

1. Click **Add** to include a service template for the endpoint. A dialog box is displayed with the list of service templates associated with the service definition that is used to create the service order. The templates selected in this dialog box are displayed in the Template Selection table for the specified endpoint. Such templates are considered to be attached to that endpoint.

If you specified a template as a default template during the service definition creation, the template is displayed by default in the template selection table. You can associate non-default templates with the service order by clicking the **Add** button.

2. Click the link in the template name to open the Template Details dialog box. The template settings are displayed in the popup dialog box. For the selected template, the Configuration Page is displayed in the lower-right pane of the Template Settings page.
3. Modify any template-specific service components as necessary.
4. Click **Save** to submit the changes.
5. Select a template from the Template Selection table, and click Delete to remove the template from being associated with the service order for a particular endpoint.

Reviewing the Configured Settings

The Review page of the service definition or service order creation and modification wizards enable you to view and evaluate the service parameters and components you configured in preceding steps or pages of the wizard. This page provides a comprehensive, single-page view of all the service elements configured in the different pages of the wizard. You can either click the buttons corresponding to the various settings at the top of the wizard page to directly traverse to the page you want to modify or click the navigation buttons at the bottom of the wizard page to go to the different pages of the wizard.



NOTE: On the Review page, in the Service Templates section, the names of the service templates with which the service definition is associated are displayed. The Default Service Template column indicates whether the attached template is the default template.

Create Point-to-Point Service Order.

General/Connectivity Settings > Endpoint A Settings > Endpoint Z Settings > Template Settings > Review

You are here: Review

General/Connectivity Settings Edit

Service Order Name:	P2P_SO
Customer Name:	Amazon
Customer ID:	725842
Policy Name:	P2P_Template
Policy ID:	492786
Service Type:	ELineMartini

Connectivity Settings

MTU:	1522
Auto-Pick VC ID:	true
VLAN normalization:	Normalize to None

Endpoint A Settings Edit

Device Name:	960R1_EP_Alok_re
Device ID:	721066
UNI Interface Name:	ge-0/0/2

Back Next Done Cancel

1. Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify.
2. Click **Edit** next to the section that contains the parameter you want to modify. You are navigated to the corresponding page of the wizard in which the parameter settings are defined.

3. Click **Finish** to save the service definition or service order.
4. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

The service order inventory window appears.

Specifying Connectivity and Endpoint Information for Managing VLANs

The Connectivity Services Director application provides greater flexibility for provisioning VLANs for Point-to-Point service orders by extending the VLAN normalization options.

You can create logical interfaces that define both the **Outer-VLAN-tag-to-stack** protocol ID and **Inner-VLAN-tag-to-stack** protocol ID. The following illustration shows the **General/Connectivity** window. The **Connectivity Settings** panel displays the **Outer-VLAN-tag-to-stack** and **Inner-VLAN-tag-to-stack** parameters.

Connectivity Services Director now enables you to manually select a value for the **Outer VLAN tag to stack** and **Inner VLAN tag to stack** parameters for a service that specifies the **qinq Ethernet** option.

The following illustration displays the service order **Connectivity Settings** based upon a service definition that set the **VLAN normalization parameter** to **Normalize to Dot1q tag**.

For service orders that are based on service definitions that set the **Ethernet** option to **dot1q** or **qinq**, the **Unit ID** parameter appears in the **Logical IF Settings** panel in the service order **Endpoint Settings** window.

Deploying and Monitoring the Progress of the New Service

To deploy the new service:

1. Perform one of the following actions in the Deploy mode of the Service View of Connectivity Services Director:
 - To deploy the service immediately, select **Deploy now**, then click **OK**.
 - To deploy the service later, select **Schedule deployment**, select a date and time, then click **OK**.

The time field specifies the time kept by the server, but in the time zone of the client.

2. To monitor the progress and status of the deployment, use the Jobs workspace.

Related Documentation

- [Creating a Service Order on page 815](#)
- [Creating a Point-to-Point ATM or TDM Pseudowire Service Order on page 816](#)
- [Cloning Deployed Point-to-Point Services](#)
- [Creating a Bulk-Provisioning Service Order for Pseudowire Services on page 845](#)
- [Creating an Inverse Multiplexing for ATM Service Order on page 849](#)
- [Provisioning a Single-Ended Point-to-Point Service on page 853](#)

- [Selecting Specific LSPs for Connectivity Services on page 855](#)

Creating a Bulk-Provisioning Service Order for Pseudowire Services

Bulk provisioning allows for devices with similar configurations to be deployed as a group. The groups can be defined based on some characteristic common to all of the devices in a group, such as their functional role. Mobile backhaul deployments, for example, can run into hundreds of thousands of devices. These devices are commonly grouped according to their functional rules such as Cell Site Devices, Pre-aggregation or Hub-site devices, Aggregation Devices, Edge Routers and so on. To use this feature, tags must be defined and created so that groups can be selected. This feature is intended to simplify deployments of large groups of devices.

Prerequisites

- You can create a bulk provisioning service order only using the Services Activation Director GUI and not using the Connectivity Services Director GUI.
- Existing point-to-point pseudowire service definitions that will be used for the bulk-provisioning service order.
- Tags - You must have defined tags in the Prestaging workspace that you intend to use for groups of devices for which you will be creating the bulk service order. If you do not have tags already created, you can select **Prestage Devices > Manage Device Roles** and either select existing tags to apply to devices or create new tags.

Name	Management Address	Loopback Address
kochin	10.216.114.110	50.1.2.1
junos-space5	10.216.114.123	30.1.2.11
junos-space3	10.216.114.121	30.1.2.9
junos-space2	10.216.114.120	30.1.2.8
junos-space1	10.216.114.119	30.1.2.7
junos-mx80-2-space	10.216.114.105	30.1.2.3
junos-mx80-1-space	10.216.114.104	30.1.2.5
junos-mx480-space	10.216.114.100	30.1.2.6
junos-m10-2-space	10.216.114.103	30.1.2.2
junos-m10-1-space	10.216.114.102	30.1.2.4
jaipur	10.216.114.112	50.1.2.2

To begin the bulk provisioning process, in the Network Activate task pane, select **Prestage Devices > Manage Device Roles** and choose a service definition from the list. Click on the tag view of the inventory list.

1. Select the tag you want to use from the left **Tag** panel.
2. Select the devices you want to include in the tagged group.
3. Click, **Apply Tag**.
4. In the Network Activate task pane, select **Service Design > Manage Service Definitions**. The Manage Services Definitions page displays a list of service definitions.
5. Right-click on the point-to-point service definition, and select **Create Bulk P2P Service Order**.

The Create Bulk P2P Service Order window appears.

Name	State	Service Type	Signaling	Created By	Created Date
p2pst2	Published	Point-to-Point Pseudowire	LDP	super	Oct 31, 2012 8:11:40 AM EDT
QOS2	Published	VPLS (MultiPoint-MultiPoint)			Oct 31, 2012 7:54:18 AM EDT
QOS1	Published	VPLS (MultiPoint-MultiPoint)			Oct 31, 2012 7:50:18 AM EDT
ldp_qinq_bandwi...	Published	Point-to-Point Pseudowire			Oct 31, 2012 7:07:10 AM EDT
cfm-vpls	Unpublished	VPLS (MultiPoint-MultiPoint)			Oct 31, 2012 6:46:35 AM EDT
VPLS_CFM	Unpublished	VPLS (MultiPoint-MultiPoint)	LDP	super	Oct 31, 2012 6:39:43 AM EDT
P2P_ST	Published	Point-to-Point Pseudowire	BGP	super	Oct 31, 2012 5:48:46 AM EDT

6. In the Bulk point-to-point provisioning window, define the settings for the service order.

Create Bulk P2P Service Order

General Settings

Signaling: LDP

Service definition: ELine-QinQ-VLANRange

Name:

Customer: HCL

VLAN normalization: Normalization not required

CFM definition: StdDef-CFMSERVICE

Service tag: Type or select from choices...

Description:

Endpoint Settings

Bandwidth: 10 Mbps

MTU (Bytes): 1522

A End Settings

PE Device/Tag: fortius-f2100-a

UNI interface: ge-1/0/3

UNIT ID: 1

UNIT ID increment: 0

VLAN ID:

VLAN ID increment: 0

Customer VLAN start:

Customer VLAN end:

Z End Settings

PE Device/Tag: junos-space5

UNI interface: ge-0/1/6

UNIT ID: 1

UNIT ID increment: 0

VLAN ID:

VLAN ID increment: 0

Customer VLAN start:

Customer VLAN end:

Create

Cancel

Field	Action
Name	Provide a name for the bulk service order
Customer	Select the customer name from the list of defined customers.
VLAN normalization	<p>The options available in the VLAN normalization are based on the value set for the Ethernet interface.</p> <p>For information on VLAN normalization, see “Creating a Point-to-Point Ethernet Service Definition” on page 599.</p>
Bandwidth	Specify the bandwidth for the endpoints
MTU (Bytes)	Specify the MTU size in bytes.
Service tag	Select the service tag from the defined list. This tag will be applied to the services you create.
Description	Provide a description for the service tag.

Copyright © 2019, Juniper Networks, Inc.

847

Field	Action
Defining the Endpoint Settings	
To define the endpoint settings, you will define both the A endpoint and the Z endpoint.	
As an example of how you can use the bulk provisioning and how the endpoints work, if you want to establish a hub-spoke pseudowire between an Aggregation PE and a set of CSR devices, you can tag all the CSRs with a certain tag in the Manage Device Roles page. You can then select the PE device on the A end and the tag that you have already created for all the CSR devices on the Z end. If the endpoint is a tag then you can provide a wild-card interface (for example, ge-0/*/*) that matches all the devices under that tag.	
Define the A End Settings	
PE Device/Tag	Select the device or tag from the defined list.
UNI interface	Select the UNI interface from the list
VLAN ID	VLANs are created as part of this process. Enter the beginning VLAN ID that you want to use for creating the new service orders.
VLAN ID increment	Indicate how the VLAN IDs will be assigned for each of the new services. The number of VLANs created depends on the number of new services you are creating. One service order will be created for each device in the tag group.
UNIT ID	Specify the unit ID. Range: 1 through 1073741823
UNIT ID increment	Indicate how the unit IDs are assigned for each of the new services. The number of units created depends on the number of new services you are creating. One service order will be created for each device in the tag group.
Define the Z End Settings	
PE Device/Tag	Select the device or tag from the defined list.
UNI interface	Select the UNI interface from the list
VLAN ID	Enter the VLAN ID from the list of existing VLANs. VLAN range cannot be used for this feature.
VLAN ID increment	Indicate how the VLAN ID
UNIT ID	Specify the unit ID. Range: 1 through 1073741823
UNIT ID increment	Indicate how the unit IDs are assigned for each of the new services. The number of units created depends on the number of new services you are creating. One service order will be created for each device in the tag group.

- When required information has been entered, click **Create**.

The service order that you have created is graphically represented in the topology. To view the service order that you have created in the topology, select **Platform > Network Monitoring > Topology > Service > NA service order name**. Select the service order to view its parameters.

8. From the **Deploy Service** window, select the deployment method you wish to use.

**Related
Documentation**

- [Creating a Point-to-Point ATM or TDM Pseudowire Service Definition on page 618](#)

Creating an Inverse Multiplexing for ATM Service Order

Before you can create a service order that implements Inverse Multiplexing for ATM (IMA), you must preconfigure a T1 or E1 IMA Group interface (at-fpc/pic/g) on the devices upon which you want to deploy the service, before you prestage the devices in the Junos Space Connectivity Services Director application.

To create an inverse multiplexing for ATM service order:

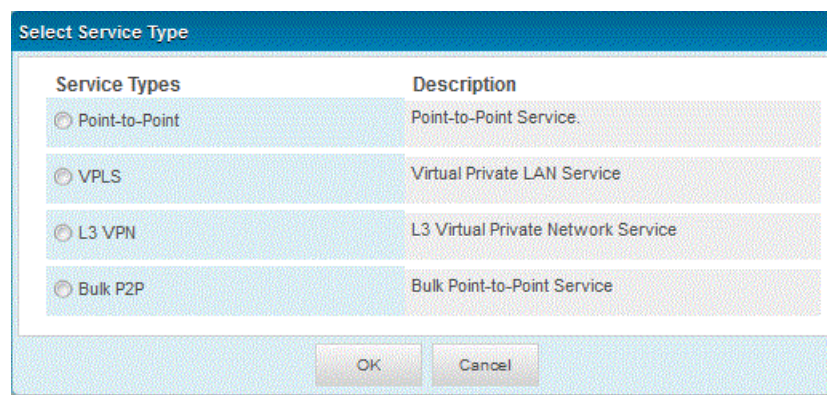
A wizard is available to create a service order in an intuitive and easily-navigable format. The settings that you can configure in the service order are organized in separate pages of the wizard, which you can launch by clicking the appropriate buttons at the top of the Create a Service Order page. Alternatively, you can proceed to the corresponding setting-related pages by clicking the **Back** and **Next** buttons at any point in the wizard during the creation of the service order.

With the Service View selected and in the Deploy mode of Connectivity Services Director, from the Network Services > Connectivity task pane, select **Service Provisioning > Deploy Services**.

The Manage Network Services page is displayed in the upper part of the right pane.

Click the **New** icon at the top of the lower half of the page that displays previously created service orders. The Select Service Type dialog box appears. Do one the following

- Select **Point-to-Point** to create a point-to-point service order.
- Select **VPLS** to create a VPLS service order.
- Select **L3 VPN** to create a Layer 3 VPN service order.
- Select **Bulk P2P** to create a bulk point-to-point service order.



1. Select **P2P** to create a point-to-point service order. The **Create P2P Service Order** window appears.
2. Select the service definition upon which you want to create the service order. Click **Next** to move to the next page of the wizard. The left panel displays a representation of the connection you are configuring. The right panel displays the **General/Connectivity Settings**.
3. Fill in the fields in the **General/Connectivity** panel.



NOTE: In the service order creation wizard for point-to-point services, the search function has been enhanced to enable you to easily sort and filter the parameters that are of interest and relevance for the services you want to configure. The Choose Customer dialog box that is displayed when you click **Select** beside the Customer field contains the Search box, which enables you to perform a search on all of the columns. The search utility that is present in the Choose Service Definition dialog box that is displayed when you click **Select** beside the Service Definition field enables you to search by Name, Created by, and Signaling columns; search utility is not supported for other columns in the dialog box. The search box that is present in the Choose Endpoints dialog box when you click **Select** beside the PE Device and UNI Interface fields enables search across all the columns displayed in the dialog box. For any string-based search (which shows strings that match any part of the text you enter in the search box), only the Name, Platform, and OS Version columns are supported. For exact string-based search (which shows strings that exactly match the text you enter in the search box), the IPAddress, State, and Manage State columns are supported.

4. Click **Next**. The **Endpoint Settings** panel for Endpoint A appears.
5. Fill in the Endpoint A settings. Ensure that you select a device on which a T1 or E1 IMA Group interface was preconfigured.
6. Click **Next**. The **Endpoint Settings** panel for Endpoint Z appears.
7. Fill in the Endpoint Z settings. Ensure that you select a device on which a T1 or E1 IMA Group interface was preconfigured.
8. Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.
9. After you complete reviewing the settings, click **Finish** to complete the service order creation.
10. To deploy or deactivate the service order on devices, click the **Deploy** icon in the Service View of the Connectivity Services Director banner, and from the **Network Services > Connectivity** task pane, select **Service Provisioning > Deploy Services > Manage Service Orders > service order name**. Select the service order to view its configuration parameters, decommission the settings applied to devices, or deploy the service order to devices.

11. Select the deployment option you want from the top of the page that lists the created service orders:

- **Deploy now**
- **Schedule deploy** (Specify the date and time.)

The Connectivity Services Director application displays the **Job Details** window, which includes a **Job Details ID** number.

12. In the Network Services > Connectivity view pane, select **Service Provisioning > Deploy Services**.

13. In the **Manage Network Services** window, you can view the status of the service.

**Related
Documentation**

- [Creating a Point-to-Point ATM or TDM Pseudowire Service Definition on page 618](#)
- [Viewing Functional Audit Results for an Inverse Multiplexing for ATM Service on page 1106](#)

Provisioning a Single-Ended Point-to-Point Service

You can create a point-to-point link between the end points of a managed device and an unmanaged device. An unmanaged device is a third-party device. In cases where interoperability with a third-party device is necessary, Junos Space allows you to define the link between a Juniper Networks managed device and the third-party device. You need to specify the IP address and the end point interface name of the unmanaged device. The Junos Space does not validate the information of an unmanaged device. You cannot configure an unmanaged device. The Junos Space pushes the configuration only to managed devices.

You can configure the primary endpoint device as an unmanaged device. With the primary endpoint as an unmanaged device, the following combinations of primary and backup endpoints are supported:

- Primary (endpoint Z) as an unmanaged device and no backup (endpoint Z) device.
- Primary (endpoint Z) as an unmanaged device and backup (endpoint Z) as a managed device.

The following combinations are not supported:

- Primary (endpoint Z) as an unmanaged device and backup (endpoint Z) as an unmanaged device.
- Primary (endpoint Z) as a managed device and backup (endpoint Z) as an unmanaged device.

You cannot configure the backup endpoint Z as an unmanaged device using Connectivity Services Director. P2P Resiliency cannot be configured if any one of the endpoints is unmanaged. A validation is performed for the supported combinations of endpoints.

To create a point-to-point link to an end point that is not managed by Junos Space, in the Network Services > Connectivity view pane, select **Service Provisioning > Manage Service Orders > New > P2P**. The **Manage Service Orders** page displays an inventory of all available point-to-point service definitions.

Name	Service Type	Customer	State	Status	Fault Status	Definition	Activation Date	Last Modified Date
ldp_fm_test1	VPLS	test	DeploymentPending	Down		ldp_fm_test1	August 28, 2015, 1...	August 28, 2015, 1...
p2p_12l	P2P	test	Deployed-Active	Down		ELine-QinQ-AI/VLA...	August 27, 2015, 1...	August 28, 2015, 2...
p2p_noservice...	P2P	test	Deployed-Active	Down		p2p_eccc	August 28, 2015, 1...	August 28, 2015, 1...
P2p_existingser...	P2P	test	DeploymentPending	Down		p2p_eccc	August 28, 2015, 1...	August 28, 2015, 1...
Raj-P2P-1055	P2P	test	Deployed-Active	Up		ELine-Dot1q-Single...	August 29, 2015, 2...	August 29, 2015, 2...
Apple-P2P-1075	P2P	Apple	Deployed-Active	Down		ELine-Dot1q-Single...	August 29, 2015, 2...	August 29, 2015, 2...
p2p_cfm	P2P	test	Deployed-Inactive	Down		ELine-Dot1q-Single...	August 29, 2015, 3...	August 29, 2015, 3...
P2P_Traffic_R1-R4	P2P	Apple	Deployed-Active	Up		ELine-Dot1q-Single...	August 29, 2015, 1...	August 29, 2015, 1...
p2p_template	P2P	Apple	DeploymentPending	Down		P2P_template	August 30, 2015, 4...	August 30, 2015, 4...
ldp9131313	P2P	test	Deployed-Active	Down		ldp1	August 30, 2015, 9...	August 30, 2015, 9...
vpls_pr	VPLS	test	Deployed-Active	Up		ldp_fm_test1	August 28, 2015, 1...	August 28, 2015, 1...
VPLS-Traffic-R1...	VPLS	Apple	Deployed-Active	Down		ELAN-BGP-Dot1Q...	August 29, 2015, 1...	August 29, 2015, 1...
new_sot1	VPLS	Apple	Deployed-Active	Up		ELAN-BGP-Dot1Q...	August 30, 2015, 2...	August 30, 2015, 2...
vpls_ldp_324321...	VPLS	test	Deployed-Active	Down		vpls_ldp0908097097	August 30, 2015, 9...	August 30, 2015, 9...
QinQTagging	L3VPN	Apple	DeploymentPending	Down		L3VPN-OSPF-Static	August 30, 2015, 1...	August 30, 2015, 1...

1. Select the service definition upon which you want to base your service order from the Service Definition field.
2. Specify the general/connectivity settings. For details on creating a point-to-point service order, see [“Creating a Point-to-Point Service Order”](#) on page 829
3. Click **Next** to specify the endpoint settings.
 - If this end point is N-PE device, select a device from the **PE Device**. Configure the endpoint settings as mentioned in [“Creating a Point-to-Point Service Order”](#) on page 829
 - If this endpoint is a third-party device, select **Unmanaged device** from the **PE Device**.

Fill in the fields as indicated in the table:

Field	Actions
PE Device	Since the endpoint is a third-party device, select Unmanaged device from the list.
Loopback IP Address	Specify the loopback IP address of the third-party device. Range: 1.0.0.1 through 223.255.255.254, excluding 127.x.x.x
Unmanaged Interface	Specify the end point interface name of the unmanaged device, which is the third-party device.

4. Click **Next** to specify another endpoint settings.



NOTE: Both the endpoints cannot be a third-party device.

5. To finish creating the service order, click **Finish**.



NOTE: The functional audit is performed only on the Juniper Networks devices (managed devices). To perform a successful functional audit of an unmanaged device, configure the following attributes of an unmanaged device:

- Neighbor IP
- Virtual circuit ID
- Unit ID
- Encapsulation
- Filter
- Policer

**Related
Documentation**

- [Creating a Point-to-Point Service Order on page 829](#)

Selecting Specific LSPs for Connectivity Services

This feature allows you to associate a policy with a point-to-point service. This in turn attaches the pseudowire to an LSP, which satisfies the conditions of the policy. The configuration for the service order includes the LSP name as the Next hop name. The following topics provide information on attaching an LSP and viewing its details:

- [Associating an LSP with a Point-to-Point Service on page 855](#)
- [Viewing LSP Details in a Service Order on page 856](#)
- [Viewing LSP Details in a Service on page 857](#)
- [Viewing LSP Configuration Details on page 857](#)

Associating an LSP with a Point-to-Point Service

To associate an LSP with a point-to-point service:

1. Create a point-to-point service order.

- a. From Deploy mode of Service View, In the **Network Services > Connectivity** task pane, select **Service Provisioning > Deploy Services**, and from the **Manage Network Services** page, select **New > P2P**.

The **Manage Network Services** page displays an inventory of all available point-to-point services. For each selected service, you can view the associated service orders from the **Manage Service Orders** page in the lower part of the right pane.

- b. Select the service definition you want to base your service order on, and click **Next**. The **General/Connectivity Settings** window is displayed.
- c. Specify the general/connectivity settings.
- d. Click **Next**. The **Endpoint Settings** window is displayed. You can now attach an LSP tunnel to a service order. To provision the specific LSP, select an LSP tunnel from the **LSP tunnel**.



NOTE: The LSP tunnel is not a mandatory field. The service order is created even if you do not specify the LSP tunnel name.

- e. Click **Next** to configure another endpoint. To provision the specific LSP, select an LSP tunnel from the **LSP tunnel**
- f. To create a point-to-point service order, click **Finish**.

For more information on creating a point-to-point service order, see [“Creating a Point-to-Point Service Order” on page 829](#)

2. Deploy the point-to-point service order.

The LSP is now associated with the point-to-point service order.

Viewing LSP Details in a Service Order

From the Deploy mode of Service View, In the **Network Services > Connectivity** task pane, select **Service Provisioning > Deploy Services**. The **Manage Network Services** page is displayed in the top part of the right pane, which displays all of the configured services. The **Manage Service Orders** page is displayed in the bottom part of the right pane, which displays all of the service orders associated with a service.

To view the details of a point-to-point service order, double-click a point-to-point service order in the **Manage Service Orders** inventory page. If an LSP is associated with a point-to-point service order, the **Endpoint Details** window includes the following information:

- LSP tunnel name—Name of the LSP tunnel attached to the point-to-point service order.
- Community name—Name of the community. A community is a group of destinations that share a common property.

- Community member—One or more community members.

Viewing LSP Details in a Service

From the Deploy mode of Service View, In the **Network Services > Connectivity** task pane, select **Service Provisioning > Deploy Services**. The Manage Network Services page is displayed in the top part of the right pane, which displays all of the configured services. The Manage Service Orders page is displayed in the bottom part of the right pane, which displays all of the service orders associated with a service.

To view the details of a point-to-point service, double-click a point-to-point service in the **Manage Network Services** inventory page.

If an LSP is associated with a point-to-point service order, the **Endpoint Details** of a point-to-point service includes the information on the LSP.



NOTE: You cannot modify the LSP tunnel in a service.

Viewing LSP Configuration Details

In the **Network Services > Connectivity** task pane, select **Service Provisioning > Deploy Services**. The Manage Network Services page is displayed in the top part of the right pane, which displays all of the configured services. The Manage Service Orders page is displayed in the bottom part of the right pane, which displays all of the service orders associated with a service.

From the Manage Network Services page, select a service and click the **View Service Configuration** button at the top of the table of listed services.

If an LSP selection is provisioned, you can view the LSP selection configuration in the **Service Configuration** window.

Related Documentation

- [Creating a Point-to-Point Service Order on page 829](#)

Stitching Two Point-to-Point Pseudowires

A multi-segment pseudowire (MS-PW) is a static or dynamically configured set of two or more contiguous pseudowire segments that behave and function as a single point-to-point pseudowire. Each end of an MS-PW, by definition, terminates on a T-PE.

Pseudowires are deployed in large networks. Such networks typically encompass hundreds or thousands of aggregation devices at the edge, each of which would be a provider edge (PE). These networks can be partitioned into separate metro and core pseudowire domains, with multi-segment pseudowires connecting endpoints across the various domains. You can stitch two point-to-point pseudowires.

To stitch two point-to-point pseudowires:

1. Create a point-to-point service definition.

In the General tab, you must select the **Enable Multi Segment Pseudowire** check box to enable multi-segment pseudowire.

For more information on creating a point-to-point service definition, see [“Creating a Point-to-Point Ethernet Service Definition” on page 625](#).

2. Create a point-to-point service order.

The fields displayed in the point-to-point service order are based on the point-to-point service definition that you created in Step 1. In the second endpoint settings page, select an interworking (iw) interface and specify the stitching unit.

For more information on creating a point-to-point service order, see [“Creating a Point-to-Point Service Order” on page 829](#).

3. Deploy the point-to-point service order.

- a. Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane. From the **Network Services > Connectivity** task pane, select **Service Provisioning > Deploy Services**.

The Manage Network Services page is displayed in the top part of the right pane, which displays all of the configured services. The Manage Service Orders page is displayed in the bottom part of the right pane, which displays all of the service orders associated with a service.

- b. In the Manage Service Orders page, select the point-to-point service order you created in Step 2.
- c. Select the **Deploy now** option button at the top of the page and click **OK**.

The service order is deployed.

4. In the Manage Services inventory page, select the check box next to the point-to-point service that you created and select **Actions > Stitch PW Segment**. The Stitch PW Segment inventory page is displayed.

The Stitch PW Segment inventory page lists only the point-to-point service definitions with the **Enable Multi Segment Pseudowire** check box enabled. This inventory page must also list the point-to-point service definition you created in Step 1.

5. In Build mode of Service View, from the Manage Service Definitions page, select a point-to-point service definition and click **Next**.
6. Specify the General Setting, Connectivity Settings, and Endpoints details. For more information on these fields, see [“Creating a Point-to-Point Service Order” on page 829](#).



NOTE: The fields of the first endpoint are auto-filled. Notice that the second endpoint fields of the service order you created in Step 2 and the first endpoint fields of this service order are same.

7. Deploy the stitched service order.
 - a. Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane. From the **Network Services > Connectivity** task pane, select **Service Provisioning > Deploy Services**.

The Manage Network Services page is displayed in the top part of the right pane, which displays all of the configured services. The Manage Service Orders page is displayed in the bottom part of the right pane, which displays all of the service orders associated with a service.
 - b. In the Manage Service Orders page, select the point-to-point service order you created in Step 6.
 - c. Select the **Deploy now** option button at the top of the page and click **Ok**.

The service order is deployed.

The two point-to-point pseudowires are stitched.

The Manage Services lists both services. The point-to-point Service Details window displays the **Stitch PW Segment** details.



NOTE: The number of pseudowire segments that you can stitch is limited to two.

You can perform a functional audit to the first service only. You can view the details of the stitched pseudowire in the Functional Audit Results window.

- Related Documentation**
- [Creating a Point-to-Point ATM or TDM Pseudowire Service Order on page 816](#)
 - [Creating a Point-to-Point Service Order on page 829](#)

Deactivating a Service

This procedure disables a service for a particular protocol that you have previously created on the network. By disabling a service, the traffic processing for the traversed packets is impacted. In certain network topologies, you might require a service-related settings to be disabled for a certain period to perform troubleshooting or modification to the traffic-handling method, and you might want to reactivate a disabled service later when you have completed network maintenance and analysis work. In such a case, it might be beneficial to use the deactivation functionality for a service. When you disable a service, the configuration attributes associated with such a service are deactivated and commented out in the device settings. The deactivated service is propagated to the devices associated with the service order. To disable a service, the service must not contain any pending or uncommitted changes. Also, the service must be in the Deployed or Re-Activated state.



NOTE: To modify a service order, it must not be in the Deactivated state.

To deactivate a service:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
5. From the task pane, select **Service Provisioning > Deploy Services**. The top part of the right pane displays the Manage Network Services page, with the table of services, and the bottom part of the right pane displays the Manage Service Orders page, with the table of service orders.

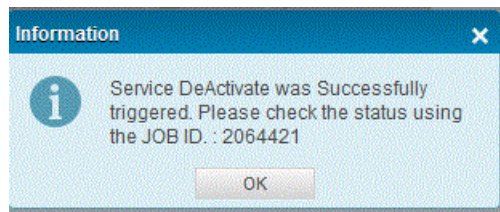


TIP: In Build mode of Service View, from the View pane, if you select the Network Services node and do not expand the Network Services > Connectivity tree, the top pane displays a pie chart that enables you to view and examine the different services configured for devices, and the types of service protocols configured. The Services by Type graph displays the count of services for each type of service definition. Mouse over each segment of the pie to view the number corresponding to the percentage of service orders for each of the charts. This chart provides a visual overview of customers and service orders on your network, and enables you to quickly access related and commonly needed information. For example, you can check for failed service orders and then access a list of failed requests so you can begin to take restoration measure.

6. From the Manage Network Services page, select the check box next to the service you want to deactivate.
7. Click the down arrow on the **Action** menu, above the table of listed services, and select **Deactivate** to disable the selected service. A dialog box is displayed prompting you to confirm your action.

The image shows a 'Confirmation' dialog box with a blue title bar and a close button (X). The main text reads: 'Deactivating a service will affect the traffic on the network. Are you sure you want to go ahead and create service modification request for the selected services'. Below this is a text field containing 'SO_edit1'. Under the heading 'Deployment Options:', there are two radio buttons: 'Deactivate Now' (which is selected) and 'Deactivate Later'. Below the 'Deactivate Later' option, there is a 'Date' field with the value '2015-03-26' and a 'Time' field with a dropdown arrow. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

8. Do one of the following in the Confirmation dialog box:
 - To deactivate the service immediately, select Deactivate now, and click Yes. If you click Yes, a pending change request is created for each selected service. Alternatively, if you click No, the deactivate operation is discarded.
 - To deactivate the service at a later time, select Deactivate later, and select a date and time for deployment, then click OK. The time field specifies the time kept by the server, but in the time zone of the client. After scheduling the service order for deactivation, the provisioning software begins validating the service order.



9. Use the Jobs workspace to monitor the outcome of the deployment.

- Related Documentation**
- [Reactivating a Service on page 862](#)
 - [Force-Deploying a Service on page 864](#)
 - [Decommissioning a Service on page 868](#)

Reactivating a Service

After you disable a service to deactivate the configuration settings on devices mapped to the service, you might require the service settings to be reenabled after you have modified the service parameters, either directly on the device or using the Connectivity Services Director application. In such a case, you can use the reactivation functionality to revive and activate the service properties on devices. To disable a service, the service must not contain any pending or uncommitted changes. Also, the service must be in the Deactivated state.

To reactivate a service:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
5. From the task pane, select **Service Provisioning > Deploy Services**. The top part of the right pane displays the Manage Network Services page, with the table of services, and the bottom part of the right pane displays the Manage Service Orders page, with the table of service orders.



TIP: In Build mode of Service View, from the View pane, if you select the Network Services node and do not expand the Network Services > Connectivity tree, the top pane displays a pie chart that enables you to view and examine the different services configured for devices, and the types of service protocols configured. The Services by Type graph displays the count of services for each type of service definition. Mouse over each segment of the pie to view the number corresponding to the percentage of service orders for each of the charts. This chart provides a visual overview of customers and service orders on your network, and enables you to quickly access related and commonly needed information. For example, you can check for failed service orders and then access a list of failed requests so you can begin to take restoration measure.

6. From the Manage Network Services page, select the check box next to the service you want to reactivate.
7. Click the down arrow on the Action menu, above the table of listed service orders, and select Reactivate to reenab the selected service order. A dialog box is displayed prompting you to confirm your action.
8. Do one of the following in the Confirmation dialog box:
 - To reactivate the service immediately, select Reactivate now, and click Yes. If you click Yes, the selected service is activated immediately. Alternatively, if you click No, the deactivate operation is discarded.
 - To reactivate the service at a later time, select Reactivate later, and select a date and time for reactivating, then click OK. The time field specifies the time kept by the server, but in the time zone of the client.
9. Use the Jobs workspace to monitor the outcome of the deployment.

**Related
Documentation**

- [Reactivating a Service on page 862](#)
- [Force-Deploying a Service on page 864](#)
- [Decommissioning a Service on page 868](#)

Force-Deploying a Service

When a service fails a configuration audit because configuration changes on a PE device do not match the configuration required for the service, you can force-deploy the service to push the configuration to the device.

Force deployment pushes the same configuration to the device that was pushed during the deployment of the service, thus allowing the operator to recover from a state in which the configuration on the device was lost or changed out-of-band.

The validation before generating the configuration for a force-deployed service order will be performed against the current configuration on the device and the configuration is not pushed if the validation fails. If the forced deployment is unable to push the configuration again, then you might need to manually configure the device.

This procedure forces deployment of a service on the network.

You cannot force-deploy an invalid service order.

To schedule a service for forced deployment:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
5. From the task pane, select **Service Provisioning > Deploy Services**. The top part of the right pane displays the Manage Network Services page, with the table of services, and the bottom part of the right pane displays the Manage Service Orders page, with the table of service orders.
6. From the Manage Network Services page, select the check box next to the service you want to forcibly deploy.

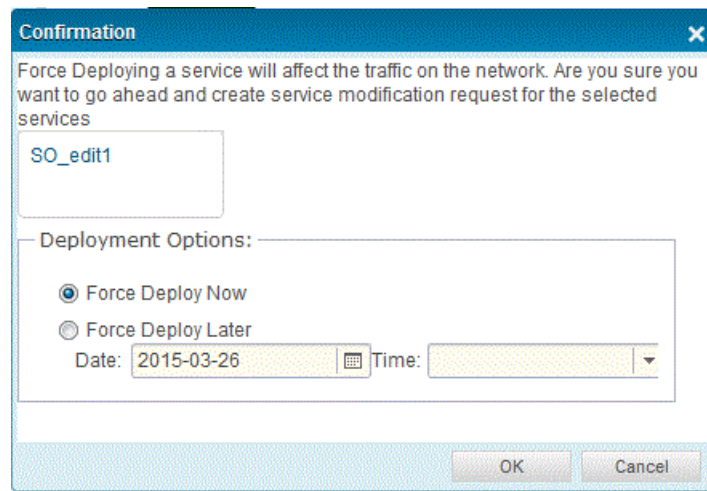


TIP: In Build mode of Service View, from the View pane, if you select the Network Services node and do not expand the Network Services > Connectivity tree, the top pane displays a pie chart that enables you to view and examine the different services configured for devices, and the types of service protocols configured. The Services by Type graph displays the count of services for each type of service definition. Mouse over each segment of the pie to view the number corresponding to the percentage of service orders for each of the charts. This chart provides a visual overview of customers and service orders on your network, and enables you to quickly access related and commonly needed information. For example, you can check for failed service orders and then access a list of failed requests so you can begin to take restoration measure.

The top pane displays information about the services that have been previously created, such as the name of the service, the functional audit status, the performance management status, and the status of the service. You can modify the properties of the service, conduct a functional or configuration audit, force-deploy or deactivate the service, and view alarms associated with a particular service order for debugging and corrective action. Services can be in one of the following service states:

- Completed—The service order has been successfully deployed.
 - Scheduled for deployment—The service provisioner has scheduled the service order for deployment.
 - Deployment Failed—An attempted service deployment was not successfully completed or failed an audit.
 - In Progress—The Connectivity Services Director application is in the process of deploying the service.
 - Requested—The service provisioner has created the service order, but has not yet attempted to deploy it or schedule it for deployment.
 - Invalid—The service order is not valid.
7. Open the **Actions** menu and click **Force Deploy Service**.

The **Schedule Force Deployment** window appears.



8. To deploy the service immediately, select **Force deploy now**, and click **OK**.

To deploy the service at a later time, select **Force deploy later**, select a date and time for deployment, then click **OK**.

The time field specifies the time kept by the server, but in the time zone of the client.

After scheduling the service order for deployment, the provisioning software begins validating the service order.

9. Use the Jobs workspace to monitor the outcome of the forced deployment.

**Related
Documentation**

- [Deactivating a Service on page 860](#)
- [Reactivating a Service on page 862](#)
- [Decommissioning a Service on page 868](#)

Recovering a Service Definition through Force Upload

You can use the force-upload feature to overwrite the service definitions that were recovered using the service recovery feature and do not contain the changes made through CLI configuration or through templates. You do this by creating a service definition containing templates that matches the configuration, and uploading it to the Connectivity Services Director application.



NOTE: You use service recovery to manage a service on the device. You can only upload data which is part of the service definition. The **Force Upload** feature is used to upload templates associated with the service definition.



NOTE: You can use templates to recover changes made through the CLI configuration. You use the **Force Upload** feature to upload a template for one or more endpoints associated with the service.

In Connectivity Services Director Release 2.0 and earlier, you cannot recover changes made to service definitions through CLI configuration or through templates.

To perform the force-upload action:

1. In the Connectivity Services Director Application, select **Service View** from the Views list.

The workspaces applicable to the services are displayed.

2. Click the **Deploy** tab in the Task Categories banner.

The features that you can configure in this mode are displayed in the Tasks pane.

3. From the Service View pane, click **Network Services**.

The tasks you can perform are displayed in the **Tasks** pane.

4. From the Tasks pane, select **Key Tasks > Manage Services**.

The **Manage Network Services** page is displayed.

5. Select the service you want to force-upload by selecting the check box next to the service.

6. Click the **Action** tab and select **Force Upload** from the list of actions.

The **Force Upload** page is displayed.

7. From the **Service Details** table in the force upload page:

- a. Click the arrow in the **Device Name** column of the table. From the list that appears, choose the device by selecting the check box next to it.

The device is added to the **Device Name** column.



NOTE: You can add more than one device at a time.

- b. Click the arrow in the **Interfaces** column of the table. From the list that appears, you can select more than one interface associated with the device.

The interface is added to the **Interfaces** column.



NOTE: Selection of devices and interfaces is optional. If you select a device or an interface, the template associated with the selected device or selected interface is uploaded.

If you select a device, all interfaces associated with that device are uploaded. If you select a device and an interface, the interface associated with that device is uploaded.

8. Click **Ok** to confirm force-upload.

The service definition is uploaded on the selected device and interface.

- Related Documentation**
- [Deactivating a Service on page 860](#)
 - [Reactivating a Service on page 862](#)
 - [Decommissioning a Service on page 868](#)

Decommissioning a Service

You can decommission a service that a customer no longer needs.

You cannot decommission a service if a service order requesting action on that service is in the Requested, Scheduled, In Progress, or Invalid state. The Y.1731 monitoring functionality must be in the disabled state (by selecting PM Statistics > Start from the task pane after selecting the specified service in the View pane in Monitor mode of Service View) for the service to be decommissioned.

To decommission a service:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
3. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
4. From the task pane, select **Service Provisioning > Deploy Services**. The top part of the right pane displays the Manage Network Services page, with the table of services, and the bottom part of the right pane displays the Manage Service Deployment page, with the table of service orders.
5. From the Manage Network Services page, select the check box next to the service you want to decommission.



TIP: In Build mode of Service View, from the View pane, if you select the Network Services node and do not expand the Network Services > Connectivity tree, the top pane displays a pie chart that enables you to view and examine the different services configured for devices, and the types of service protocols configured. The Services by Type graph displays the count of services for each type of service definition. Mouse over each segment of the pie to view the number corresponding to the percentage of service orders for each of the charts. This chart provides a visual overview of customers and service orders on your network, and enables you to quickly access related and commonly needed information. For example, you can check for failed service orders and then access a list of failed requests so you can begin to take restoration measure.

The top pane displays information about the services that have been previously created, such as the name of the service, the functional audit status, the performance management status, and the status of the service. You can modify the properties of the service, conduct a functional or configuration audit, force-deploy or deactivate the service, and view alarms associated with a particular service order for debugging and corrective action. Services can be in one of the following service states:

- **Completed**—The service order has been successfully deployed.
- **Scheduled for deployment**—The service provisioner has scheduled the service order for deployment.
- **Deployment Failed**—An attempted service deployment was not successfully completed or failed an audit.

- **In Progress**—The Connectivity Services Director application is in the process of deploying the service.
 - **Requested**—The service provisioner has created the service order, but has not yet attempted to deploy it or schedule it for deployment.
 - **Invalid**—The service order is not valid.
6. Open the **Actions** menu and click **Decommission Service**. Alternatively, select **Decommission** by drilling down the Manage Services tree in the task pane.

The **Schedule Decommission** window appears.

The image shows a 'Confirmation' dialog box with a blue header and a close button (X) in the top right corner. The main text reads: 'Decommissioning a service will affect the traffic on the network. Are you sure you want to go ahead and create service modification request for the selected services'. Below this text is a text input field containing 'SO_edit1'. Underneath the input field is a section titled 'Deployment Options:'. This section contains two radio buttons: 'Decommission Now' (which is selected) and 'Decommission Later'. Below the 'Decommission Later' option, there are two fields: 'Date:' with the value '2015-03-26' and a calendar icon, and 'Time:' with a dropdown arrow. At the bottom right of the dialog box are two buttons: 'OK' and 'Cancel'.

7. Do one of the following:
- To decommission the service immediately, select **Decommission now**, and click **OK**.

In the **Order Information** window, click the job ID of the decommission job.

The **Job Management** page appears and shows a filtered view of the job inventory, showing only the decommission job. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details.



NOTE: Alternatively, to display the Job Management page, click the **System** icon on the Connectivity Services Director banner, and select **Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

- To deploy the service at a later time, select **Decommission later**, select a date and time to perform the operation, then click **OK**.

If you decommission a service and the device confirms the deletion, the resources associated with the service are immediately released and are available for reuse without waiting for the device synchronization. If you want the synchronization to happen before the resources are released, you need to configure the decommissioning settings.

To configure the service decommissioning settings:

1. Select **Network Management Platform > Administration > Applications**. The Applications page displays the list of applications.
2. Right-click the Connectivity Services Director row and select **Modify Applications Settings**. The Modify Connectivity Services Director Settings page displays the list of parameters that can be modified.
3. Select **ServiceDecommission**.
4. Specify values for the parameters in the Service Decommission page as described in the following tables.

Field	Action
Wait for Device Sync Before Releasing Resource	Select this check box to wait for the device synchronization before resources are released. To revert the decommissioning to the normal behavior clear this check box.
Device sync wait time	Specify the device synchronization waiting time. This is the maximum wait time to complete the device synchronization. After this time duration, irrespective of the device synchronization status, the resources are released. Default: 60 seconds Range: 30 seconds to 300 seconds

5. Click **Modify**.

The service decommissioning settings are configured.

Related Documentation

- [Viewing Service Order and Service Details on page 803](#)

Viewing Alarms for a Service

Activity on a network device consists of a series of events. A software component on the network device, called an entity, is responsible for running the Simple Network Management Protocol (SNMP) to log and monitor these events. You can view the details of alarms and events generated for a particular service order to examine and diagnose the problems that are generating the alarms. These alarms provide essential and cohesive information about system conditions, any discrepancies and malfunctioning, and protocols or components that need to be examined and debugged for better efficiency and working capacity.

To view alarm and event details for a service:

1. Select Service View from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Build** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
4. From the task pane, select **Service Provisioning > Deploy Services**. The top part of the right pane displays the Manage Network Services page, with the table of services, and the bottom part of the right pane displays the Manage Service Deployment page, with the table of service orders.
5. From the task pane, select Service Provisioning > Deploy Services. The table of services is displayed.
6. Select the check box next to the service for which you want to view alarm details.
7. Click the **View Alarms** button, above the table of listed services.

The Alarm Detail dialog box is displayed.
8. Click **Close** after you finish evaluating the information to return to the Manage Network Services page.

Related Documentation • [Alarm Detail Monitor \(Service View\) on page 1280](#)

Inline Editing of VPLS and Layer 3 VPN Service Orders

The Manage Service Order windows that enable the provisioning of L3VPN and VPLS services utilize grids as a navigation element to add sites and interfaces to a VPN. In addition, grids are also used to select individual elements and configure any details that might be required for such element to be part of the VPN. For example, a typical VPLS configuration workflow involves the following steps:

Entering general service parameters that apply to all nodes in the VPN, such as the name of the service, signaling protocol used, route distinguishers, and route targets

Selecting the set of nodes that participate in the VPN instance. Per-node parameters can be configured by going through one node at a time, or through a bulk edit operation by selecting and editing multiple nodes simultaneously.

Choosing the set of interfaces on each node that connect to the customer devices and configure the interface-specific characteristic of each interface. Similar to the node settings, users can perform bulk edits to modify multiple interfaces at a time.

In your network environment, the VPLS and L3VPN services, owing to their multipoint nature, involve multiple devices and interfaces, which causes the configuration to require many steps, and becomes cumbersome and complicated. To simplify and optimize the configuration of multipoint services by allowing users to configure devices and interfaces in a grid so that the operator can easily view and modify the most important parameters of the service, the inline edit mechanism is implemented. Inline modification signifies the ability to perform changes to previously defined settings in an easy and quick manner.

Embedded editing is enabled, which causes the grids showing the devices and interfaces to become modifiable directly without the need to perform the process of highlighting, editing, and saving the changes every time you want to edit a particular parameter. The page that displays the configured settings presents as a form in which the fields or cells of the table are editable.

Because the inline edit functionality enables you to directly edit the grids, only the salient and most important parameters for each service in the grids are displayed.

For parameters that you can enable or disable, you can select or clear the check boxes.

For parameters that require a value to be specified, an auto drop-down list is displayed that enables you select a value from the list of available or configured values.

Device Name	Role	Spoke Settings		Mesh Settings		Topology
		Neighbour Hub	Backup Neigh...	Name	AutoPick/VCID	VCID
VPLS (Point-MultiPoint)						

Popup Dialog Box:

Name	Roles
400R3_BC_Rajesh_re	N_PE
400R4_BC_Rajesh_re	N_PE
960R1_BC_Rajesh_re	N_PE
960R1_BC_Verizon_re	N_PE
960R2_BC_Rajesh_re	N_PE
960R2_BC_Verizon_re	N_PE

OK Cancel

Page 1 of 1 Displaying 1 - 6 of 6

Advanced parameters can be continued to be edited by selecting the rows and clicking Edit. A popup dialog box is displayed with the list of all parameters supported for editing. You can perform inline edits by double-clicking in the cell or the field under a particular column in the table of displayed settings. The field becomes editable when you double-click within the cell.

For a VPLS service order, the following node settings can be modified using the inline edit method:

Service loopback, Hub, Mac learning, Mac Interface limit, Mac statistics

Parameter	Editable	Dependencies
Node	Yes	None
Status	No	None
Platform	No	None
Service loopback	Not available	None
Hub	Yes	Only available for hub-spoke topologies
Mac learning	Yes	None
Mac Interface limit	Yes	None
Mac statistics	Yes	None

For a VPLS service order, the following site settings can be modified using the inline edit method:

Node, Interface, Autopick Unit, Unit ID, VLAN tagging, Autopick VLAN ID, Outer VLAN ID, Inner VLAN ID, Rate Limit, Interface Description

Parameter	Editable	Dependencies
Node	Yes	None
Interface	Yes	The Node name has to be configured
Status	No	None
Autopick Unit	Yes	None
Unit ID	Yes	Only enabled when autopick unit ID is not checked
VLAN tagging	Yes	None. This is a combo box with 3 options (Disabled, Dot1Q and QinQ)
Autopick VLAN ID	Yes	Enabled when VLAN tagging is set to Dot1Q or QinQ
Outer VLAN ID	Yes	Enabled when VLAN tagging is set to Dot1Q or QinQ and autopick VLAN ID is not checked
Inner VLAN ID	Yes	Only available for QinQ VLAN tagging
Rate Limit	Yes	None
Interface Description	Yes	None

For an L3VPN service order, the following node settings can be modified using the inline edit method:

Node, Hub, Stitching point

Parameter	Editable	Dependencies
Node	Yes	None
Hub	Yes	Only editable for Hub-and-spoke topologies
Stitching point	Yes	When hub is selected, stitching point must be disabled

For an L3VPN service order, the following site settings can be modified using the inline edit method:

Node, Interface, Autopick Unit, Unit ID, VLAN tagging, Autopick VLAN ID, Outer VLAN ID, Inner VLAN ID, Auto pick IP, IP Address, Subnet

Parameter	Editable	Dependencies
Node	Yes	None
Interface	Yes	The Node name has to be configured
Status	No	None
Autopick Unit	Yes	None
Unit ID	Yes	Only enabled when autopick unit ID is not checked
VLAN tagging	Yes	Only enabled when the interface selected is not a loopback (lo0). For loopback interfaces the VLAN tagging should be set to disabled. For other ethernet-based interfaces, this should be a combo box with 3 options (Disabled, Dot1Q and QinQ)
Autopick VLAN ID	Yes	Enabled when VLAN tagging is set to Dot1Q or QinQ
Outer VLAN ID	Yes	Enabled when VLAN tagging is set to Dot1Q or QinQ and autopick VLAN ID is not checked
Inner VLAN ID	Yes	Only available for QinQ VLAN tagging
Auto pick IP	Yes	None
IP Address	Yes	If autopick is enabled this should be a combo box showing the available pools. If autopick is disabled, this should be an input text box allowing users to enter the IP
Subnet	Yes	None, when autopick is enabled this sets the block size. Then autopick is disabled it sets up the subnet size

Related Documentation

- [Modifying a Point-to-Point Ethernet Service on page 1024](#)
- [Modifying a Multipoint-to-Multipoint Ethernet Service on page 1026](#)
- [Modifying a Point-to-Multipoint Ethernet Service on page 1033](#)
- [Modifying a Hub-and-Spoke Layer 3 VPN Service Order on page 1042](#)
- [Modifying a Full Mesh Layer 3 VPN Ethernet Service on page 1057](#)

Interconnecting a Layer 3 VPN Service with a VPLS Service

You can stitch or interconnect a Layer 3 VPN service with a VPLS service. You must enable the stitching functionality to perform this interconnection. If the stitching capability is enabled, when you select the interfaces for the endpoints added to a service, only the integrated routing and bridging (IRB) physical and logical interfaces are available for selection. If you select a physical IRB interface, a new logical interface is created with the logical unit identifier of the interface you specify. If you select a logical IRB interface, the existing logical interface is used to create the service.

You can stitch or interconnect a Layer 3 VPN service with a VPLS service during the creation or modification of a Layer 3 VPN service order. Follow the steps outlined in for performing the tasks in the Service Settings and Node Settings pages of the wizard. To enable the stitching of a Layer 3 VPN service with a VPLS service, you can select the Stitch check box for a device associated with the service order on the Site Settings page of the Layer 3 VPN service order creation or modification wizard.

Before you begin:

- Ensure that you have already created a Layer 3 VPN service.
- Complete the configuration of settings on the Service Settings and Node Settings pages of the service order creation or modification wizard.

To interconnect a Layer 3 VPN service with a VPLS service:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the View pane, click the plus sign (+) to expand the tree and select the type of service.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
5. From the Tasks pane, select **Service Provisioning > Deploy Services**.

The Manage Network Services page is displayed in the top half of the right pane, which displays all of the configured services. The Manage Service Orders page is displayed in the bottom half of the right pane, which displays all of the service orders corresponding to a service.

6. From the Manage Network Services page, select **New > L3VPN Service**.

The **Create L3VPN Service Order** window appears and shows a filtered inventory view of only those published service definitions designed to work with multipoint Ethernet services. You can select the service definition based on the signaling type.

See [“Creating a Full Mesh Layer 3 VPN Ethernet Service Order” on page 941](#) and [“Creating a Hub-and-Spoke Layer 3 VPN Service Order” on page 964](#) for detailed information about the settings that you can configure on the Service Settings and Node Settings pages of the wizard.

7. After you complete the configuration of settings on the Service Settings and Node Settings pages of the service order creation or modification wizard, click **Site Settings** at the top of the wizard page.

The Site Settings page is displayed.

8. Select the check box beside the device for which you want to enable the stitching of VPLS and L3VPN services.

The device that you select is available for stitching.

9. Select the **Stitch** check box to enable the interconnection of the Layer 3 VPN service with a VPLS service.

10. Click inside the Interface Name field to select an IRB interface. A popup dialog box is displayed with the list of all configured IRB interfaces. If the stitching capability is enabled, when you select the interfaces for the endpoints added to a service, only the IRB physical and logical interfaces are available for selection.

11. Select a physical or logical IRB interface that you want to use to stitch the Layer 3 VPN service with a VPLS service.

The selected interface is used for interconnection of the services.

12. (Optional) If you select a physical IRB interface, you can specify the logical unit of the interface in the UNIT ID field.

The specified logical IRB interface is used for stitching the services.

13. For service orders associated with a service definition that contains a service template, click **Next** to modify the template settings.

14. Click **Review** to examine and modify the settings as necessary.

15. Click **Finish** when you have completed examining the settings to confirm the creation of the service order.
16. You can proceed to enable the stitching functionality for the same IRB interface with the VPLS service. See [“Interconnecting a VPLS Service with a Layer 3 VPN Service” on page 936](#) for detailed information about enabling the stitching functionality for the VPLS service.

Related • Documentation

Changing the Logical Loopback Interface for Provisioning

The loopback interface supports many different network and operational functions and is an *always-up* interface. This means that the loopback interface ensures that the device is reachable, even if some of the physical interfaces are down or removed, or an IP address has changed. In most cases, you always define a loopback interface.

Junos OS follows the IP convention of identifying the loopback interface as lo0.

Junos OS requires that the loopback interface always be configured with a /32 network mask, thus avoiding any unnecessary allocation of address space.

Typically, the VRF or virtual-router routing instance IP address is drawn from among the IP addresses associated with interfaces configured for that routing instance. If none of the interfaces associated with a VRF or virtual-router routing instance is configured with an IP address, you need to explicitly configure a logical loopback interface with an IP address. This interface must then be associated with the routing instance.

You change the logical unit of the loopback interface to be a logical unit other than unit 0 to be used as the default loopback logical interface for all provisioning tasks that are initiated from Connectivity Services Director



NOTE: Although Junos OS allows you to assign multiple loopback addresses to the same loopback unit, the Junos Space software recognizes only the first address assigned to the loopback unit. Therefore, when you change the loopback address of an N-PE device, it must be to that of a different loopback unit.

To change the logical unit of the loopback interface:

1. From the Junos Space user interface, click the **System** icon on the Connectivity Services Director banner.

The options that you can configure in System mode are displayed in a drop-down menu.

2. Select **Preferences** from the drop-down menu to open the Preferences page.

The Preferences page opens with User Preferences as the default tab.

3. Click the **Services Activation** tab to configure the services activation-related settings.

The settings that you can configure on the Services Activation tab are displayed.

4. Click the right arrow beside the **Prestage Device** section to expand it.

The parameters that you can configure for prestaging devices are displayed.

5. In the Loopback Unit field, specify the logical unit of the loopback interface that must be used as the default loopback logical interface for all provisioning tasks that are initiated from Connectivity Services Director. The default logical unit for the loopback interface is 0.

6. Click **OK** to save the settings. You are prompted to confirm the changes you made to services-activation preferences.

7. Click **Yes** to confirm. The Preferences page is closed. A dialog box is displayed to confirm the successful saving of the preferences. Click **OK** to close the dialog box.

**Related
Documentation**

- [Modifying the Application Settings of Connectivity Services Director on page 1082](#)

Service Provisioning: Managing VPLS Service Orders

- [Creating a Multipoint-to-Multipoint VPLS Service Order on page 881](#)
- [Creating a Point-to-Multipoint VPLS Service Order on page 905](#)
- [Creating a Service Order for VPLS Access into Layer 3 Networks on page 930](#)
- [Creating a VPLS Service Order with CFM on page 933](#)
- [Interconnecting a VPLS Service with a Layer 3 VPN Service on page 936](#)

Creating a Multipoint-to-Multipoint VPLS Service Order

The Connectivity Services Director application implements multipoint-to-multipoint Ethernet services as virtual private LAN (VPLS) services.

To create a multipoint-to-multipoint Ethernet service order, complete these tasks in order:

1. [Selecting the Service Definition on page 881](#)
2. [Entering Service Parameters Information on page 884](#)
3. [Specifying OAM Settings on page 890](#)
4. [Selecting N-PE Devices on page 891](#)
5. [Specifying Node Settings on page 893](#)
6. [Modifying Site Settings on page 896](#)
7. [Specifying QoS Settings on page 902](#)
8. [Specifying Template Settings on page 903](#)
9. [Reviewing the Configured Settings on page 904](#)
10. [Deploying the New Service on page 905](#)

Selecting the Service Definition

To select a service definition on which to base the new service order:

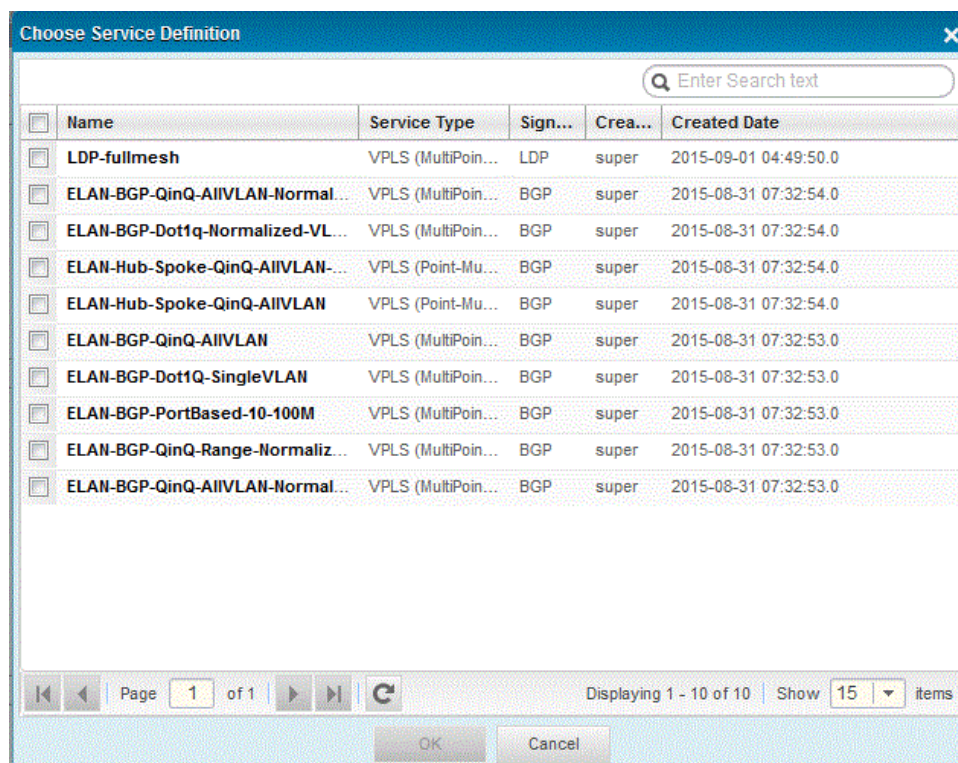
1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the View pane, click the plus sign (+) to expand the tree and select the type of service.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.

5. From the Tasks pane, select **Service Provisioning > Deploy Services**.

The Manage Network Services page is displayed in the top half of the right pane, which displays all of the configured services. The Manage Service Orders page is displayed in the bottom half of the right pane, which displays all of the service orders corresponding to a service.

6. From the Manage Network Services page, select **New > VPLS Service**.

The **Create VPLS Service Order** window appears and shows a filtered inventory view of only those published service definitions designed to work with multipoint Ethernet services. You can select the service definition based on the signaling type.



The **Service Parameters** page appears.

- From the Service Definition field, click **Select** to choose the service definition you want to base your service order on. The Choose Service Definition inventory page displays a view of only those published service definitions designed to work with the type of services you need.

Based on the fields or parameters that you defined in the service definition to be enabled for modification in the service order, the corresponding fields are available for editing. The fields that are disabled for modification in the service order can only be edited in the service definition.

- Select the check box beside the service definition that you want to associate with the service order, and click **OK**.
- Click **View** to open a popup dialog box that displays the details of the selected service definition. The service definition properties, such as the name, signaling type (LDP or BGP), service type (point-to-point pseudowire, ATM, or TDM), are displayed. The interface-specific attributes, such as rate-limiting details, encapsulation, and VLAN tags, are also displayed in the dialog box. Close the dialog box to return to the service order creation wizard.

Entering Service Parameters Information

This part of the create multipoint Ethernet service order procedure sets general information about the service order in the **Service Parameters** page of the Create VPLS Service Order wizard:

A wizard is available to create a service order in an intuitive and easily-navigable format. The settings that you can configure in the service order are organized in separate pages of the wizard, which you can launch by clicking the appropriate buttons at the top of the Create a Service Order page. Alternatively, you can proceed to the corresponding setting-related pages by clicking the **Back** and **Next** buttons at any point in the wizard during the creation of the service order.

In the General Settings section of the Service Parameters page, enter general settings or service parameters information by doing the following tasks:

The screenshot shows the 'Create VPLS Service Order' wizard with the 'Service Settings' tab selected. The 'General Settings' section contains fields for 'Name' (VPLS-SO), 'Comments', 'Customer' (amazon), and 'Service Definition' (LDP-fullmesh). The 'VPLS Settings' section has several checkboxes: 'Auto Pick Route Target' (checked), 'Auto Pick Route Distinguisher' (checked), 'Auto Pick VPLS ID' (unchecked), 'Auto Pick VPN ID' (checked), 'Auto Discovery' (checked), 'Allow L3 Access' (unchecked), 'Auto Pick Hub Route Target' (unchecked), and 'Auto Pick Spoke Route Target' (unchecked). The 'Site Settings' section includes 'MTU (bytes)' (10) and 'Normalize VLAN ID Tag' (2). At the bottom right, there are buttons for 'Back', 'Next', 'Done', and 'Cancel'.

1. In the **Name** field, type a unique name for the multipoint service.

The service order name can consist of only letters, numbers, and underscores.



NOTE: The name you specify for a VPLS service order becomes the routing-instance name in the device configuration when you deploy the service. Consequently, you cannot use any Juniper Networks keywords, for example, “bgp” or “vpls”, as the name of a service order.

2. In the **Customer** field, select the customer requesting the service. To speed your search, type the first few letters of the customer name and then select from the list.

If the customer is not in the list, you must add the customer to the database before proceeding. See *Adding a New Customer*.

3. In the **Comments** field, provide a description of the service. This description appears in information windows about the request or service instance created from the request.

The **Customer traffic type** parameter is not selectable. Its value is set in the service definition.

QoS settings are added to a service order, depending on the configuration attributes that are defined in the service templates associated with it.

In the Connectivity Settings section of the Service Parameters page, enter the connectivity information by doing the following tasks:

The **Signaling** cannot be changed in the service order.

The following check boxes are displayed based on the service definition you have selected:

- Enable PW Extension
- Enable PW Resiliency
- Allow access to L3 network

You cannot change these check boxes in the service order.

1. Specify whether the route distinguisher can be selected automatically or manually.



NOTE: You cannot edit the route distinguisher if you have not selected the **Editable in Service Order** check box in the service definition.

- To assign the route distinguisher automatically, select the **Autopick Route Distinguisher** check box.
- To assign the route distinguisher manually, clear the **Autopick Route Distinguisher** check box.

If you choose to assign the route distinguisher manually, the window expands to include the **Route distinguisher** field. In the **Route distinguisher** field, type a value. Junos Space accepts either of the following two formats:

- *prefix-number: assigned-number*

Where *prefix-number* can be any numeric value from 1 through 65,535, and *assigned-number* can be any numeric value from 0 through 2,147,483,647

- *IPV4-address: assigned-number*

Where *IPV4-address* can be any valid IPv4 address, and *assigned-number* can be any numeric value from 0 through 65,535



NOTE: The **Route distinguisher** field is available in either of the following cases:

- The **Signaling** type is BGP
- The **Signaling** type is LDP and **Auto Discovery** is enabled

2. Specify whether the route target can be selected automatically or manually.



NOTE: You cannot edit the route target if you have not selected the **Editable in Service Order** check box in the service definition.

- To assign the route target automatically, select the **Autopick Route target** check box.
- To assign the route target manually, clear the **Autopick Route target** check box.

If you choose to assign the route target manually, the window expands to include the **Route Target** field. In the **Route Target** field, type a value. Junos Space accepts either of the following two formats:

- *prefix-number:assigned-number*

Where *prefix-number* can be any numeric value from 1 through 65,535, and *assigned-number* can be any numeric value from 0 through 2,147,483,647

- *IPV4-address:assigned-number*

Where *IPV4-address* can be any valid IPv4 address, and *assigned-number* can be any numeric value from 0 through 65,535



NOTE: The **Route Target** field is available in either of the following cases:

- The Signaling type is BGP
- The Signaling type is LDP and Auto Discovery is enabled

3. In the **Revert time (sec)** field, specify the revert time for redundant Layer 2 circuits and VPLS pseudowires.

Default: 5 seconds

Range: 0 through 65,535 seconds

This field is available only if you have enabled the **Enable PW Resiliency** check box in the selected service definition.

4. In the **Switch Over Delay (sec)** field, specify the time to wait before the backup pseudowire takes over.

Default: 0 seconds

Range: 0 through 180 seconds

This field is available only if you have enabled the **Enable PW Resiliency** check box in the selected service definition.

5. If **Autopick VPLS ID** is disabled, specify the **VPLS ID**.

Range: 1 through 2147483647



NOTE: If the signaling type is LDP and if auto discovery is enabled, **Autopick VPLS ID** appears dimmed. This field is not editable in the service order.

If the signaling type is BGP, **Autopick VPLS ID** is not available.

6. If **Autopick VPN ID** is enabled, specify the **VPN ID**.

Range: 1 through 65535



NOTE: If the signaling type is LDP and if auto discovery is enabled, **Autopick VPN ID** appears dimmed. This field is not editable in the service order.

If the signaling type is BGP, **Autopick VPN ID** is not available.

7. Select the **Autopick Hub Route Target** and **Autopick Spoke Route Target** check boxes if you want the Route target chosen automatically by the Network Activate software.



NOTE: You cannot edit this field if you have not selected the **Editable in Service Order** check box in the service definition.

To manually assign a Route target:

1. Clear the **Autopick Hub Route Target** and **Autopick Spoke Route Target** check boxes to activate the **Hub Route Target** and **Spoke Route Target** fields respectively.
2. In the **Route Target** field, enter a value.

When you manually enter route target, Junos Space accepts either of the following two formats:

- *<prefix-number>: <assigned-number>*

Where *<prefix-number>* can be any numeric value from 1 to 65535, inclusive.

The *<assigned-number>* can be any numeric value from 0 to 2,147,483,647, inclusive.

- *<IPV4-address>: <assigned-number>*

Where *<IPV4-address>* can be any valid IPV4 address (in W.X.Y.Z "dot" notation), and *<assigned-number>* can be any numeric value from 0 to 65535, inclusive.

In the Default Endpoints Settings section of the Service Parameters page, enter the endpoint or device settings information by doing the following tasks:

1. Select a value for **Ethernet option**.

- **Port**
- **Dot1Q**

Specifying the **Dot1Q** Ethernet option enables you to apply a Unit ID, a single VLAN ID, a VLAN Range, or a VLAN list to the service order.

- **QinQ**

Specifying the **QinQ** Ethernet option enables you to apply a single VLAN, a VLAN Range, or a VLAN list to the service order. For an L3VPN service deployed on a dual tagged interface, the inner tag determines the VPN routing and forwarding instance(VRF).

2. In the **Bandwidth** field, select a value from the list to limit the bandwidth of the service you are creating.

This field is present only if bandwidth limiting is allowed by the service definition, and is configurable in the service order only if the service definition allows it.

3. In the **MTU** field, type the maximum transmission unit size for the UNI.

This field is present in all service orders. However, you can set this field only if the service definition allows it.

The **Auto-pick VLAN range constraint** field is displayed and validates the VLAN range specified in the service definition.

4. Specify the Logical interface settings:



NOTE: The Autopick Interface Unit ID field is not available if you have selected the Ethernet option as Port.

- Specify whether the **Autopick Interface Unit ID** can be selected automatically or manually.
 - To assign the **Unit** automatically, select the **Autopick Interface Unit ID** check box.
 - To assign the **Unit** manually, clear the **Autopick Interface Unit ID** check box.

The window expands to include the **Unit** field. In the **Unit** field, type a value.

Range: 1 through 1073741823



NOTE: You can edit this field only if you have selected the Editable in Service Order check box for the VLAN ID selection in the service definition.

- Specify whether the **Autopick VLAN ID** can be selected automatically or manually.
 - To assign the **VLAN ID** automatically, select the **Autopick VLAN ID** check box.
 - To assign the **VLAN ID** manually, clear the **Autopick VLAN ID** check box.

The window expands to include the **VLAN ID** field. In the **VLAN ID** field, type a value.

5. Select the preferred option for calculating the burst size:

- **MTU Based**

If you select the option **MTU Based**, you can specify a value for **MTU Factor** in the range 1 through 1087902.

The default value for **MTU Factor** is 10.

- **Line Rate Based**

If you select the option **Line Rate Based**, you can specify a value for **Burst Period** in the range 1 through 7450 milliseconds.

The default value for **Burst Period** is 1.

6. In the **Customer VLAN Range Start** and **Customer VLAN Range End** fields, type the first and last VLAN ID of the range of customer VLANs to be transported over the network.

These fields are present only for services with UNIs that have Q-in-Q interface types and allow a range of VLANs to be transported.

7. In the **Normalize - VLAN ID Tag** field, type a value for the customer VLAN.

This field is present only for services that specify Normalize to Dot1q tags.

8. In the **Normalize - Inner VLAN Tag (for QinQ)** field, type a value to provide a default inner VLAN tag for the UNI endpoints.

This field is present only for services that specify Normalize to QinQ tags.

9. In the **Normalize - Outer VLAN Tag** field, type a value to provide an outer VLAN tag that matches the Outer VLAN tag of at least one of the UNI endpoints.

This field is present only for services that specify Normalize to QinQ tags.

10. Click **Next** to proceed to the subsequent step of the wizard, which is to define the node or endpoint parameters.

Specifying OAM Settings

To enable OAM on the service definition, type information in the OAM Settings of the Service Parameters page of the wizard.

1. In the **OAM Profile** field, select a profile from the list.



NOTE: For OAM Settings, if you specify a CFM profile (for example, a CFM action profile with remote MEP), or an SLA-Iterator profile, first you must ensure that the profile is attached to the same device upon which you intend to deploy the P2P service order. If the profile is not previously attached (using the OAM Insight application), it will not be present on the device to support the service order.

To remove a previously associated CFM definition or OAM profile from a service definition, click the **Detach** button next to the OAM Profile field to remove the association. To associate a new OAM profile, you must dissociate the existing OAM profile and attach a fresh OAM profile. Detaching an OAM profile is enabled when you modify a service or service order.



NOTE: For Juniper Networks PTX3000 Packet Transport Routers and Junos Space Release 13.1P1, if you attach a CFM Definition to the service order, the CFM session will operate for MEPs in either the Up or Down direction when the service is deployed.

2. Click **CFM Details** beside the OAM Profile field to view the profile configuration details in a dialog box.
3. Continue with specifying the endpoint information.

Selecting N-PE Devices

This part of the create multipoint Ethernet service order procedure selects the N-PE devices. The selection is made from the **Node Parameters** page of the Create VPLS Service Order wizard.

If there is a service template attached to the service definition, there is a link to that template at the bottom of the **Node Parameters** section of the window. For instructions on working with service templates in service orders, see [“Creating a Service Order Based on a Service Definition with a Template” on page 990](#).



NOTE: The **Choose Endpoints** window shows only assigned NPE devices that have an AS number configured. If you do not see the device you are looking for, use the CLI on the device to check for and assign an AS number.

Figure 41: Choose Endpoints Dialog Box

Name	IP Address	State	Managed State	Platform	OS Version	Roles
<input checked="" type="checkbox"/> 960R2_EP_Alok_re	10.216.194.110	up	In Sync	MX960	14.2-20140916.0	N_PE
<input type="checkbox"/> 480R4_EP_Alok_re	10.216.194.105	up	In Sync	MX480	14.2-20140916.0	N_PE
<input type="checkbox"/> 480R3_EP_Alok_re	10.216.194.108	up	In Sync	MX480	14.2-20140916.0	N_PE
<input type="checkbox"/> 960R1_EP_Alok_re	10.216.194.118	up	In Sync	MX960	14.2-20140916.0	N_PE
<input type="checkbox"/> RouterZ-re	10.92.35.185	down	In Sync	MX960	15.1-20141022_L...	N_PE
<input type="checkbox"/> RouterY-re	10.92.35.187	up	In Sync	MX960	15.1-20141022_L...	N_PE
<input type="checkbox"/> RouterX-re	10.92.35.189	up	In Sync	MX960	15.1-20141022_L...	N_PE
<input type="checkbox"/> RouterXCore-re	10.92.35.183	down	In Sync	MX960	15.1-20141022_L...	-
<input type="checkbox"/> Merg1_006_re	10.92.37.13	up	In Sync	MX960	15.1-20150727_...	N_PE

Page 1 of 3 Displaying 1 - 9 of 25 Show 9 items

Name	Status	Encapsulation	Index
ae0	down	none	508
ae1	down	none	509
em1	up	none	23
em2	up	none	116
ge-0/0/2	up	flexible-ethernet-services	533
ge-0/0/3	up	flexible-ethernet-services	539
ge-0/0/4	up	flexible-ethernet-services	542
ge-0/0/5	up	none	550
ge-0/0/6	up	none	551
ge-0/0/7	up	none	552
ge-0/0/8	up	none	553
ge-0/0/9	up	none	554

To select endpoint N-PE devices:

1. In the **Node Parameters** page, click **Add** in the Service Nodes table. From the Choose Endpoints dialog box that appears, select the devices that you want to participate in the service. Use the multiple selection feature to select one or more devices.



NOTE: In the Choose Endpoints dialog box, you can sort and segregate the devices and their corresponding interfaces based on the roles of the devices to easily and quickly view only the devices of interest. Click the down arrow on the Filter Role menu, and select P2E to view only the provider edge devices, P to view only the provider devices, and L2E to view only Layer 2 Ethernet devices.

2. Based on the devices you select in the top half of the dialog box, the interfaces that are present in the selected device are displayed in the lower half of the dialog box.

Select the check boxes next to the interfaces that you want to associate with the service.

3. Click **OK**.

The **Node Parameters** window appears.

4. Continue with modifying or entering the node parameters.

Specifying Node Settings

This part of the create multipoint Ethernet service order procedure sets the attributes that are usually common for all endpoints in the service.



NOTE: If you are using a definition with multiple templates, you can set different attributes for the endpoints.

In any case, the values that you type depend on the service definition on which the service order is based. Follow the steps in one of the following tasks, depending on whether or not the service provides flexible VLAN tagging. To create a service with flexible VLAN tagging, the service definition that you selected for the service order must include the Ethernet option **asymmetric tag depth** in the UNI settings step.

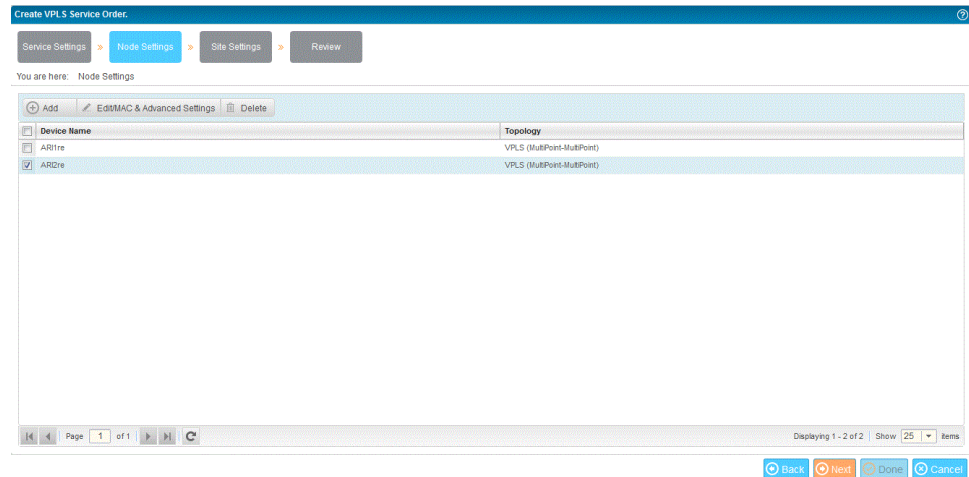
- [Setting Attributes for Nodes or Devices on a Service on page 893](#)
- [Setting Attributes for Nodes or Devices on a Service with Flexible VLAN Tagging on page 896](#)

Setting Attributes for Nodes or Devices on a Service

If these attributes are not the same on all endpoints, you can set them to be the same for now and then make changes later, or you can choose to skip this step and apply the attribute values one at a time later, or use a definition with multiple templates.

This procedure sets the attributes listed in the Node Settings page of the of the Create VPLS Service Order wizard. The attributes shown depend on the interface type and the signaling type.

The Node Settings page displays configuration attributes for the device selected in the table of all added nodes. If multiple devices are selected, data is displayed beneath the table for the last selected device. If you do not select a device, the service definition details for nodes are displayed.



To set attributes common to most endpoints:

1. Fill in the following fields under the MAC Settings section

Field	Action
MAC Settings	
MAC learning	To enable MAC learning , select the check box.
Interface MAC limit	Maximum number of MAC addresses learned from an interface. Range: 1 through 131071 MAC addresses per interface
MAC statistics	To enable MAC statistic , select the check box.
MAC Table Size	Modify the size of the MAC address table for the bridge domain. Range: 16 through 1048575 To allow the service provisioner to override the MAC settings, select Editable in Service Order .

2. Fill in the following fields under the Topology Settings section.

- a. In the Topology field, the type of network connection or circuit is displayed as Full Mesh (Multipoint-to-Multipoint) or Hub-Spoke (Point to Multipoint), based on the type of service definition selected. In this case, the topology is shown as multipoint-to-multipoint.
- b. Define a route distinguisher option from the **Auto Pick Route Distinguisher** check box and **Route Distinguisher** field:
 - Select the check box to enable the service provider to specify the route distinguisher.

- Select the check box to enable the route distinguisher to be selected automatically.

3. Fill in the following fields under the Advanced Settings section.

Advanced Settings—This section enables you to specify the parameters that define advanced connectivity between sites across the service provider network. Configuring advanced settings is optional. You can click on the Advanced link to view the default values for Advanced Settings. If the advanced settings can be edited in the service order, you can override the default values. If you do not click the Advanced link, the default advanced settings are applied to the service order.

Include	<p>Select the Include check box for each advanced setting that you want to include in the service definition.</p> <p>NOTE: If you select any advanced parameters for a service definition, you must also select the Include check box for the Disable tunnel services parameter, and select or clear the Disable tunnel services check box.</p> <p>For MX Series devices, if you deploy a VPLS service without selecting the Include check box for Disable tunnel services parameter, the VPLS service is down. As a work around, you can push the configuration to each PE device for the service by running the following command:</p> <pre>root@test_device# set chassis fpc 0 pic 1 tunnel-services bandwidth 1g</pre>
Disable Tunnel Services	<p>Enable or disable tunnel-services to specify that traffic for particular VPLS routing instances be forwarded to specific virtual tunnel (VT) interfaces.</p> <ul style="list-style-type: none"> • To enable tunnel-services, clear the Disable Tunnel Services check box. • To disable tunnel-services, select the Disable Tunnel Services check box (default).
Disable Local Switching	<p>Enable or disable local switching. In local switching mode, you can terminate multiple Layer 2 circuit pseudowires at a single VPLS mesh group:</p> <ul style="list-style-type: none"> • To enable local switching across the network, clear the Disable Local Switching check box. • To disable local switching across the network, select the Disable Local Switching check box (default).
Fast Reroute-Priority	<p>In this drop-down list, specify the reroute priority for a VPLS routing instance:</p> <ul style="list-style-type: none"> • HIGH—Set the fast reroute priority for a VPLS routing instance to high. During a fast reroute event, the router repairs next hops for high-priority VPLS routing instances first. • MEDIUM—Set the fast reroute priority for a VPLS routing instance to medium. During a fast reroute event, the router repairs next hops for medium-priority VPLS instances after high-priority VPLS routing instances but before low-priority VPLS routing instances. • LOW—Set the fast reroute priority for a VPLS routing instance to low, which is the default. During a fast reroute event, the router repairs next hops for low-priority VPLS routing instances last.
Label Block Size	<p>Configure the label block size for VPLS labels by using one of the following values.</p> <ul style="list-style-type: none"> • 2—Allocate the label blocks in increments of 2. Use this setting for a VPLS domain that has only two sites with no future expansion plans. • 4—Allocate the label blocks in increments of 4. • 8—Allocate the label blocks in increments of 8. This is the default. • 16—Allocate the label blocks in increments of 16. A label block size of 16 enables you to minimize the number of routes in the VPLS domain. Use this setting only if the number of routes is the primary concern. <p>NOTE: This field is unavailable if the Signaling type is LDP and the Auto discovery check box is enabled.</p>

Connectivity type

Select a connection-type to specify when a VPLS connection is taken down, depending on whether the interface for the VPLS routing instance is customer-facing or integrated routing and bridging (IRB):

- **ce**—Require that for the VPLS connection to be up, the customer-facing interface for the VPLS routing instance must also be up. If the customer-facing interface fails, the VPLS connection is taken down. This is the default.
- **irb**—Allow a VPLS connection to remain up so long as an IRB interface is configured for the VPLS routing instance.

NOTE: This field is unavailable if the **Signaling** type is LDP and the **Auto discovery** is enabled.

4. Click **Next**.

The **Site Settings** page of the Create VPLS Service Order wizard appears.

5. Continue with specifying the UNI or interface settings.

Setting Attributes for Nodes or Devices on a Service with Flexible VLAN Tagging

A service with flexible VLAN tagging can include port-based, 802.1Q, and Q-in-Q interfaces.

If these attributes are not the same on all endpoints, you can set them to be the same for now and then make changes later, or you can choose to skip this step and apply the attribute values one at a time later, or you can use a definition with multiple templates.

If there is a service template attached to the service definition, there is a link to that template at the bottom of the **Node Settings** page of the wizard. For instructions on working with service templates in service orders, see *Changes in Behavior and Syntax*.

This procedure sets the attributes listed in the Node Settings page of the of the Create VPLS Service Order wizard. The attributes shown depend on the signaling type and interface type. The following example shows the endpoints settings box for a multipoint-to-multipoint service with flexible VLAN tagging that transports a single VLAN and specifies Normalize to Dot1Q tag.

Modifying Site Settings

This part of the create multipoint Ethernet service order procedure sets the attributes for each interface of an endpoint or a device in the service. Selection is made using the **Site Settings** page of the wizard that enables you to create a VPLS service order.

This window shows one interface for each device that you selected from the **Choose Endpoints** dialog box of the Node Settings page, as described in [“Selecting N-PE Devices” on page 891](#).

The Site Settings page enables you to select a device to add interfaces for that device. You can select multiple interfaces for the device. If the Enable L3 Access check box is enabled, the UNI lists available integrated routing and bridging (IRB) interfaces for the selected device. If the device role is a P2P spoke, you can select one UNI and it is required for such devices. If Ethernet Option is set as port-to-port, the UNI can be added only once as an endpoint for the device.

The interface shown in the **UNI Interface** field is automatically selected by the Connectivity Services Director application, which chooses the UNI that has the highest available capacity among interfaces that are in the Up state. To calculate the available capacity of the interface, the system subtracts the bandwidth reserved for each service deployed on that interface from the total capacity of the interface.

For each endpoint, the **Site Settings** page shows the following value for each UNI attribute:

- For port-to-port services, the displayed values are Bandwidth and MTU.
- For 802.1Q UNIs, the displayed attributes are Bandwidth, AutoPick VLAN ID, VLAN ID, and MTU.
- For Q-in-Q UNIs, the displayed attributes include Bandwidth, AutoPick VLAN ID, and VLAN ID. For a service with Q-in-Q UNIs that specifies a customer VLAN range, the displayed attributes also include C-VLAN ID Start and C VLAN End.

For each endpoint on a service with flexible VLAN tagging, the Endpoint Settings window shows the following value for each UNI attribute:

- For a service with flexible VLAN tagging that transports a single VLAN and specifies Normalize to Dot1q tags, the displayed attributes include Ethernet Option, Bandwidth, AutoPick VLAN ID, Inner VLAN ID, and MTU. For a service with flexible VLAN tagging that specifies a customer VLAN range, the displayed attributes also include C-VLAN ID Start and C VLAN End.

- For a service with flexible VLAN tagging that transports a single VLAN and specifies Normalized to QinQ tags, the displayed attributes include Bandwidth, AutoPick VLAN ID, and VLAN ID. For a service with flexible VLAN tagging that specifies a customer VLAN range, the displayed attributes also include C-VLAN ID Start and C VLAN End.
- For a service with flexible VLAN tagging that transports a VLAN range, the displayed attributes include Bandwidth, AutoPick VLAN ID, and VLAN ID. For a service with flexible VLAN tagging that specifies a customer VLAN range, the displayed attributes also include C-VLAN ID Start and C VLAN End.

The values shown are initially the values you set earlier on the Service Parameters page of the creation of VPLS service order wizard, as described in [“Specifying Node Settings” on page 893](#).

To add a UNI and specify its settings:

1. Click the **Add** icon at the top of the User-to-Network Interfaces table. The Choose Endpoints dialog box is displayed.

Figure 42: Choose Endpoints Dialog Box

Choose Endpoints

Filter Role: [v] Enter Search text

<input type="checkbox"/>	Name	IP Address	State	Managed State	Platform	OS Version	Roles
<input checked="" type="checkbox"/>	960R2_EP_Alok_re	10.216.194.110	up	In Sync	MX960	14.2-20140916.0	N_PE
<input type="checkbox"/>	480R4_EP_Alok_re	10.216.194.105	up	In Sync	MX480	14.2-20140916.0	N_PE
<input type="checkbox"/>	480R3_EP_Alok_re	10.216.194.108	up	In Sync	MX480	14.2-20140916.0	N_PE
<input type="checkbox"/>	960R1_EP_Alok_re	10.216.194.118	up	In Sync	MX960	14.2-20140916.0	N_PE
<input type="checkbox"/>	RouterZ-re	10.92.35.185	down	In Sync	MX960	15.1-20141022_i...	N_PE
<input type="checkbox"/>	RouterY-re	10.92.35.187	up	In Sync	MX960	15.1-20141022_i...	N_PE
<input type="checkbox"/>	RouterX-re	10.92.35.189	up	In Sync	MX960	15.1-20141022_i...	N_PE
<input type="checkbox"/>	RouterXCore-re	10.92.35.183	down	In Sync	MX960	15.1-20141022_i...	-
<input type="checkbox"/>	Merg1_006_re	10.92.37.13	up	In Sync	MX960	15.1-20150727_...	N_PE

Page 1 of 3 Displaying 1 - 9 of 25 Show 9 items

<input type="checkbox"/>	Name	Status	Encapsulation	Index
<input type="checkbox"/>	ae0	down	none	508
<input type="checkbox"/>	ae1	down	none	509
<input type="checkbox"/>	em1	up	none	23
<input type="checkbox"/>	em2	up	none	116
<input type="checkbox"/>	ge-0/0/2	up	flexible-ethernet-services	533
<input type="checkbox"/>	ge-0/0/3	up	flexible-ethernet-services	539
<input type="checkbox"/>	ge-0/0/4	up	flexible-ethernet-services	542
<input type="checkbox"/>	ge-0/0/5	up	none	550
<input type="checkbox"/>	ge-0/0/6	up	none	551
<input type="checkbox"/>	ge-0/0/7	up	none	552
<input type="checkbox"/>	ge-0/0/8	up	none	553
<input type="checkbox"/>	ge-0/0/9	up	none	554

OK Cancel

2. Select the check box next to the endpoint or device from which you want to add a UNI to the service order. After you select the check box, the view refreshes to display the configured interfaces for that corresponding device in the lower part of the dialog box



NOTE: In the Choose Endpoints dialog box, you can sort and segregate the devices and their corresponding interfaces based on the roles of the devices to easily and quickly view only the devices of interest. Click the down arrow on the Filter Role menu, and select P2E to view only the provider edge devices, P to view only the provider devices, and L2E to view only Layer 2 Ethernet devices.

3. Based on the devices you select in the top half of the dialog box, the interfaces that are present in the selected device are displayed in the lower half of the dialog box. Select the check boxes next to the interfaces that you want to associate with the service.
4. Click **Add** to save the settings, and click **Close** to exit from the dialog box. You are returned to the Site Settings page.
5. For a service with flexible VLAN tagging, set the interface type in the Ethernet Option column for each endpoint in the service.
6. To select a different UNI on a device, from the **User-to-Network Interfaces** section, click the UNI name you want to change and choose another interface from the list.

7. Select the **Enable CFM** check box beside a particular interface of a device in the service order creation and modification wizards to enable connectivity fault management (CFM) on the interface. Based on your network needs, you can create a point-to-multipoint and a multipoint-to-multipoint VPLS service with service-level CFM enabled. The CFM profile is propagated to a single endpoint when multiple interfaces are selected for a given device (the last interface overrides the other configurations). When you select the **Enable CFM** check box for an interface of a particular device, you cannot enable CFM on other interfaces of the same device. The CFM configuration is pushed only on the selected interface.

When you delete the interface with CFM enabled, the CFM configuration on the particular device is also removed. When you attempt to delete an interface with CFM enabled, you are prompted to confirm the deletion.

8. In the **Customer VLAN Range Start** and **Customer VLAN Range End** fields, type the first and last VLAN ID of the range of customer VLANs to be transported over the network. These fields are present only for services with UNIs that have Q-in-Q interface types and allow a range of VLANs to be transported.

9. Select a value for **Ethernet option**.

- **Port**
- **Dot1Q**

Specifying the **Dot1Q** Ethernet option enables you to apply a Unit ID, a single VLAN ID, a VLAN Range, or a VLAN list to the service order.

- **QinQ**

Specifying the **QinQ** Ethernet option enables you to apply a single VLAN, a VLAN Range, or a VLAN list to the service order. For an L3VPN service deployed on a dual tagged interface, the inner tag determines the VPN routing and forwarding instance(VRF).

10. To enter the description for an UNI interface, click the corresponding **Description** cell.

11. To change the bandwidth on an endpoint, click the bandwidth value for the endpoint and select another value from the list.
12. The **AutoPick Interface Unit ID** and the **Unit ID** columns appear, if you have not selected the **Ethernet option** as port-to-port.
 - To change an automatically selected service UNIT ID to manual selection, clear the **AutoPick Interface Unit ID** check box, and type a service UNIT ID value in the **Unit ID** field.
 - To change from manual selection to automatic selection, select the **AutoPick Interface Unit ID** check box.
 - To change the value of a manually selected service Unit ID, type a new value in the **Unit ID** field.



NOTE: The unit ID value that you have specified in the Enter Order Information page is displayed in the Unit ID field.

13. For Q-in-Q interface endpoints, you can change how the service VLAN ID is selected:
 - To change an automatically selected service VLAN ID to manual selection, clear the **AutoPick VLAN ID** check box, and type an VLAN ID value in the **VLAN ID** field.
 - To change from manual selection to automatic selection, select the **AutoPick VLAN ID** check box.
 - To change the value of a manually selected service VLAN ID, type a new value in the **VLAN ID** field.
14. For Q-in-Q interface endpoints with customer VLAN ranges specified, you can also change the range limits for an endpoint.
15. For 802.1Q interface endpoints, you can change the customer VLAN ID.
16. To change the MTU for the UNI, click the value in the **MTU** field and type a new value.
17. To add a UNI on a selected device, click **Add** to open the Choose Endpoints dialog box and then select the interface you want from the UNI interface list.
18. If the interface you selected in the previous step is already configured (duplicate) you must either type a different value in the **VLAN ID** field manually, or check the **Autopick VLAN ID** field.
19. To delete a UNI from a device, select the interface and click **Delete** in the table that displays the UNIs.

If the deleted UNI is the only UNI selected from the device, then the device is deleted from the service configuration.

20. When you have finished modifying the endpoint settings, click **Review** to examine and modify the settings.

The screenshot shows the 'Create VPLS Service Order' wizard in the 'Review' step. At the top, there are four tabs: 'Service Settings', 'Node Settings', 'Site Settings', and 'Review'. The 'Review' tab is active. Below the tabs, a breadcrumb trail reads 'You are here: Review'. The main content area is titled 'Service Settings' and contains three sections: 'General Settings', 'Connectivity Settings', and 'OAM Settings'. The 'General Settings' section includes fields for 'Service Order Name' (VPLS-SO), 'Customer Name' (amazon), 'Customer ID' (688244), 'Policy Name' (LDP-fullmesh), 'Policy ID' (1212416), and 'Service Type' (VPLS(LDP)). The 'Connectivity Settings' section includes 'Auto-Pick VPN ID' (true), 'Auto pick Route' (true), 'Distinguisher' (true), 'Auto pick Route Target' (true), 'AllowAccessToL3Network' (false), 'Enable PW Extension' (false), and 'Enable PW Resiliency' (false). The 'OAM Settings' section includes 'Default Settings' and 'Normalize VLAN ID Tag' (2). At the bottom right, there are four buttons: 'Back', 'Next', 'Done', and 'Cancel'.

21. For service orders associated with a service definition that contains a service template, click **Next** to modify the template settings.
22. Click **Finish** when you have completed examining the settings to confirm the creation of the service order.
23. You can proceed with deploying the service.

Specifying QoS Settings

CoS profiles enable the grouping of class-of-service (CoS) parameters and apply them to one or more interfaces. Connectivity Services Director provides you with predefined traffic types for each CoS profile that you create. These traffic types represent the most common types of traffic for the device type. Each of these templates has preconfigured values for all CoS parameters based on the typical application requirements. You can change the preconfigured values of these parameters to suit your requirements. To display the CoS Profiles page, in Build mode, select CoS under Profile and Configuration Management in the Tasks pane. The Manage CoS Profiles page appears.

If QoS is enabled on the service definition, configure the QoS Settings of the Site Settings panel of the service order creation wizard.

1. In the **QoS profile** field, select a profile from the list.

The **QoS profile** list displays the QoS profiles that are currently configured in the Manage CoS Profiles page of the Connectivity Services Director application.

A QoS profile classifies traffic into defined service groups to provide the special treatment of traffic across the network service.

Specifying Template Settings

The Template Settings page of the service order creation and modification wizards enables you to associate service templates with a point-to-point, VPLS, and Layer 3 VPN service order. You can apply only the templates that are previously configured in a service definition with the corresponding service order. The Template Settings page is available in the service order wizard only if the service definition that you selected to apply to the service order contains a service template. Otherwise, the Template Settings page is not displayed in the service order wizard. You can perform template operations for all endpoints in a service order.

If you defined a service template as the default service template, it is attached to the endpoint by default. You have the flexibility to create and provision a dynamic attribute in a service template. You can mark an attribute of a service template as dynamic, and you can obtain the values for these dynamic attributes from a specific device. To create a dynamic attribute, you must first mark an attribute of a service template as dynamic and then specify the device XPath for the dynamic attribute.

The Template Settings page is displayed before the Review page, which is the final step of the service order wizard.

In the Service Settings page of the Select Service Definition field of the service order creation wizard, you can double-click a service definition name displayed in the table to view the details of the definition in a popup dialog box. You can use this information to determine if the service definition is appropriate for your deployment needs. To filter and sort the display of service templates, enter the name of the template as a match criterion in the Search box and click the Search icon. The page refreshes to display only the template names that match with the search term. You can use the paging controls to navigate across multiple pages of templates as necessary.

All the tasks that you can perform with service templates are presented in the Template Settings page. The page is divided into three panes. The top half of the page displays a table of selected endpoints. All the endpoints or UNIs that you selected in the preceding pages of the service order wizard are displayed in this table. You can configure the template pertaining to only one endpoint at a point in time. If the selected endpoints (in previous pages of the wizard) contained a manually-entered unit number, that number is displayed in the table of selected endpoints. Otherwise, the Auto-pick label is displayed.

The lower half of the page is divided into two panes. The left pane displays the template selection table for the endpoint you selected. All the templates associated with the service definition are displayed. You can add and delete templates using the template selection table. The right pane displays all the parameters that you can modify for a selected service template. All such editable parameters are displayed in a consolidated

form of a configuration page. This pane is displayed after you select a template. If any configuration parameter in template is set as a service-specific value, such attributes are not displayed in this pane.

To associate a service template with a service order:

1. Click **Add** to include a service template for the endpoint. A dialog box is displayed with the list of service templates associated with the service definition that is used to create the service order. The templates selected in this dialog box are displayed in the Template Selection table for the specified endpoint. Such templates are considered to be attached to that endpoint.

If you specified a template as a default template during the service definition creation, the template is displayed by default in the template selection table. You can associate non-default templates with the service order by clicking the **Add** button.

2. Click the link in the template name to open the Template Details dialog box. The template settings are displayed in the popup dialog box. For the selected template, the Configuration Page is displayed in the lower-right pane of the Template Settings page.
3. Modify any template-specific service components as necessary.
4. Click **Save** to submit the changes.
5. Select a template from the Template Selection table, and click **Delete** to remove the template from being associated with the service order for a particular endpoint.

Reviewing the Configured Settings

The Review page of the service definition or service order creation and modification wizards enable you to view and evaluate the service parameters and components you configured in preceding steps or pages of the wizard. This page provides a comprehensive, single-page view of all the service elements configured in the different pages of the wizard. You can either click the buttons corresponding to the various settings at the top of the wizard page to directly traverse to the page you want to modify or click the navigation buttons at the bottom of the wizard page to go to the different pages of the wizard.



NOTE: On the Review page, in the Service Templates section, the names of the service templates with which the service definition is associated are displayed. The Default Service Template column indicates whether the attached template is the default template.

To examine the configured service settings:

1. Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify.
2. Click **Edit** next to the section that contains the parameter you want to modify. You are navigated to the corresponding page of the wizard in which the parameter settings are defined.
3. Click **Finish** to save the service definition or service order.
4. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

The service order inventory window appears.

Deploying the New Service

This part of the create multipoint Ethernet service order procedure deploys the service.

To deploy the service from the **Manage Deploy Services** window:

1. Perform one of the following actions in the Deploy mode of the Service View of Connectivity Services Director:
 - To deploy the service immediately, select **Deploy now**, then click **OK**.
 - To deploy the service later, select **Schedule deployment**, select a date and time, then click **OK**.

The time field specifies the time kept by the server, but in the time zone of the client.
2. To monitor the status of the deployment, use the Jobs workspace.

The service order is now complete.

The **Manage Service Orders** page shows the service order you just added.

Related Documentation

- [Creating a Point-to-Multipoint VPLS Service Order on page 905](#)
- [Creating a Service Order for VPLS Access into Layer 3 Networks on page 930](#)

Creating a Point-to-Multipoint VPLS Service Order

The Connectivity Services Director application implements point-to-multipoint Ethernet services as virtual private LAN (VPLS) services. These services are also referred to as hub-and-spoke services.

To create a point-to-multipoint Ethernet service order, complete the following tasks in order:

- [Selecting the Service Definition on page 906](#)
- [Entering Service Parameters Information on page 909](#)
- [Specifying OAM Settings on page 915](#)
- [Selecting N-PE Devices on page 916](#)
- [Specifying Node Settings on page 918](#)
- [Modifying Site Settings on page 922](#)
- [Specifying QoS Settings on page 927](#)
- [Specifying Template Settings on page 928](#)
- [Reviewing the Configured Settings on page 929](#)
- [Deploying the New Service on page 930](#)

Selecting the Service Definition

To select a service definition on which to base the new service order:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the View pane, click the plus sign (+) to expand the tree and select the type of service.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
5. From the Tasks pane, select **Service Provisioning > Deploy Services**.

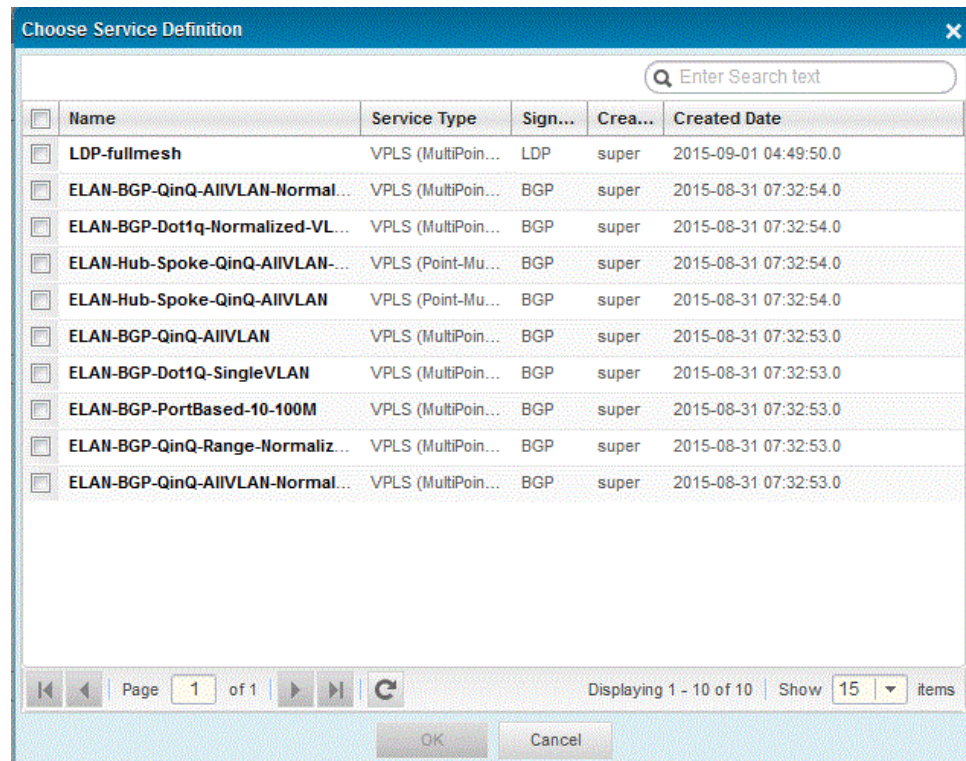
The Manage Network Services page is displayed in the top half of the right pane, which displays all of the configured services. The Manage Service Orders page is displayed in the bottom half of the right pane, which displays all of the service orders corresponding to a service.

Figure 43: Manage Service Orders Page

The image shows a 'Confirmation' dialog box with a blue header. The main text reads 'Confirm Delete partial configuration of' followed by a text field containing 'ldp_fm_test1'. Below this is a section titled 'Deployment Options:' containing two radio buttons: 'Partial Delete Now' (which is selected) and 'Partial Delete Later'. Under these options are two input fields: 'Date:' with the value '2015-08-31' and 'Time:' with a dropdown arrow. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

6. From the **Manage Network Services** page, select **New > VPLS Service**.

The **Create VPLS Service Order** window appears and shows a filtered inventory view of only those published service definitions designed to work with point-to-multipoint Ethernet services. You can select the service definition based on the signaling type.



The **Service Parameters** page appears.

- From the Service Definition field, click **Select** to choose the service definition you want to base your service order on. The Choose Service Definition inventory page displays a view of only those published service definitions designed to work with the type of services you need.

Based on the fields or parameters that you defined in the service definition to be enabled for modification in the service order, the corresponding fields are available for editing. The fields that are disabled for modification in the service order can only be edited in the service definition.

- Select the check box beside the service definition that you want to associate with the service order, and click **OK**.
- Click **View** to open a popup dialog box that displays the details of the selected service definition. The service definition properties, such as the name, signaling type (LDP or BGP), service type (point-to-point pseudowire, ATM, or TDM), are displayed. The interface-specific attributes, such as rate-limiting details, encapsulation, and VLAN tags, are also displayed in the dialog box. Close the dialog box to return to the service order creation wizard.

If a template is attached to the service definition on which the service order is based, you can invoke the template editor from the Template page of the wizard.

Entering Service Parameters Information

This part of the create point-to-multipoint Ethernet service order procedure sets general information about the service order in the **Service Parameters** page of the Create VPLS Service Order wizard:

The screenshot shows the 'Create VPLS Service Order' wizard, specifically the 'Service Settings' page. The wizard has four steps: Service Settings, Node Settings, Site Settings, and Review. The 'Service Settings' step is currently active. It contains three main sections: General Settings, VPLS Settings, and Site Settings. The General Settings section includes fields for Name (VPLS-SO), Comments, Customer (amazon), and Service Definition (LDP-fullmesh). The VPLS Settings section includes checkboxes for Auto Pick Route Target, Auto Pick Route Distinguisher, Auto Pick VPLS ID, Auto Pick VPN ID, Auto Discovery, Allow L3 Access, Auto Pick Hub Route Target, and Auto Pick Spoke Route Target. The Site Settings section includes fields for MTU/Fragment (10) and Normalize VLAN ID Tag. Navigation buttons (Back, Next, Done, Cancel) are located at the bottom right of the page.

A wizard is available to create a service order in an intuitive and easily-navigable format. The settings that you can configure in the service order are organized in separate pages of the wizard, which you can launch by clicking the appropriate buttons at the top of the Create a Service Order page. Alternatively, you can proceed to the corresponding setting-related pages by clicking the **Back** and **Next** buttons at any point in the wizard during the creation of the service order.

In the General Settings section of the Service Parameters page, enter general settings or service parameters information by doing the following tasks:

1. In the **Name** field, type a unique name for the multipoint service.

The service order name can consist of only letters, numbers, and underscores.



NOTE: The name you specify for a VPLS service order becomes the routing-instance name in the device configuration when you deploy the service. Consequently, you cannot use any Juniper Networks keywords, for example, “bgp” or “vpls”, as the name of a service order.

2. In the **Customer** field, select the customer requesting the service. To speed your search, type the first few letters of the customer name and then select from the list.

If the customer is not in the list, you must add the customer to the database before proceeding. See [“Adding a New Customer” on page 737](#).

3. In the **Comments** field, provide a description of the service. This description appears in information windows about the request or service instance created from the request.

The **Customer traffic type** parameter is not selectable. Its value is set in the service definition.

QoS settings are added to a service order, depending on the configuration attributes that are defined in the service templates associated with it.

In the Connectivity Settings section of the Service Parameters page, enter the connectivity information by doing the following tasks:

The **Signaling** cannot be changed in the service order.

The following check boxes are displayed based on the service definition you have selected:

- Enable PW Extension
- Enable PW Resiliency
- Allow access to L3 network

You cannot change these check boxes in the service order.

1. Specify whether the route distinguisher can be selected automatically or manually.



NOTE: You cannot edit the route distinguisher if you have not selected the **Editable in Service Order** check box in the service definition.

- To assign the route distinguisher automatically, select the **Autopick Route Distinguisher** check box.
- To assign the route distinguisher manually, clear the **Autopick Route Distinguisher** check box.

If you choose to assign the route distinguisher manually, the window expands to include the **Route distinguisher** field. In the **Route distinguisher** field, type a value. Junos Space accepts either of the following two formats:

- *prefix-number: assigned-number*

Where *prefix-number* can be any numeric value from 1 through 65,535, and *assigned-number* can be any numeric value from 0 through 2,147,483,647

- *IPV4-address: assigned-number*

Where *IPV4-address* can be any valid IPv4 address, and *assigned-number* can be any numeric value from 0 through 65,535



NOTE: The **Route distinguisher** field is available in either of the following cases:

- The **Signaling** type is BGP
- The **Signaling** type is LDP and **Auto Discovery** is enabled

2. Specify whether the route target can be selected automatically or manually.



NOTE: You cannot edit the route target if you have not selected the **Editable in Service Order** check box in the service definition.

- To assign the route target automatically, select the **Autopick Route target** check box.
- To assign the route target manually, clear the **Autopick Route target** check box.

If you choose to assign the route target manually, the window expands to include the **Route Target** field. In the **Route Target** field, type a value. Junos Space accepts either of the following two formats:

- *prefix-number:assigned-number*

Where *prefix-number* can be any numeric value from 1 through 65,535, and *assigned-number* can be any numeric value from 0 through 2,147,483,647

- *IPv4-address:assigned-number*

Where *IPv4-address* can be any valid IPv4 address, and *assigned-number* can be any numeric value from 0 through 65,535



NOTE: The **Route Target** field is available in either of the following cases:

- The Signaling type is BGP
 - The Signaling type is LDP and Auto Discovery is enabled
-

3. In the **Revert time (sec)** field, specify the revert time for redundant Layer 2 circuits and VPLS pseudowires.

Default: 5 seconds

Range: 0 through 65,535 seconds

This field is available only if you have enabled the **Enable PW Resiliency** check box in the selected service definition.

4. In the **Switch Over Delay (sec)** field, specify the time to wait before the backup pseudowire takes over.

Default: 0 seconds

Range: 0 through 180 seconds

This field is available only if you have enabled the **Enable PW Resiliency** check box in the selected service definition.

5. If **Autopick VPLS ID** is disabled, specify the **VPLS ID**.

Range: 1 through 2147483647



NOTE: If the signaling type is LDP and if auto discovery is enabled, **Autopick VPLS ID** appears dimmed. This field is not editable in the service order.

If the signaling type is BGP, **Autopick VPLS ID** is not available.

6. If **Autopick VPN ID** is enabled, specify the **VPN ID**.

Range: 1 through 65535



NOTE: If the signaling type is LDP and if auto discovery is enabled, **Autopick VPN ID** appears dimmed. This field is not editable in the service order.

If the signaling type is BGP, **Autopick VPN ID** is not available.

7. Select the **Autopick Hub Route Target** and **Autopick Spoke Route Target** check boxes if you want the Route target chosen automatically by the Network Activate software.



NOTE: You cannot edit this field if you have not selected the **Editable in Service Order** check box in the service definition.

To manually assign a Route target:

1. Clear the **Autopick Hub Route Target** and **Autopick Spoke Route Target** check boxes to activate the **Hub Route Target** and **Spoke Route Target** fields respectively.
2. In the **Route Target** field, enter a value.

When you manually enter route target, Junos Space accepts either of the following two formats:

- *<prefix-number>: <assigned-number>*

Where *<prefix-number>* can be any numeric value from 1 to 65535, inclusive.

The *<assigned-number>* can be any numeric value from 0 to 2,147,483,647, inclusive.

- *<IPV4-address>: <assigned-number>*

Where *<IPV4-address>* can be any valid IPV4 address (in W.X.Y.Z "dot" notation), and *<assigned-number>* can be any numeric value from 0 to 65535, inclusive.

In the Default Endpoints Settings section of the Service Parameters page, enter the endpoint or device settings information by doing the following tasks:

1. Select a value for **Ethernet option**.

- **Port**
- **Dot1Q**

Specifying the **Dot1Q** Ethernet option enables you to apply a Unit ID, a single VLAN ID, a VLAN Range, or a VLAN list to the service order.

- **QinQ**

Specifying the **QinQ** Ethernet option enables you to apply a single VLAN, a VLAN Range, or a VLAN list to the service order. For an L3VPN service deployed on a dual tagged interface, the inner tag determines the VPN routing and forwarding instance(VRF).

2. In the **Bandwidth** field, select a value from the list to limit the bandwidth of the service you are creating.

This field is present only if bandwidth limiting is allowed by the service definition, and is configurable in the service order only if the service definition allows it.

3. In the **MTU** field, type the maximum transmission unit size for the UNI.

This field is present in all service orders. However, you can set this field only if the service definition allows it.

The **Auto-pick VLAN range constraint** field is displayed and validates the VLAN range specified in the service definition.

4. Specify the Logical interface settings:



NOTE: The Autopick Interface Unit ID field is not available if you have selected the Ethernet option as Port.

- Specify whether the **Autopick Interface Unit ID** can be selected automatically or manually.
 - To assign the **Unit** automatically, select the **Autopick Interface Unit ID** check box.
 - To assign the **Unit** manually, clear the **Autopick Interface Unit ID** check box.

The window expands to include the **Unit** field. In the **Unit** field, type a value.

Range: 1 through 1073741823



NOTE: You can edit this field only if you have selected the Editable in Service Order check box for the VLAN ID selection in the service definition.

- Specify whether the **Autopick VLAN ID** can be selected automatically or manually.
 - To assign the **VLAN ID** automatically, select the **Autopick VLAN ID** check box.
 - To assign the **VLAN ID** manually, clear the **Autopick VLAN ID** check box.

The window expands to include the **VLAN ID** field. In the **VLAN ID** field, type a value.

5. Select the preferred option for calculating the burst size:

- **MTU Based**

If you select the option **MTU Based**, you can specify a value for **MTU Factor** in the range 1 through 1087902.

The default value for **MTU Factor** is 10.

- **Line Rate Based**

If you select the option **Line Rate Based**, you can specify a value for **Burst Period** in the range 1 through 7450 milliseconds.

The default value for **Burst Period** is 1.

6. In the **Customer VLAN Range Start** and **Customer VLAN Range End** fields, type the first and last VLAN ID of the range of customer VLANs to be transported over the network.

These fields are present only for services with UNIs that have Q-in-Q interface types and allow a range of VLANs to be transported.

7. In the **Normalize - VLAN ID Tag** field, type a value for the customer VLAN.

This field is present only for services that specify Normalize to Dot1q tags.

8. In the Inner **Normalize - Inner VLAN Tag (for QinQ)** field, type a value to provide a default inner VLAN tag for the UNI endpoints.

This field is present only for services that specify Normalize to QinQ tags.

9. In the **Normalize - Outer VLAN Tag** field, type a value to provide an outer VLAN tag that matches the Outer VLAN tag of at least one of the UNI endpoints.

This field is present only for services that specify Normalize to QinQ tags.

10. Click **Next** to proceed to the next step of the wizard, which is to define the node or endpoint parameters.

Specifying OAM Settings

To enable OAM on the service definition, type information in the OAM Settings of the Service Parameters page of the wizard.

1. In the **OAM Profile** field, select a profile from the list.



NOTE: For OAM Settings, if you specify a CFM profile (for example, a CFM action profile with remote MEP), or an SLA-Iterator profile, first you must ensure that the profile is attached to the same device upon which you intend to deploy the P2P service order. If the profile is not previously attached (using the OAM Insight application), it will not be present on the device to support the service order.

To remove a previously associated CFM definition or OAM profile from a service definition, click the **Detach** button next to the OAM Profile field to remove the association. To associate a new OAM profile, you must dissociate the existing OAM profile and attach a fresh OAM profile. Detaching an OAM profile is enabled when you modify a service or service order.



NOTE: For Juniper Networks PTX3000 Packet Transport Routers and Junos Space Release 13.1P1, if you attach a CFM Definition to the service order, the CFM session will operate for MEPs in either the Up or Down direction when the service is deployed.

2. Click **CFM Details** beside the OAM Profile field to view the profile configuration details in a dialog box.
3. Continue with specifying the endpoint information.

Selecting N-PE Devices

This part of the create point-to-multipoint Ethernet service order procedure selects the N-PE devices. The selection is made from the **Node Parameters** page of the Create VPLS Service Order wizard.

If there is a service template attached to the service definition, there is a link to that template at the bottom of the **Node Parameters** section of the window. For instructions on working with service templates in service orders, see [“Creating a Service Order Based on a Service Definition with a Template” on page 990](#).



NOTE: The **Choose Endpoints** window shows only assigned NPE devices that have an AS number configured. If you do not see the device you are looking for, use the CLI on the device to check for and assign an AS number.

To select endpoint N-PE devices:

1. In the **Node Parameters** page, click **Add** in the Service Nodes table. From the Choose Endpoints dialog box that appears, select the devices that you want to participate in the service. Use the multiple selection feature to select one or more devices.

Figure 44: Choose Endpoints Dialog Box

Name	IP Address	State	Managed State	Platform	OS Version	Roles
<input checked="" type="checkbox"/> 960R2_EP_Alok_re	10.216.194.110	up	In Sync	MX960	14.2-20140916.0	N_PE
<input type="checkbox"/> 480R4_EP_Alok_re	10.216.194.105	up	In Sync	MX480	14.2-20140916.0	N_PE
<input type="checkbox"/> 480R3_EP_Alok_re	10.216.194.108	up	In Sync	MX480	14.2-20140916.0	N_PE
<input type="checkbox"/> 960R1_EP_Alok_re	10.216.194.118	up	In Sync	MX960	14.2-20140916.0	N_PE
<input type="checkbox"/> RouterZ-re	10.92.35.185	down	In Sync	MX960	15.1-20141022_L...	N_PE
<input type="checkbox"/> RouterY-re	10.92.35.187	up	In Sync	MX960	15.1-20141022_L...	N_PE
<input type="checkbox"/> RouterX-re	10.92.35.189	up	In Sync	MX960	15.1-20141022_L...	N_PE
<input type="checkbox"/> RouterXCore-re	10.92.35.183	down	In Sync	MX960	15.1-20141022_L...	-
<input type="checkbox"/> Merg1_006_re	10.92.37.13	up	In Sync	MX960	15.1-20150727_...	N_PE

Page 1 of 3 Displaying 1 - 9 of 25 Show 9 items

Name	Status	Encapsulation	Index
<input type="checkbox"/> ae0	down	none	508
<input type="checkbox"/> ae1	down	none	509
<input type="checkbox"/> em1	up	none	23
<input type="checkbox"/> em2	up	none	116
<input type="checkbox"/> ge-0/0/2	up	flexible-ethernet-services	533
<input type="checkbox"/> ge-0/0/3	up	flexible-ethernet-services	539
<input type="checkbox"/> ge-0/0/4	up	flexible-ethernet-services	542
<input type="checkbox"/> ge-0/0/5	up	none	550
<input type="checkbox"/> ge-0/0/6	up	none	551
<input type="checkbox"/> ge-0/0/7	up	none	552
<input type="checkbox"/> ge-0/0/8	up	none	553
<input type="checkbox"/> ge-0/0/9	up	none	554

OK Cancel



NOTE: In the Choose Endpoints dialog box, you can sort and segregate the devices and their corresponding interfaces based on the roles of the devices to easily and quickly view only the devices of interest. Click the down arrow on the Filter Role menu, and select P2E to view only the provider edge devices, P to view only the provider devices, and L2E to view only Layer 2 Ethernet devices.

- 2.
3. Click **OK**.

The **Node Parameters** window appears.

4. Continue with modifying or entering the node parameters.

Specifying Node Settings

This part of the create point-to-multipoint Ethernet service order procedure sets the attributes that are usually common for all endpoints in the service.



NOTE: If you are using a definition with multiple templates, you can set different attributes for the endpoints.

In any case, the values that you type depend on the service definition on which the service order is based. Follow the steps in one of the following tasks, depending on whether or not the service provides flexible VLAN tagging. To create a service with flexible VLAN tagging, the service definition that you selected for the service order must include the Ethernet option **asymmetric tag depth** in the UNI settings step.

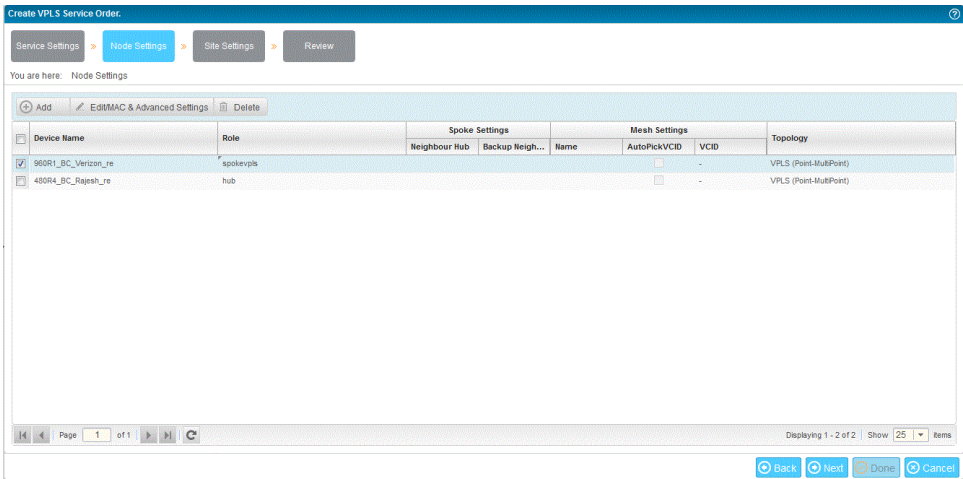
- [Setting Attributes for Nodes or Devices on a Service on page 918](#)
- [Setting Attributes for Nodes or Devices on a Service with Flexible VLAN Tagging on page 922](#)

Setting Attributes for Nodes or Devices on a Service

If these attributes are not the same on all endpoints, you can set them to be the same for now and then make changes later, or you can choose to skip this step and apply the attribute values one at a time later, or use a definition with multiple templates.

This procedure sets the attributes listed in the Node Settings page of the of the Create VPLS Service Order wizard. The attributes shown depend on the interface type and the signaling type.

The Node Settings page displays configuration attributes for the device selected in the table of all added nodes. If multiple devices are selected, data is displayed beneath the table for the last selected device. If you do not select a device, the service definition details for nodes are displayed.



To set attributes common to most endpoints:

1. Fill in the following fields under the MAC Settings section

Field	Action
MAC Settings	
MAC learning	To enable MAC learning , select the check box.
Interface MAC limit	Maximum number of MAC addresses learned from an interface. Range: 1 through 131071 MAC addresses per interface
MAC statistics	To enable MAC statistic , select the check box.
MAC Table Size	Modify the size of the MAC address table for the bridge domain. Range: 16 through 1048575 To allow the service provisioner to override the MAC settings, select Editable in Service Order .

2. Fill in the following fields under the Topology Settings section.
 - a. In the Topology field, the type of network connection or circuit is displayed as Full Mesh (point-to-multipoint) or Hub-Spoke (Point to Multipoint), based on the type of service definition selected. In this case, the topology is shown as point-to-multipoint.
 - b. Define a route distinguisher option from the **Auto Pick Route Distinguisher** check box and **Route Distinguisher** field:
 - Select the check box to enable the service provider to specify the route distinguisher.

- Select the check box to enable the route distinguisher to be selected automatically.

3. Fill in the following fields under the Advanced Settings section.

Advanced Settings—This section enables you to specify the parameters that define advanced connectivity between sites across the service provider network. Configuring advanced settings is optional. You can click on the Advanced link to view the default values for Advanced Settings. If the advanced settings can be edited in the service order, you can override the default values. If you do not click the Advanced link, the default advanced settings are applied to the service order.

Include	<p>Select the Include check box for each advanced setting that you want to include in the service definition.</p> <p>NOTE: If you select any advanced parameters for a service definition, you must also select the Include check box for the Disable tunnel services parameter, and select or clear the Disable tunnel services check box.</p> <p>For MX Series devices, if you deploy a VPLS service without selecting the Include check box for Disable tunnel services parameter, the VPLS service is down. As a work around, you can push the configuration to each PE device for the service by running the following command:</p> <pre>root@test_device# set chassis fpc 0 pic 1 tunnel-services bandwidth 1g</pre>
Disable Tunnel Services	<p>Enable or disable tunnel-services to specify that traffic for particular VPLS routing instances be forwarded to specific virtual tunnel (VT) interfaces.</p> <ul style="list-style-type: none"> • To enable tunnel-services, clear the Disable Tunnel Services check box. • To disable tunnel-services, select the Disable Tunnel Services check box (default).
Disable Local Switching	<p>Enable or disable local switching. In local switching mode, you can terminate multiple Layer 2 circuit pseudowires at a single VPLS mesh group:</p> <ul style="list-style-type: none"> • To enable local switching across the network, clear the Disable Local Switching check box. • To disable local switching across the network, select the Disable Local Switching check box (default).
Fast Reroute-Priority	<p>In this drop-down list, specify the reroute priority for a VPLS routing instance:</p> <ul style="list-style-type: none"> • HIGH—Set the fast reroute priority for a VPLS routing instance to high. During a fast reroute event, the router repairs next hops for high-priority VPLS routing instances first. • MEDIUM—Set the fast reroute priority for a VPLS routing instance to medium. During a fast reroute event, the router repairs next hops for medium-priority VPLS instances after high-priority VPLS routing instances but before low-priority VPLS routing instances. • LOW—Set the fast reroute priority for a VPLS routing instance to low, which is the default. During a fast reroute event, the router repairs next hops for low-priority VPLS routing instances last.
Label Block Size	<p>Configure the label block size for VPLS labels by using one of the following values.</p> <ul style="list-style-type: none"> • 2—Allocate the label blocks in increments of 2. Use this setting for a VPLS domain that has only two sites with no future expansion plans. • 4—Allocate the label blocks in increments of 4. • 8—Allocate the label blocks in increments of 8. This is the default. • 16—Allocate the label blocks in increments of 16. A label block size of 16 enables you to minimize the number of routes in the VPLS domain. Use this setting only if the number of routes is the primary concern. <p>NOTE: This field is unavailable if the Signaling type is LDP and the Auto discovery check box is enabled.</p>

Connectivity type

Select a connection-type to specify when a VPLS connection is taken down, depending on whether the interface for the VPLS routing instance is customer-facing or integrated routing and bridging (IRB):

- **ce**—Require that for the VPLS connection to be up, the customer-facing interface for the VPLS routing instance must also be up. If the customer-facing interface fails, the VPLS connection is taken down. This is the default.
- **irb**—Allow a VPLS connection to remain up so long as an IRB interface is configured for the VPLS routing instance.

NOTE: This field is unavailable if the **Signaling** type is LDP and the **Auto discovery** is enabled.

4. Fill in the following fields under the Spoke Settings section.

For spoke devices you can update the **Neighbor Hub** details only if:

- The **Signaling** type is LDP and the **Auto discovery** check box is disabled
- The **Signaling** type is BGP and the **Enable PW Extension** check box is enabled
- **Enable P2P-Spoke**—If selected, the spoke acts as a stitched point-to-point pseudowire. This check box is available only if you have enabled the **Enable PW Extension** in the selected service definition. If you have added more than one UNI interface for a spoke device, you cannot select this check box.
- **NeighborHub**—Select the neighbor hub device from the list. If the **Signaling** type is BGP, enable the **Enable P2P-Spoke** check box to select the neighbor hub.
- **Backup neighbor**—Select the backup neighbor hub device from the list. This field is available if the **Enable PW Resiliency** check box is enabled in the selected service definition. If the **Signaling** type is BGP, enable the **Enable P2P-Spoke** check box to select the backup neighbor.



NOTE: You cannot select the same device for **NeighborHub** and **Backup neighbor**.

- **PW-Hub Connectivity name**— If the **Signaling** type is BGP and if you have enabled the **Enable P2P-Spoke** check box, select or type the mesh group name from other pseudowire spoke.

Range: 1 through 32 characters

If the **Signaling** type is LDP, the pseudowire-hub connectivity name is auto generated.

- **Auto pick VC ID**—This field is available if the **Signaling** type is BGP and if you have enabled the **Enable P2P-Spoke**.

If the **Signaling** type is LDP, the **VPLS ID** of the routing instance is used.

- **VC ID**—If the **Signaling** type is BGP and if you have enabled **Enable P2P-Spoke**, specify the VC ID.

You can also modify the VCID field in the Modify Service Order window.

Range: 1 through 2147483647

If the **Signaling** type is LDP, the **VPLS ID** of the routing instance is used.

5. Click **Next**.

The **Site Settings** page of the Create VPLS Service Order wizard appears.

6. Continue with specifying the UNI or interface settings.

Setting Attributes for Nodes or Devices on a Service with Flexible VLAN Tagging

A service with flexible VLAN tagging can include port-based, 802.1Q, and Q-in-Q interfaces.

If these attributes are not the same on all endpoints, you can set them to be the same for now and then make changes later, or you can choose to skip this step and apply the attribute values one at a time later, or you can use a definition with multiple templates.

If there is a service template attached to the service definition, there is a link to that template at the bottom of the **Node Settings** page of the wizard. For instructions on working with service templates in service orders, see [“Creating a Service Order Based on a Service Definition with a Template” on page 990](#).

This procedure sets the attributes listed in the Node Settings page of the of the Create VPLS Service Order wizard. The attributes shown depend on the signaling type and interface type. The following example shows the endpoints settings box for a point-to-multipoint service with flexible VLAN tagging that transports a single VLAN and specifies Normalize to Dot1Q tag.

Modifying Site Settings

This part of the create point-to-multipoint Ethernet service order procedure sets the attributes for each interface of an endpoint or a device in the service. Selection is made using the **Site Settings** page of the wizard that enables you to create a VPLS service order.

This window shows one interface for each device that you selected from the **Choose Endpoints** dialog box of the Node Settings page, as described in [“Selecting N-PE Devices” on page 891](#).

The Site Settings page enables you to select a device to add interfaces for that device. You can select multiple interfaces for the device. If the Enable L3 Access check box is enabled, the UNI lists available integrated routing and bridging (IRB) interfaces for the selected device. If the device role is a P2P spoke, you can select one UNI and it is required for such devices. If Ethernet Option is set as port-to-port, the UNI can be added only once as an endpoint for the device.

Create VPLS Service Order

Service Settings > Node Settings > Site Settings > Review

You are here: Site Settings

Device	Interface	Unit		Tagging	AutoPick	VLAN				TPID		RateLimit(Mb/s)
		AutoPick	ID			VLAN	CVLAN	CVLANStart	CVLANEnd	OuterTPID	InnerTPID	
960R1_BC_V...	NA	<input checked="" type="checkbox"/>	-	qinq	<input checked="" type="checkbox"/>	-	-	-	-	-	-	10
480R4_BC_R...	NA	<input checked="" type="checkbox"/>	-	qinq	<input checked="" type="checkbox"/>	-	-	-	-	-	-	10

Page 1 of 1

Displaying 1 - 2 of 2 | Show 25 items

Back Next Done Cancel

The interface shown in the **UNI Interface** field is automatically selected by the Connectivity Services Director application, which chooses the UNI that has the highest available capacity among interfaces that are in the Up state. To calculate the available capacity of the interface, the system subtracts the bandwidth reserved for each service deployed on that interface from the total capacity of the interface.

For each endpoint, the **Site Settings** page shows the following value for each UNI attribute:

- For port-to-port services, the displayed values are Bandwidth and MTU.
- For 802.1Q UNIs, the displayed attributes are Bandwidth, AutoPick VLAN ID, VLAN ID, and MTU.
- For Q-in-Q UNIs, the displayed attributes include Bandwidth, AutoPick VLAN ID, and VLAN ID. For a service with Q-in-Q UNIs that specifies a customer VLAN range, the displayed attributes also include C-VLAN ID Start and C VLAN End.

For each endpoint on a service with flexible VLAN tagging, the Endpoint Settings window shows the following value for each UNI attribute:

- For a service with flexible VLAN tagging that transports a single VLAN and specifies Normalize to Dot1q tags, the displayed attributes include Ethernet Option, Bandwidth, AutoPick VLAN ID, Inner VLAN ID, and MTU. For a service with flexible VLAN tagging that specifies a customer VLAN range, the displayed attributes also include C-VLAN ID Start and C VLAN End.
- For a service with flexible VLAN tagging that transports a single VLAN and specifies Normalized to QinQ tags, the displayed attributes include Bandwidth, AutoPick VLAN ID, and VLAN ID. For a service with flexible VLAN tagging that specifies a customer VLAN range, the displayed attributes also include C-VLAN ID Start and C VLAN End.
- For a service with flexible VLAN tagging that transports a VLAN range, the displayed attributes include Bandwidth, AutoPick VLAN ID, and VLAN ID. For a service with flexible VLAN tagging that specifies a customer VLAN range, the displayed attributes also include C-VLAN ID Start and C VLAN End.

The values shown are initially the values you set earlier on the Service Parameters page of the creation of VPLS service order wizard, as described in [“Specifying Node Settings” on page 893](#).

To add a UNI and specify its settings:

1. Click the **Add** icon at the top of the User-to-Network Interfaces table. The Choose Endpoints dialog box is displayed.
2. Select the check box next to the endpoint or device from which you want to add a UNI to the service order. After you select the check box, the view refreshes to display the configured interfaces for that corresponding device in the lower part of the dialog box

Figure 45: Choose Endpoints Dialog Box

Name	IP Address	State	Managed State	Platform	OS Version	Roles
<input checked="" type="checkbox"/> 960R2_EP_Alok_re	10.216.194.110	up	In Sync	MX960	14.2-20140916.0	N_PE
<input type="checkbox"/> 480R4_EP_Alok_re	10.216.194.105	up	In Sync	MX480	14.2-20140916.0	N_PE
<input type="checkbox"/> 480R3_EP_Alok_re	10.216.194.108	up	In Sync	MX480	14.2-20140916.0	N_PE
<input type="checkbox"/> 960R1_EP_Alok_re	10.216.194.118	up	In Sync	MX960	14.2-20140916.0	N_PE
<input type="checkbox"/> RouterZ-re	10.92.35.185	down	In Sync	MX960	15.1-20141022_i...	N_PE
<input type="checkbox"/> RouterY-re	10.92.35.187	up	In Sync	MX960	15.1-20141022_i...	N_PE
<input type="checkbox"/> RouterX-re	10.92.35.189	up	In Sync	MX960	15.1-20141022_i...	N_PE
<input type="checkbox"/> RouterXCore-re	10.92.35.183	down	In Sync	MX960	15.1-20141022_i...	-
<input type="checkbox"/> Merg1_006_re	10.92.37.13	up	In Sync	MX960	15.1-20150727_...	N_PE

Page 1 of 3 | Displaying 1 - 9 of 25 | Show 9 items

Name	Status	Encapsulation	Index
<input type="checkbox"/> ae0	down	none	508
<input type="checkbox"/> ae1	down	none	509
<input type="checkbox"/> em1	up	none	23
<input type="checkbox"/> em2	up	none	116
<input type="checkbox"/> ge-0/0/2	up	flexible-ethernet-services	533
<input type="checkbox"/> ge-0/0/3	up	flexible-ethernet-services	539
<input type="checkbox"/> ge-0/0/4	up	flexible-ethernet-services	542
<input type="checkbox"/> ge-0/0/5	up	none	550
<input type="checkbox"/> ge-0/0/6	up	none	551
<input type="checkbox"/> ge-0/0/7	up	none	552
<input type="checkbox"/> ge-0/0/8	up	none	553
<input type="checkbox"/> ge-0/0/9	up	none	554

OK Cancel



NOTE: In the Choose Endpoints dialog box, you can sort and segregate the devices and their corresponding interfaces based on the roles of the devices to easily and quickly view only the devices of interest. Click the down arrow on the Filter Role menu, and select P2E to view only the provider edge devices, P to view only the provider devices, and L2E to view only Layer 2 Ethernet devices.

3. Select the check boxes next to the interfaces to add to the service order.
4. Click **Add** to save the settings, and click **Close** to exit from the dialog box. You are returned to the Site Settings page.
5. For a service with flexible VLAN tagging, set the interface type in the Ethernet Option column for each endpoint in the service.
6. To select a different UNI on a device, from the **User-to-Network Interfaces** section, click the UNI name you want to change and choose another interface from the list.
7. Select the **Enable CFM** check box beside a particular interface of a device in the service order creation and modification wizards to enable connectivity fault management (CFM) on the interface. Based on your network needs, you can create a point-to-multipoint and a multipoint-to-multipoint VPLS service with service-level CFM enabled. The CFM profile is propagated to a single endpoint when multiple interfaces are selected for a given device (the last interface overrides the other configurations). When you select the **Enable CFM** check box for an interface of a particular device, you cannot enable CFM on other interfaces of the same device. The CFM configuration is pushed only on the selected interface.

When you delete the interface with CFM enabled, the CFM configuration on the particular device is also removed. When you attempt to delete an interface with CFM enabled, you are prompted to confirm the deletion.

8. In the **Customer VLAN Range Start** and **Customer VLAN Range End** fields, type the first and last VLAN ID of the range of customer VLANs to be transported over the network. These fields are present only for services with UNIs that have Q-in-Q interface types and allow a range of VLANs to be transported.
9. Select a value for **Ethernet option**.
 - **Port**
 - **Dot1Q**

Specifying the **Dot1Q** Ethernet option enables you to apply a Unit ID, a single VLAN ID, a VLAN Range, or a VLAN list to the service order.

- **QinQ**

Specifying the **QinQ** Ethernet option enables you to apply a single VLAN, a VLAN Range, or a VLAN list to the service order. For an L3VPN service deployed on a dual tagged interface, the inner tag determines the VPN routing and forwarding instance(VRF).

10. To enter the description for an UNI interface, click the corresponding **Description** cell.
11. To change the bandwidth on an endpoint, click the bandwidth value for the endpoint and select another value from the list.
12. The **AutoPick Interface Unit ID** and the **Unit ID** columns appear, if you have not selected the **Ethernet option** as port-to-port.
 - To change an automatically selected service UNIT ID to manual selection, clear the **AutoPick Interface Unit ID** check box, and type a service UNIT ID value in the **Unit ID** field.
 - To change from manual selection to automatic selection, select the **AutoPick Interface Unit ID** check box.
 - To change the value of a manually selected service Unit ID, type a new value in the **Unit ID** field.



NOTE: The unit ID value that you have specified in the Enter Order Information page is displayed in the Unit ID field.

13. For Q-in-Q interface endpoints, you can change how the service VLAN ID is selected:
 - To change an automatically selected service VLAN ID to manual selection, clear the **AutoPick VLAN ID** check box, and type an VLAN ID value in the **VLAN ID** field.
 - To change from manual selection to automatic selection, select the **AutoPick VLAN ID** check box.
 - To change the value of a manually selected service VLAN ID, type a new value in the **VLAN ID** field.
14. For Q-in-Q interface endpoints with customer VLAN ranges specified, you can also change the range limits for an endpoint.
15. For 802.1Q interface endpoints, you can change the customer VLAN ID.
16. To change the MTU for the UNI, click the value in the **MTU** field and type a new value.
17. To add a UNI on a selected device, click **Add** to open the Choose Endpoints dialog box and then select the interface you want from the UNI interface list.

18. If the interface you selected in the previous step is already configured (duplicate) you must either type a different value in the **VLAN ID** field manually, or check the **Autopick VLAN ID** field.

19. To delete a UNI from a device, select the interface and click **Delete** in the table that displays the UNIs.

If the deleted UNI is the only UNI selected from the device, then the device is deleted from the service configuration.

20. When you have finished modifying the endpoint settings, click **Review** to examine and modify the settings.

The screenshot shows the 'Create VPLS Service Order' wizard in the 'Review' step. The breadcrumb trail at the top indicates the sequence: Service Settings > Node Settings > Site Settings > Review. The 'You are here: Review' text is displayed below the breadcrumbs. The main content area is titled 'Service Settings' and contains three expandable sections: 'General Settings', 'Connectivity Settings', and 'OAM Settings'. The 'General Settings' section is expanded, showing fields for Service Order Name (VPLS-SO), Customer Name (Shell), Customer ID (1278007), Policy Name (ELAN-Hub-Spoke-QinQ-AI/VLAN), Policy ID (852165), and Service Type (VPLS(BGP)). The 'Connectivity Settings' section is also expanded, showing fields for Auto-Pick VPN ID (false), Auto pick Route (true), Distinguisher, Auto pick Route Target (false), AllowAccessToL3Network (false), Enable PW Extension (false), and Enable PW Resiliency (false). The 'OAM Settings' section is collapsed. At the bottom right of the form, there are four buttons: Back, Next, Done, and Cancel.

21. Click **Finish** when you have completed examining the settings to confirm the creation of the service order.

22. You can proceed with deploying the service.

Specifying QoS Settings

CoS profiles enable the grouping of class-of-service (CoS) parameters and apply them to one or more interfaces. Connectivity Services Director provides you with predefined traffic types for each CoS profile that you create. These traffic types represent the most common types of traffic for the device type. Each of these templates has preconfigured values for all CoS parameters based on the typical application requirements. You can change the preconfigured values of these parameters to suit your requirements. To display the CoS Profiles page, in Build mode, select CoS under Profile and Configuration Management in the Tasks pane. The Manage CoS Profiles page appears.

If QoS is enabled on the service definition, configure the QoS Settings of the Site Settings panel of the service order creation wizard.

1. In the **QoS profile** field, select a profile from the list.

The **QoS profile** list displays the QoS profiles that are currently configured in the Manage CoS Profiles page of the Connectivity Services Director application.

A QoS profile classifies traffic into defined service groups to provide the special treatment of traffic across the network service.

Specifying Template Settings

The Template Settings page of the service order creation and modification wizards enables you to associate service templates with a point-to-point, VPLS, and Layer 3 VPN service order. You can apply only the templates that are previously configured in a service definition with the corresponding service order. The Template Settings page is available in the service order wizard only if the service definition that you selected to apply to the service order contains a service template. Otherwise, the Template Settings page is not displayed in the service order wizard. You can perform template operations for all endpoints in a service order.

If you defined a service template as the default service template, it is attached to the endpoint by default. You have the flexibility to create and provision a dynamic attribute in a service template. You can mark an attribute of a service template as dynamic, and you can obtain the values for these dynamic attributes from a specific device. To create a dynamic attribute, you must first mark an attribute of a service template as dynamic and then specify the device XPath for the dynamic attribute.

The Template Settings page is displayed before the Review page, which is the final step of the service order wizard.

In the Service Settings page of the Select Service Definition field of the service order creation wizard, you can double-click a service definition name displayed in the table to view the details of the definition in a popup dialog box. You can use this information to determine if the service definition is appropriate for your deployment needs. To filter and sort the display of service templates, enter the name of the template as a match criterion in the Search box and click the Search icon. The page refreshes to display only the template names that match with the search term. You can use the paging controls to navigate across multiple pages of templates as necessary.

All the tasks that you can perform with service templates are presented in the Template Settings page. The page is divided into three panes. The top half of the page displays a table of selected endpoints. All the endpoints or UNIs that you selected in the preceding pages of the service order wizard are displayed in this table. You can configure the template pertaining to only one endpoint at a point in time. If the selected endpoints (in previous pages of the wizard) contained a manually-entered unit number, that number is displayed in the table of selected endpoints. Otherwise, the Auto-pick label is displayed.

The lower half of the page is divided into two panes. The left pane displays the template selection table for the endpoint you selected. All the templates associated with the service definition are displayed. You can add and delete templates using the template selection table. The right pane displays all the parameters that you can modify for a selected service template. All such editable parameters are displayed in a consolidated

form of a configuration page. This pane is displayed after you select a template. If any configuration parameter in template is set as a service-specific value, such attributes are not displayed in this pane.

To associate a service template with a service order:

1. Click **Add** to include a service template for the endpoint. A dialog box is displayed with the list of service templates associated with the service definition that is used to create the service order. The templates selected in this dialog box are displayed in the Template Selection table for the specified endpoint. Such templates are considered to be attached to that endpoint.

If you specified a template as a default template during the service definition creation, the template is displayed by default in the template selection table. You can associate non-default templates with the service order by clicking the **Add** button.

2. Click the link in the template name to open the Template Details dialog box. The template settings are displayed in the popup dialog box. For the selected template, the Configuration Page is displayed in the lower-right pane of the Template Settings page.
3. Modify any template-specific service components as necessary.
4. Click **Save** to submit the changes.
5. Select a template from the Template Selection table, and click Delete to remove the template from being associated with the service order for a particular endpoint.

Reviewing the Configured Settings

The Review page of the service definition or service order creation and modification wizards enable you to view and evaluate the service parameters and components you configured in preceding steps or pages of the wizard. This page provides a comprehensive, single-page view of all the service elements configured in the different pages of the wizard. You can either click the buttons corresponding to the various settings at the top of the wizard page to directly traverse to the page you want to modify or click the navigation buttons at the bottom of the wizard page to go to the different pages of the wizard.

To review the configured service settings in the wizard:

1. Click **Review** to view the defined parameters. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify.
2. Click **Edit** next to the section that contains the parameter you want to modify. You are navigated to the corresponding page of the wizard in which the parameter settings are defined.

3. Click **Finish** to save the service definition or service order.
4. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

The service order inventory window appears.

Deploying the New Service

This part of the create point-to-multipoint Ethernet service order procedure deploys the service.

To deploy the service from the **Manage Deploy Services** window:

1. Perform one of the following actions in the Deploy mode of the Service View of Connectivity Services Director:
 - To deploy the service immediately, select **Deploy now**, then click **OK**.
 - To deploy the service later, select **Schedule deployment**, select a date and time, then click **OK**.

The time field specifies the time kept by the server, but in the time zone of the client.
2. To monitor the status of the deployment, use the Jobs workspace.

The service order is now complete.

The **Manage Service Orders** page shows the service order you just added.

Related Documentation

- [Creating a Multipoint-to-Multipoint VPLS Service Order on page 881](#)
- [Creating a Service Order for VPLS Access into Layer 3 Networks on page 930](#)

Creating a Service Order for VPLS Access into Layer 3 Networks

To select a service definition on which to base the new service order:

1. Select **Service View** from the View Selector. The workspaces that are applicable to network and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the View pane, click the plus sign (+) to expand the tree and select the type of service.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.

- Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
5. From the Tasks pane, select **Service Provisioning > Deploy Services**.

The Manage Network Services page is displayed in the top half of the right pane, which displays all of the configured services. The Manage Service Orders page is displayed in the bottom half of the right pane, which displays all of the service orders corresponding to a service.

6. From the **Manage Network Services** page, select **New > VPLS Service Order**.

The **Create VPLS Service Order** window appears and shows a filtered inventory view of only those published service definitions designed to work with multipoint Ethernet services.

7. From the **Service Parameters** page, select the service definition you want to base your service order

8. Specify the **General Settings**.

Field	Action
Name	<p>Enter a unique name for the VPLS multipoint service.</p> <p>The service order name can consist of only letters, numbers, and underscores.</p> <p>NOTE: The name you specify for a VPLS service order becomes the routing-instance name in the device configuration when you deploy the service. Consequently, you cannot use any Juniper Networks keywords, for example, “bgp” or “vpls”, as the name of a service order.</p>
Customer	<p>Select the customer requesting the service. To speed your search, enter the first few letters of the customer name and then select from the list.</p> <p>If the customer is not in the list, you must add the customer to the database before proceeding. See “Adding a New Customer” on page 737.</p>
Comments	<p>Enter a description of the service. This description appears in the information screens about the request or service instance created from the request.</p> <p>The Customer traffic type field is not selectable. Its value is set in the service definition.</p> <p>The Autopick Route Target field cannot be changed. Route targets are always selected automatically.</p>
Autopick route target	<p>Check the box if you are allowing the system to choose the VPLS routing instance.</p> <p>NOTE: The Autopick route target is not editable in service order. By default, the check box is always selected.</p>

Field	Action
Allow access to L3 network	<p>Check this box to create the access path into the Layer 3 network.</p> <p>Required for VPLS service orders with access into Layer 3 networks.</p> <p>NOTE: The Allow access to L3 network is not editable in service order. By default, the check box is always selected.</p>

- Continue with the **Node Settings** page.

Node Settings

Field	Action
Bandwidth	Specify the bandwidth or use the default that appears in the field.
MTU (Bytes)	Specify the MTU value or use the default that appears in the field.
VLAN ID	Specify the VLAN ID associated with the IRB subinterface that will provide the link into the Layer 3 network. This must be a VLAN that already exists.
VLAN Tag to stack	The VPLS service definition requires a normalized VLAN. Indicate the VLAN to push at the relevant end points. This should be the same VLAN specified as the VLAN ID.

- Click **Next** to display the device list where you will select the the interfaces for the endpoint devices.
- Select the devices you will use for this Layer 3 access.
- The VPLS service order requires three interface: One IRB interface for the tunnel and two endpoints to ping end-to-end. Add your three interfaces using the **Site Settings** page.
- Select the IRB interface and click **Finish**. The service order is saved.

Related Documentation

- [Creating a Point-to-Multipoint VPLS Service Order on page 905](#)

Creating a VPLS Service Order with CFM

Ethernet interfaces support the IEEE 802.1ag standard for Operation, Administration, and Management (OAM). The IEEE 802.1ag specification provides for Ethernet connectivity fault management (CFM). CFM monitors Ethernet networks that might comprise one or more service instances for network-compromising connectivity faults.

The major features of CFM are:

- Fault monitoring using the continuity check protocol. This is a neighbor discovery and health check protocol that discovers and maintains adjacencies at the VLAN or link level.
- Path discovery and fault verification using the linktrace protocol. Similar to IP traceroute, this protocol maps the path taken to a destination MAC address through one or more bridged networks between the source and destination.
- Fault isolation using the loopback protocol. Similar to IP ping, this protocol works with the continuity check protocol during troubleshooting.

CFM partitions the service network into various administrative domains. For example, operators, providers, and customers might be part of different administrative domains.

Each administrative domain is mapped into one maintenance domain providing enough information to perform its own management, thus avoiding security breaches and making end-to-end monitoring possible. Each maintenance domain is associated with a maintenance domain level from 0 through 7. Level allocation is based on the network hierarchy, where outermost domains are assigned a higher level than the innermost domains.

Customer end points have the highest maintenance domain level. In a CFM maintenance domain, each service instance is called a maintenance association. A *maintenance association* can be thought as a full mesh of maintenance endpoints (MEPs) having similar characteristics. MEPs are active CFM entities generating and responding to CFM protocol messages.

There is also a maintenance intermediate point (MIP), which is a CFM entity similar to the MEP, but more passive (MIPs only respond to CFM messages).

MEPs can be *up MEPs* or *down MEPs*. A link can connect a MEP at level 5 to a MEP at level 7. The interface at level 5 is an up MEP (because the other end of the link is at MEP level 7), and the interface at level 7 is a down MEP (because the other end of the link is at MEP level 5).

In a Metro Ethernet network, CFM is commonly used at two levels:

- By the service provider to check the connectivity among its provider edge (PE) routers
- By the customer to check the connectivity among its customer edge (CE) routers



NOTE: The configured customer CFM level must be greater than service provider CFM level.

In many Metro Ethernet networks, CFM is used to monitor connectivity over a VPLS and bridge network.

The CFM profile is propagated to a single endpoint when multiple interfaces are selected for a given device (the last interface overrides the other configurations). When you enable CFM for an interface of a particular device, you cannot enable CFM on other interfaces of the same device. The CFM configuration is pushed only on the selected interface. When you delete the interface with CFM enabled, the CFM configuration on the particular device is also removed. When you attempt to delete an interface with CFM enabled, you are prompted to confirm the deletion.

To create a VPLS service order with CFM enabled:

1. Select **Service View** from the View Selector. The workspaces that are applicable to network and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the View pane, click the plus sign (+) to expand the tree and select the type of service.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
5. From the Tasks pane, select **Service Provisioning > Deploy Services**.

The Manage Network Services page is displayed in the top half of the right pane, which displays all of the configured services. The Manage Service Orders page is displayed in the bottom half of the right pane, which displays all of the service orders corresponding to a service.

6. From the **Manage Network Services** page, select **New > VPLS Service Order**.

The **Create VPLS Service Order** window appears and shows a filtered inventory view of only those published service orders designed to work with multipoint Ethernet services.

See [“Creating a Multipoint-to-Multipoint VPLS Service Order” on page 881](#) and [“Creating a Point-to-Multipoint VPLS Service Order” on page 905](#) for detailed information about

the settings that you can configure on the Service Settings and Node Settings pages of the wizard.

7. After you complete the configuration of settings on the Service Settings and Node Settings pages of the service order creation or modification wizard, click **Site Settings** at the top of the wizard page.

The Site Settings page is displayed.

8. Select the **Enable CFM** check box beside a particular interface of a device in the service order creation and modification wizards to enable connectivity fault management (CFM) on the interface. Based on your network needs, you can create a point-to-multipoint and a multipoint-to-multipoint VPLS service with service-level CFM enabled. The CFM profile is propagated to a single endpoint when multiple interfaces are selected for a given device (the last interface overrides the other configurations). When you select the **Enable CFM** check box for an interface of a particular device, you cannot enable CFM on other interfaces of the same device. The CFM configuration is pushed only on the selected interface.

When you delete the interface with CFM enabled, the CFM configuration on the particular device is also removed. When you attempt to delete an interface with CFM enabled, you are prompted to confirm the deletion.

9. For service orders associated with a service definition that contains a service template, click **Next** to modify the template settings.
10. Click **Review** to examine and modify the settings as necessary.
11. Click **Finish** when you have completed examining the settings to confirm the creation of the service order.

**Related
Documentation**

- [Creating a Point-to-Multipoint VPLS Service Order on page 905](#)

Interconnecting a VPLS Service with a Layer 3 VPN Service

You can stitch or interconnect a VPLS service with a Layer 3 VPN service. You must enable the stitching functionality to perform this interconnection. If the stitching capability is enabled, when you select the interfaces for the endpoints added to a service, only the integrated routing and bridging (IRB) physical and logical interfaces are available for selection. If you select a physical IRB interface, a new logical interface is created with the logical unit identifier of the interface you specify. If you select a logical IRB interface, the existing logical interface is used to create the service.

You can stitch or interconnect a VPLS service with a Layer 3 VPN service during the creation or modification of a VPLS service order. Follow the steps outlined in for performing the tasks in the Service Settings and Node Settings pages of the wizard. To enable the stitching of a VPLS service with a Layer 3 VPN service, you can select the Stitch check box for a device associated with the service order on the Site Settings page of the VPLS service order creation or modification wizard.

- Ensure that you have already created a VPLS service.
- Complete the configuration of settings on the Service Settings and Node Settings pages of the service order creation or modification wizard.

To interconnect a VPLS service with a Layer 3 VPN service:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the View pane, click the plus sign (+) to expand the tree and select the type of service.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
5. From the Tasks pane, select **Service Provisioning > Deploy Services**.

The Manage Network Services page is displayed in the top half of the right pane, which displays all of the configured services. The Manage Service Orders page is displayed in the bottom half of the right pane, which displays all of the service orders corresponding to a service.

6. From the Manage Network Services page, select **New > VPLS Service**.

The **Create VPLS Service Order** window appears and shows a filtered inventory view of only those published service definitions designed to work with multipoint Ethernet services. You can select the service definition based on the signaling type.

See [“Creating a Multipoint-to-Multipoint VPLS Service Order” on page 881](#) and [“Creating a Point-to-Multipoint VPLS Service Order” on page 905](#) for detailed information about the settings that you can configure on the Service Settings and Node Settings pages of the wizard.

7. After you complete the configuration of settings on the Service Settings and Node Settings pages of the service order creation or modification wizard, click **Site Settings** at the top of the wizard page.

The Site Settings page is displayed.

8. Select the check box beside the device for which you want to enable the stitching of VPLS and L3VPN services.

The device that you select is available for stitching.

9. Select the **Stitch** check box to enable the interconnection of the VPLS service with an L3VPN service.

10. Click inside the Interface Name field to select an IRB interface. A popup dialog box is displayed with the list of all configured IRB interfaces. If the stitching capability is enabled, when you select the interfaces for the endpoints added to a service, only the IRB physical and logical interfaces are available for selection.

11. Select a physical or logical IRB interface that you want to use to stitch the VPLS service with an L3VPN service.

The selected interface is used for interconnection of the services.

12. (Optional) If you select a physical IRB interface, you can specify the logical unit of the interface in the UNIT ID field.

The specified logical IRB interface is used for stitching the services.

13. For service orders associated with a service definition that contains a service template, click **Next** to modify the template settings.

14. Click **Review** to examine and modify the settings as necessary.

15. Click **Finish** when you have completed examining the settings to confirm the creation of the service order.

16. You can proceed to enable the stitching functionality for the same IRB interface with the Layer 3 VPN service. See [“Interconnecting a Layer 3 VPN Service with a VPLS](#)

[Service” on page 876](#) for detailed information about enabling the stitching functionality for the Layer 3 VPN service.

Related •
Documentation

Service Provisioning: Managing Layer 3 VPN Service Orders

- [Stitching a Pseudowire to an L3VPN Service on page 939](#)
- [Creating a Full Mesh Layer 3 VPN Ethernet Service Order on page 941](#)
- [Creating a Hub-and-Spoke Layer 3 VPN Service Order on page 964](#)
- [Selecting a Published L3VPN Service Definition for a Service Order on page 985](#)
- [Entering Layer 3 VPN Order Information on page 986](#)
- [Selecting Endpoint PE Devices or Nodes on page 988](#)
- [Creating a Service Order Based on a Service Definition with a Template on page 990](#)
- [Deploying a Layer 3 VPN Service Order on page 993](#)
- [Creating a Multicast VPN Service Order on page 995](#)
- [Creating Policies for a Layer 3 VPN Service on page 998](#)

Stitching a Pseudowire to an L3VPN Service

You can terminate a point-to-point pseudowire service into an existing Layer 3 VPN, thereby providing access to Layer 3 services. The benefit of the pseudowire stitching feature is that devices running on Layer 2 technology continue to function when networks are upgraded and Layer 3 technologies are used. In order to stitch Layer 2 services to one another and to Layer 3 services, Junos Space utilizes tunnel PICs to peer up a pseudowire and a Layer 3 VPN.

To stitch a pseudowire to a Layer 3 VPN service:

1. Create a point-to-point service definition.

In the General page of the Create Point-to-Point Service Definition wizard, select the **Enable PW access to L3 VPN network** check box to enable pseudowire access to the Layer 3 VPN network.

For more information on creating a point-to-point service definition, see [“Creating a Point-to-Point Ethernet Service Definition” on page 625](#).

2. Create a Layer 3 VPN service definition.

For information about creating a full mesh Layer 3 VPN service definition, see [“Creating a Full-Mesh Layer 3 VPN Service Definition” on page 709](#). For information about creating a hub-and-spoke service definition, see [“Creating a Hub-and-Spoke \(One Interface\) Layer 3 VPN Service Definition” on page 719](#).

3. Create and deploy a Layer 3 VPN service order.

For information about creating a full mesh Layer 3 VPN service order, see [“Creating a Full Mesh Layer 3 VPN Ethernet Service Order” on page 941](#). For information about creating a hub-and-spoke service order, see [“Creating a Hub-and-Spoke Layer 3 VPN Service Order” on page 964](#).

4. In Deploy mode of Service View, from the Manage Network Services inventory page, select a Layer 3 VPN service that you created and select **Extend PW Service** from the Actions menu

The Extend PW Service inventory page lists the point-to-point service definitions that are enabled for Layer 3 access. This inventory page must also list the point-to-point service definition you created in Step 1.

5. Select the point-to-point service definition and click **Next**.

6. Create a point-to-point service order.

The stitched end of the point-to-point service is prepopulated with Layer 3 VPN service details.

The fields displayed in the point-to-point service order are based on the point-to-point service definition selected in Step 5. For example, in the point-to-point service definition, when pseudowire resiliency is enabled, then the **Revert time (sec)** and the **Switch Over Delay (sec)** fields are available in the service order.

You can select any one of the devices from the **PE device** field. Only the devices with logical tunnel interfaces are listed. These devices are associated with the Layer 3 VPN service.

Specify the following information in the PW Stitching box:

- **L3 routing instance name**—Name of the Layer 3 routing instance



NOTE: This field is prepopulated for a stitched end of the point-to-point service.

- **Autopick interface IP**—If enabled, specify **IP block size** and **IP address pool**; otherwise specify the **Interface IP address**.
- **Autopick peer unit**—To peer logical system unit number, select the check box; otherwise specify the **Peer unit name**.

For more information on creating a point-to-point service order, see [“Creating a Point-to-Point Service Order” on page 829](#).

The Layer 3 VPN Service Details window now displays the **PW Extension** details.

When you perform a functional audit for a Layer 3 VPN service with pseudowire termination, by default the functional audit is applicable only to the Layer 3 VPN service. To perform a functional audit for the pseudowires, select the **Include all extensions** check box in the Schedule Functional Audit window.



NOTE: For pseudowires, the functional audit is launched as a separate job.

Similarly, to perform a Force Deploy for the pseudowires, select the **Include all extensions** check box in the Schedule Force Deployment window.

You can view the details of the stitched pseudowire in the Functional Audit Results window.

**Related
Documentation**

- [Creating a Point-to-Point ATM or TDM Pseudowire Service Order on page 816](#)
- [Creating a Point-to-Point Service Order on page 829](#)

Creating a Full Mesh Layer 3 VPN Ethernet Service Order

You can use Connectivity Services Director application to implement Layer 3 VPN Ethernet services.

Creating a Layer 3 VPN full mesh Ethernet service order consists of the following tasks:

1. [Selecting the Service Definition on page 941](#)
2. [Configuring Service Parameters Information on page 943](#)
3. [Selecting N-PE Devices or Nodes on page 947](#)
4. [Setting Attributes for Endpoints or Nodes on page 948](#)
5. [Adding and Deleting UNI Interfaces on page 954](#)
6. [Setting Attributes for UNIs or Sites on page 954](#)
7. [Specifying QoS Settings on page 961](#)
8. [Specifying Template Settings on page 961](#)
9. [Reviewing the Configured Settings on page 963](#)
10. [Deploying the New Service on page 963](#)

Selecting the Service Definition

To select a service definition to base the new service order on:

1. From the Connectivity Services Director application, select **Service View** from the Views list.

The workspaces that are applicable to routing and tunnel services are displayed.

2. From the Junos Space user interface, click the **Deploy** tab in the Task Categories banner. The features that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, click the plus sign (+) to expand the tree and select the type of service.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
5. Select **L3VPN Services** and from the Tasks pane, select **Service Provisioning > Manage Services**.

The Manage Network Services page is displayed in the top half of the right pane, which displays all of the configured services. The Manage Service Orders page is displayed in the bottom half of the right pane, which displays all of the service orders corresponding to a service.

6. From the Manage Network Services page, select **New > Layer 3 VPN Service Order**.

The Service Settings page in the Create Layer 3 VPN Service Order wizard is displayed.

7. From the **Service Definition** field, click **Select** to choose the service definition you want to base your service order on.

The **Choose Service Definition** inventory page displays a view of only those published service definitions designed to work with the type of services you need.

Based on the fields or parameters that you defined in the service definition to be enabled for modification in the service order, the corresponding fields are available for editing. The fields that are disabled for modification in the service order can only be edited in the service definition.

8. Select the check box beside the service definition that you want to associate with the service order, and click **OK**.

Configuring Service Parameters Information

In this topic you configure general settings, VPN settings that can be applied to all end points, and routing protocol settings for the provider edge (PE) and customer edge (CE) devices.

- [Specifying General Settings on page 943](#)
- [Specifying PE-CE Settings Information on page 946](#)

Specifying General Settings

To specify general information for a Layer 3 VPN Service Order:

The screenshot shows the 'Create L3VPN Service Order' interface with the 'Service Settings' tab selected. The breadcrumb trail indicates the path: Service Settings > Node Settings > Site Settings > Template Settings > Review. The 'You are here' section points to 'Service Settings'.

General Settings

Name*:

Comments:

Customer*:

Service Definition*:

Connectivity Settings

- ☐ Policy Based Route Target
- ☐ Auto pick Route Target
- ☐ Auto pick Hub Route Target
- ☐ Auto pick Spoke Route Target

VPN Settings

- ☐ VRF Table Label
- ☐ Shared Group Routes
- ☐ Enable Auto Export Routes
- ☐ Enable MPLS
- ☐ Enable MC-LAG

Default UNI Settings

PE-CE Settings

At the bottom right, there are four buttons: .

1. Fill in the fields on the Service Settings page as indicated in [Table 116 on page 944](#).

Table 116: Layer 3 VPN Service Order - Service Settings

Field	Description
General Settings	
Name	<p>Type a unique name for the service. The service order name can consist of only letters, numbers, and underscores.</p> <p>NOTE: The name you specify for a Layer 3 VPN Service Order becomes the routing-instance name in the device configuration when you deploy the service.</p>
Comments	Type a description of the service.
Customer	<p>Click Select to select name of the enterprise customer that requests for a service.</p> <p>Click Clear to clear the current selection.</p>
Service Definition	<ul style="list-style-type: none"> Click Select to choose a service definition from the Choose Service Definition pop-up. The Service Order is created based on the service definition you choose. Select the check box beside the service definition that you want to associate with the service order, and click OK. Click View to view details of the service definition you selected. <p>The type of Service Definition you choose determines the fields that are available in the Connectivity Settings section, VPN Settings section, and the PE-CE Settings section of the Settings Page of the Layer 3 VPN Service Order wizard.</p>
Instance Type	The type of Service Definition you choose will determine the Instance Type displayed in the field.
Enable Distinct Instance Name	Select this check box to specify a distinct instance name for each device.
Connectivity Settings	
Policy Based Route Target	<p>Select this check box to create a policy-based vrf instance.</p> <p>Clear this check box to create a community-based vrf instance.</p> <p>For more information on creating policies for a Layer 3 VPN service, see "Creating Policies for a Layer 3 VPN Service" on page 998.</p>
Auto Pick Route Target	<p>Clear this check box, to enable the Route Target field.</p> <p>To override this setting in the service order, you can select the Editable in Service Order check box in the create Layer 3 full-mesh service definition wizard.</p>

Table 116: Layer 3 VPN Service Order - Service Settings (continued)

Field	Description
Route Target	<p>Specify the route target range in any of the following formats:</p> <ul style="list-style-type: none"> AS Number format: <ul style="list-style-type: none"> AS Number Range: 1 through 4294967295 IPv4 address format: <ul style="list-style-type: none"> If AS Number or IP is less than or equal to 65535, range is 0 through 65535. If AS Number or IP is greater than 65535, range is 0 through 4294967295. <p>NOTE: You must clear the Auto Pick Route Target check box to enable this field.</p>
Auto Pick Hub Route Target	<p>Select this check box to automatically generate a Hub Route Target.</p> <p>Clear this check box to manually enter a Hub Route Target.</p> <p>NOTE: The Auto Pick Hub Route Target check box is visible if the selected Instance Type is vrf.</p> <p>You can edit this field if you select the Editable in Service Order check box in the Create Layer 3 Hub-and-Spoke Service Definition wizard.</p>
Hub Route Target	<p>Specify the hub route target range in any of the following formats:</p> <ul style="list-style-type: none"> prefix-number:assigned-number Prefix-number can be any numeric value from 1 through 65535. Assigned-number can be any numeric value from 0 through 2147483647. IPV4-address:assigned-number IPV4-address can be any valid IPv4 address, and assigned-number can be any numeric value from 0 through 65635. <p>NOTE: To manually enter the Hub Route Target, clear the Auto Pick Hub Route Target check box.</p>
Auto Pick Spoke Route Target	<p>Select this check box to automatically generate a Spoke Route Target.</p> <p>Clear the Auto Pick Spoke Route Target check box to manually enter a Spoke Route Target.</p> <p>NOTE: The Auto Pick Spoke Route Target check box is visible only if Instance Type selected is vrf.</p> <p>You can edit this field if you select the Editable in Service Order check box in the Create Layer 3 Hub-and-Spoke Service Definition wizard.</p>
Spoke Route Target	<p>Specify the spoke route target range in any of the following formats:</p> <ul style="list-style-type: none"> prefix-number:assigned-number Prefix-number can be any numeric value from 1 through 65535. Assigned-number can be any numeric value from 0 through 2147483647. IPV4-address:assigned-number IPV4-address can be any valid IPv4 address, and assigned-number can be any numeric value from 0 through 65635.
VPN Settings	

Table 116: Layer 3 VPN Service Order - Service Settings (continued)

Field	Description
VRF Table Label	<p>Select this check box while creating a service definition to configure a separate label for each VRF to provide double lookup and egress filtering.</p> <p>This check box is visible only if the selected Instance Type is vrf.</p>
Export Direct Routes	Select this check box in the Create Layer 3 Full Mesh Service Definition wizard to export direct routes.
Enable Auto Export Routes	You can select this check box in the Create Layer 3 VPN Service Definition wizard to enable internal and external route leak as part of route target creation.
Import Internal Routes	Select this check box in the Create Layer 3 VPN Service Definition wizard to enable the internal route leak feature as part of route target policy creation.
Import External Routes	Select this check box in the Create Layer 3 VPN Service Definition wizard to enable the external route leak feature as part of route target policy creation.
Enable MVPN	<p>Select this check box to enable multicast VPN (MPVN) settings.</p> <p>If you select this check box, the Enable MC-LAG check box is disabled.</p>
Default UNI Settings	
MTU Factor	<p>Specify a value for MTU Factor in the range 1 through 1087902. The default value for MTU Factor is 10.</p> <p>The value you configure for MTU Factor should not exceed one tenth of the value you configured for burst size.</p> <p>NOTE: This field is enabled only if you select MTU Based as the Burst Size.</p>
Burst Period	<p>Specify a value for Burst Period in the range 10 through 1000. The default value for Burst Period is 10.</p> <p>NOTE: This field is enabled only when you select Line Rate Based as the Burst Size.</p>

Specifying PE-CE Settings Information

You configure VPN attributes that are usually common for all the endpoints in the service. Depending on the service definition on which the service order is based, the values that you provide vary.

If you do not expect these attributes to be the same on all endpoints, you can set them to be the same for now and then make changes later, or you can skip this step and apply the attribute values one at a time later.

Fill in the PE-CE Settings as indicated in [Table 117 on page 947](#):

Table 117: Layer 3 VPN Service Order - PE-CE Settings

Field	Description
PE-CE Settings	
Routing Protocol	The routing protocol in use is displayed.
AS Override	<p>Select this check box to allow a service provisioner to override the AS number.</p> <p>This check box is available if you select BGP as the routing protocol while creating the service definition.</p>
Maximum Prefixes	<p>Range: 1 through 4294967295</p> <p>This feature limits the number of unique destinations in a routing instance.</p>
OSPF Domain ID	<ul style="list-style-type: none"> • ID Range Prefix: 1 through 65535 • ID Range Postfix: 0 through 4294967295 <p>This check box is available only if you select OSPF as the routing protocol while creating the service definition.</p>
OSPF Version	<p>Choose an OSPF version from the OSPF Version list:</p> <ul style="list-style-type: none"> • Ver 2 • Ver 3 <p>Junos OS supports OSPF version 2 (OSPFv2) and OSPF version 3 (OSPFv3).</p> <p>This check box is available only if OSPF is selected as the routing protocol while creating the service definition.</p>

Click **Next**

The **Node Settings** page appears.

Selecting N-PE Devices or Nodes

In this topic you select the N-PE devices that you want to host the service endpoints.

To select endpoint N-PE devices:

1. Click **Add** in the **Node Settings** page of the **Create Layer 3 VPN Service Order** wizard to add a device.

A new row is added to the existing table.



NOTE: You can create a new policy by clicking **Create Policy**.

This option is available if you select **Policy Based Route Target** check box and clear the **Auto Pick Route Target** check box.

For more information on creating a policy, see [“Creating Policies for a Layer 3 VPN Service” on page 998](#)

2. Click the arrow in the name field.
3. From the list, select a device you want to add to the service.
You can select more than one device.
4. Click **OK**.

The device is added to the table.



NOTE: You can modify the device settings by selecting the check box next to the device and clicking **Edit**.

Click **Ok** to save your changes.

Continue with modifying or entering the node parameters.

Setting Attributes for Endpoints or Nodes

For instructions on working with service templates in service orders, see *Creating a Service Order Based on a Service Definition with a Template*.

You set attributes for each endpoint in the service from the **Node Settings** page.

Create L3VPN Service Order

Service Settings | **Node Settings** | Site Settings | Review

You are here: Node Settings

Add Edit Delete Create Policy

Enter Search text

Name	IP Address	Stitching Point	Autopick	RD Value
R2960EL_re	10.220.10.35	<input type="checkbox"/>	<input type="checkbox"/>	N/A
R1960EL_re	10.220.10.6	<input type="checkbox"/>	<input type="checkbox"/>	N/A

Back Next Done Cancel

For each endpoint, the **Node Settings** page shows the value for each UNI attribute.

You can enter topology settings, create static routes on the service, and enter MVPN/PIM settings in the Node Settings page. To specify these settings for a CE device on the Node Settings page:

1. Select the device and click **Edit**.

The Node Settings window appears.

Node Settings: R2960EL_re

Topology Settings

Static Routes

Destination Prefix:

Option Type:

Add Delete

Attribute	Attribute Value
-----------	-----------------

MVPN/PIM Settings

PIM Settings

MVPN Settings

MVPN Mode:

Site Type:

Provider Tunnel Name:

☐ Upstream Multicast Hop

Import Target: ☐ Sender ☐ Receiver

Import Unicast Target: ☐ Sender ☐ Receiver ☐ None

OK Cancel

2. Fill in the fields to configure or change topology settings as indicated in [Table 118 on page 950](#):

Table 118: Layer 3 VPN Service Order - Topology Settings

Field	Description
Topology	<p>The type of network circuit in use is displayed in this field:</p> <ul style="list-style-type: none"> • Full Mesh • Hub-and-spoke
Is Stitching Point	<p>Clear this check box.</p> <p>If you select the Is Stitching Point check box, all the parameters of that endpoint are disabled.</p>
Is Hub	<p>Select this check box to enable the node to function as a hub.</p> <p>Clear this check box if you want the device to function as a spoke.</p> <p>NOTE: This field is not applicable for full-mesh layer 3 VPN services.</p>
Import RT Policy	<p>Select a policy from the list.</p> <p>Policies associated with other devices and policies created as part of the service are listed. You can select more than one policy.</p> <p>You have the option to:</p> <ul style="list-style-type: none"> • Select a policy from the list. • Clear the current selection by clicking Clear. <p>NOTE: You can also add or delete a policy while modifying the service.</p>
Export RT Policy	<p>Select a policy from the list</p> <p>Policies associated with other devices and policies created as part of the service are listed. You can select more than one policy.</p> <p>You have the option to:</p> <ul style="list-style-type: none"> • Select a policy from the list. • Clear the current selection by clicking Clear. <p>NOTE: You can also add or delete a policy while modifying the service.</p>
Auto pick Route Distinguisher	<p>Select this check box to assign the Route Distinguisher automatically.</p> <p>This field is enabled if you have selected the Editable in Service Order check box in the service definition.</p>

Table 118: Layer 3 VPN Service Order - Topology Settings (continued)

Field	Description
Route Distinguisher	<p>Enter a valid Route Distinguisher range:</p> <ul style="list-style-type: none"> as-number:id—Range: 1 through 65535 ip-address:id—Range: <ul style="list-style-type: none"> ip address: any unique unicast address id: 1 through 65535 <p>Each routing instance must have a unique route distinguisher (RD) associated with it. The RD is used to place bounds around a VPN so that the same IP address prefixes can be used in different VPNs without any overlap.</p> <p>This field is available only if you have selected full-mesh as the service type while creating the service definition.</p>
Auto pick Hub Route Distinguisher	<p>Select this check box to assign the Hub Route Distinguisher automatically.</p> <p>This field is enabled if you selected the Editable in Service Order check box in the service definition.</p>
Hub Route Distinguisher	<p>Enter a valid Hub Route Distinguisher range:</p> <ul style="list-style-type: none"> as-number:id—Range: 1 through 65535 ip-address:id—Range: <ul style="list-style-type: none"> ip address: any unique unicast address id: 1 through 65535 <p>This field is available only if you selected hub-and-spoke as the service type while creating the service definition.</p>
Auto pick Spoke Route Distinguisher	<p>Select this check box to assign the Spoke Route Distinguisher automatically.</p> <p>This field is enabled only if you selected the Editable in Service Order check box in the service definition.</p>
Spoke Route Distinguisher	<p>Enter a valid Spoke Route Distinguisher range:</p> <ul style="list-style-type: none"> as-number:id—Range: 1 through 65535 ip-address:id—Range: <ul style="list-style-type: none"> ip address: any globally unique unicast address id: 1 through 65535 <p>This field is available only if you selected hub-and-spoke as the service type while creating the service definition.</p>

- Fill in the fields to create static routes on the service as indicated in [Table 119 on page 952](#):

Table 119: Layer 3 VPN Service Order - Static Routes

Field	Action
Destination Prefix	<p>Enter the endpoint for the static route in this field.</p> <ul style="list-style-type: none"> IP address—Destination IP address that the router uses to identify packets. Network mask—Network mask for associated IP subnet. Netmask value: 0-32
Option Type	<p>Choose an option type from the Option Type list:</p> <ul style="list-style-type: none"> next-hop next-table community
Hop Address	<p>Enter a valid IP address in this field. You can have multiple hop for every destination prefix.</p> <p>This field is available only if you choose next-hop as the Option Type.</p>
Route Table Name	<p>Choose one of the following options as the route table name:</p> <ul style="list-style-type: none"> inet.0 inet.3 <p>This field is available only if you choose next-table as the Option Type.</p>
Member	<p>Choose one of the following values as the member type:</p> <ul style="list-style-type: none"> no-export no-advertise no-export-subconfed <p>This field is available only if you choose community as the Option Type.</p>
Add	<p>Click Add to add a static route to the Static Route Table.</p> <p>A new row is added to the table.</p>
Delete	<p>Select the row you want to delete and click Delete to remove the static route from the Static Route Table.</p>
Attribute	<p>The Attribute column displays the Option Type you select</p>
Attribute Value	<p>The Attribute Value column displays the corresponding value for every Option Type you select.</p>

4. Specify the MVPN and PIM Settings as indicated in [Table 120 on page 953](#):



NOTE: The MVPN and PIM Settings sections are displayed only if you select the **Enable MVPN** check box in the Service Settings page of the Create Layer 3 VPN Service Order wizard.

Table 120: Layer 3 VPN Service Order - MVPN and PIM Settings

Field	Description
PIM Settings	
PIM Mode	<p>Choose the PIM Mode from the drop down list.</p> <p>Only sparse mode is currently supported.</p>
MVPN Settings	
MVPN Mode	<p>Choose one of the following MVPN modes from the MVPN Mode list:</p> <ul style="list-style-type: none"> • rpt-spt • spt-only
Site Type	<p>Choose one of the following MBGP MVPN site types from the list:</p> <ul style="list-style-type: none"> • sender • receiver
Provider Tunnel Name	Specify the provider tunnel name to configure virtual private LAN service (VPLS) flooding of unknown unicast, broadcast, and multicast traffic using point-to-multipoint LSPs in this field. You can also configure point-to-multipoint LSPs for MBGP MVPNs.
Upstream Multicast Hop	Select this check box to configure the upstream multicast hop (UMH).
Import Target	<p>Specify the import targets for sender and receiver sites in this field.</p> <p>Select the Sender radio button to import targets for sender sites, select the Receiver radio button to import targets for receiver sites.</p>
Import Unicast Target	<p>Specify the import targets specifically for sender sites or receiver sites in this field. You can also borrow import targets from a configured unicast route target.</p> <p>NOTE: A sender site export route target is always advertised when security association routes are exported. By default, the VPN routing and forwarding (VRF) import and export route targets (configured either using VRF import and export policies or using the vrf-target statement) are used for importing and exporting routes with the MBGP MVPN network layer reachability information (NLRI).</p>
Export Unicast Target	Select this check box to specify the export target to enable you to override the Layer 3 VPN export route targets used for importing and exporting routes for the MBGP MVPN network layer reachability information (NLRI).

Table 120: Layer 3 VPN Service Order - MVPN and PIM Settings (continued)

Field	Description
Auto pick Export Target	Select this check box to enable automatic selection of an export target if a configuration is not provided.
Target Community	Specify the target community value to be used when exporting sender and receiver site routes in this field. You can specify this value manually if you clear the Autopick Export Target check box.

Click **Ok** to accept all configured values.

Click **Cancel** to reject all configured values.

- Click **Next** when you have finished configuring node settings.

The Site Settings page is displayed.

Adding and Deleting UNI Interfaces

In the Site Settings page, you can add or delete UNI interfaces on the PE devices that participate in a service.

To add a UNI interface on a selected device:

- Click **Add** to add a new row to the table.
- From the newly added row, click the arrow in the **Device Name** field.
A list of interfaces is displayed.
- Select the check boxes beside the UNIs that you want to associate with the service order and click **Ok**. You can select more than one UNI.

The table now displays the UNI interfaces configured on the selected device.

To delete a UNI Interface from a selected device, select the check box next to the interface that you want to delete, and click the **Delete** button above the table.



NOTE: If the deleted UNI is the only UNI selected from the device, then the device is deleted from the service configuration.

Setting Attributes for UNIs or Sites

If there is a service template attached to the service definition, there is a link to that template at the bottom of the Site Settings section of the screen. For instructions on working with service templates in service orders, see [“Creating a Service Order Based on a Service Definition with a Template” on page 990](#).

This part of the create Ethernet service order procedure sets the attributes for each endpoint in the service. Selection is made using the Site Settings page.

The screenshot shows the 'Create L3VPN Service Order' interface. At the top, there are tabs for 'Service Settings', 'Node Settings', 'Site Settings' (selected), and 'Review'. Below the tabs, a breadcrumb trail indicates 'You are here: Site Settings'. The main area contains a table with the following columns: Device Name, Interface Name, Interface Status, Unit, VLAN, and IP. The first row is highlighted in blue and contains the following data: Device Name: R1000EL_re, Interface Name: NA, Interface Status: Autopick (checked), Unit: ID, Tagging: Det1Q, Autopick (checked), Outer: NA, Inner: NA, Autopick (checked), Address: 30, Subnet: 30. The page also includes navigation buttons (Back, Next, Done, Cancel) and a search bar.

The interface shown in the UNI Interface field is automatically selected by the Connectivity Services Director application, which chooses the UNI that has the highest available capacity among interfaces that are in the Up state. To calculate the available capacity of the interface, the system subtracts the bandwidth reserved for each service deployed on that interface from the total capacity of the interface.

For each endpoint, the Site Settings page shows the value for each UNI attribute.

To modify the values of a UNI interface:

1. To modify the device settings, select the device by clicking the check box next to it.

The row is highlighted in blue.

2. You can edit details in the row based on [Table 121 on page 955](#):

Table 121: Layer 3 VPN Service Order - Modify or alter UNI Interface

Field	Description
Device Name	Displays the name of the device associated with the UNI.
Interface Name	<p>Displays the selected interface name.</p> <p>To add a new interface:</p> <ol style="list-style-type: none"> a. Click the arrow in the Interface Name field. b. To select the interface, select the check box that corresponds to the interface. c. Click Ok. <p>The interface name is displayed and the corresponding fields are updated.</p>

Table 121: Layer 3 VPN Service Order - Modify or alter UNI Interface (continued)

Field	Description
Interface Status	<p>Displays the interface's status.</p> <ul style="list-style-type: none"> • A Green Up arrow indicates devices that are up and running. • A Red Down arrow indicates devices that are down.
Unit Autopick	<p>Select this check box to assign the Unit ID automatically.</p> <p>Clear this check box to assign the Unit ID manually.</p>
Unit ID	<p>Enter a value in this field.</p> <p>Range: 1 through 1073741823</p> <p>This field is available only if you clear the Unit Autopick checkbox.</p>
VLAN Tagging	<p>Select one of the following options from the list:</p> <ul style="list-style-type: none"> • Port • Dot1Q • QinQ(All) • QinQ(Single) <p>Specifying the Dot1Q Ethernet option enables you to apply a Unit ID, a single VLAN ID, a VLAN Range, or a VLAN list to the service order.</p> <p>Specifying the QinQ Ethernet option enables you to apply a single VLAN, a VLAN Range, or a VLAN list to the service order. For an L3VPN service deployed on a dual tagged interface, the inner tag determines the VPN routing and forwarding instance(VRF).</p>
VLAN Autopick	<p>Select this check box to assign the VLAN Outer ID automatically.</p> <p>Clear this check box to assign the VLAN Outer ID manually.</p>
VLAN Outer	<p>Enter a value in this field.</p> <p>This field is available if you clear the Unit Autopick check box.</p>
VLAN Inner	<p>Enter a value in this field.</p> <p>This field is available if you choose Dot1Q or QinQ(All) as the VLAN Tagging value.</p>
IP Autopick	<p>Select this check box to assign the IP address automatically.</p> <p>Clear this check box to assign the IP address manually.</p> <p>You cannot edit this check box if you have not selected the Editable in Service Order check box in the service definition.</p>
IP Address	<p>You can enter an IP address in this field if you have cleared the IP Autopick check box.</p> <p>You can choose an IP address from the list if you have selected the IP Autopick check box.</p>
IP Subnet	<p>Enter a valid IP subnet in this field.</p>

To configure or edit Site Settings:

1. Select the interface that you want to edit by clicking the check box next to it.

The selected row is highlighted in blue.

2. You can edit the interface details by following [Table 122 on page 957](#):

Table 122: Layer 3 VPN Service Order - Configure Site Settings

Field	Action
Site Settings	
Interface	The name of the interface you choose is displayed in this field.
Description	Type a description that describes the UNI Interface. Range: 0 to 128 characters.
UNI Settings	
Encapsulation	Choose an encapsulation value from the Encapsulation list: <ul style="list-style-type: none"> • Port • Dot1Q • QinQ(Single) • QinQ(All) <p>If you choose Port as the encapsulation value, no field in the UNI settings section is enabled.</p> <p>If you choose Dot1Q as the encapsulation value, Auto pick Interface Unit and Auto pick VLAN ID check boxes are enabled.</p> <p>If you choose QinQ(Single) or QinQ(All) as the encapsulation value, Customer VLAN Type and Outer TP ID fields are enabled.</p>
Auto pick Interface Unit	Select this check box to automatically assign the Unit ID . Clear this check box to manually enter the Unit ID .
Unit ID	Enter a unit ID in this field. Range - 1 through 16385 This field becomes available when you clear the Auto pick Interface Unit check box.
Auto pick VLAN ID	Select this check box to assign the VLAN ID automatically. Clear this check box to manually enter the VLAN ID .
VLAN ID	Enter a VLAN ID in this field. Range - 1 through 4094 This field is available when you clear the Auto pick VLAN ID check box.

Table 122: Layer 3 VPN Service Order - Configure Site Settings (continued)

Field	Action
Customer VLAN Type	<p>Choose a customer VLAN type from the Customer VLAN Type drop down box:</p> <ul style="list-style-type: none"> • Transport All Traffic—Transports traffic from all VLANs across the network • Transport Single VLAN—Transports traffic for a specific VLAN across the network. <p>This field is available only when the encapsulation value you select is QinQ(Single) or QinQ(All)</p>
Customer VLAN ID	<p>Enter a Customer VLAN ID in this field.</p> <p>Range - 1 through 4094</p> <p>This field is available only when you select Transport Single VLAN as the Customer VLAN type.</p>
Outer TP ID	<p>Choose a value form the Outer TP ID list:</p> <ul style="list-style-type: none"> • empty (default) • 0x8100 • 0x88a8 • 0x9100
Inner TP ID	<p>Choose a value form the Inner TP ID list:</p> <ul style="list-style-type: none"> • empty (default) • 0x8100 • 0x88a8 • 0x9100 <p>This field is available when you select Transport Single VLAN as the customer VLAN type.</p>
IP Settings	
Autopick Interface IP	<p>Select this check box to choose an interface IP from IP Address Pool drop down list.</p> <p>Clear this check box to manually enter an interface IP in the Interface IP Address field.</p>
IP Pool Type	<p>Displays the IP Pool Type you have selected.</p> <ul style="list-style-type: none"> • Global • Customer • None
Interface IP Address	<p>Enter an interface IP address.</p> <p>This field is available only when you clear the Autopick Interface IP check box.</p>
IP Address Pool	<p>Choose an interface IP address from the IP Address Pool drop down list.</p> <p>This field is available only if you select the Autopick Interface IP check box.</p>
IP Block size	<p>Enter a valid IP address block size value in this field.</p> <p>Range - 1 through 32</p>

Table 122: Layer 3 VPN Service Order - Configure Site Settings (continued)

Field	Action
PE-CE Settings	
Routing Protocol	<p>Select a protocol from the list:</p> <ul style="list-style-type: none"> • BGP • OSPF • Static
OSPF Area ID	<p>Enter an OSPF area id.</p> <p>Valid IP Range - 0.0.0.0 through 255.255.255.255</p> <p>This field is available only if OSPF is selected as the routing protocol in the service definition.</p>
OSPF Version	<p>Enter an OSPF version number.</p> <ul style="list-style-type: none"> • Ver 2 • Ver 3 <p>This field is available only if OSPF is selected as the routing protocol in the service definition.</p>
Group Name	<p>Enter a group name.</p> <p>Range - 0 to 255 characters</p> <p>This field is available only if BGP is selected as the routing protocol in the service definition.</p>
Local Address	<p>This field is available if BGP is selected as the routing protocol in the service definition.</p>
Autopick Neighbour IP	<p>Select this field if you want to automatically generate a Neighbour IP. You can edit this field if you select Editable in Service Order check box.</p> <p>This field is available only if BGP is selected as the routing protocol in the service definition.</p>
Neighbour IP	<p>Enter a valid IP address in this field.</p> <p>Range - 1.0.0.1 through 223.225.225.254, excluding 127.x.x.x</p> <p>This field is available if BGP is selected as the routing protocol in the service definition.</p>
Peer AS	<p>Enter a Peer AS range in this field.</p> <p>Range - 1 through 4294967295</p> <p>This field is available if BGP is selected as the routing protocol in the service definition.</p>

Table 122: Layer 3 VPN Service Order - Configure Site Settings (continued)

Field	Action
Import Policy	<p>Select the policy from the list.</p> <p>Policies associated with other devices and policies created as part of the service is listed. You can select more than one policy from the list.</p> <p>You also have the option to:</p> <ul style="list-style-type: none"> • Select a policy from the list. • Clear the current selection by clicking Clear. <p>You can also add or delete a policy while modifying the service.</p>
Export Policy	<p>Select the policy from the list.</p> <p>Policies associated with other devices and policies created as part of the service is listed. You can select more than one policy from the list.</p> <ul style="list-style-type: none"> • Select a policy from the list. • Clear the current selection by clicking Clear. <p>You can add or delete a policy while modifying the service.</p>
PIM Settings	
Add	Click Add to add a new row in the PIM Settings table.
Delete	Click Delete to delete a row from the PIM Settings table.
Rendezvous Point (device)	Click the arrow in this field to select a device from the drop down list.
Group Address	<p>Enter a group IP address.</p> <p>Range - 224.0.1.0 through 239.255.255.255</p>
Update or Cancel	<p>Click Update to update the Rendezvous Point (device) and Group Address to the PIM Settings table.</p> <p>Click Cancel to cancel any updates.</p>

3. Click **Ok** after you enter the site settings details in the **Site Settings** window.

The site settings page is displayed.

4. Click **Next**.

The **Review** page is displayed.

You can examine and modify the created service order parameters. Alternatively, you can click the corresponding buttons at the top of the wizard page to navigate to the specific pages.

5. Click **Done**. The **Confirmation** dialogue box appears.

You can choose one of the following options:

- **Save & Validate**
- **Save & Deploy**

6. Click **Ok** to confirm the deployment option.

Specifying QoS Settings

CoS profiles enable the grouping of class-of-service (CoS) parameters and apply them to one or more interfaces. Connectivity Services Director provides you with predefined traffic types for each CoS profile that you create. These traffic types represent the most common types of traffic for the device type. Each of these templates has preconfigured values for all CoS parameters based on the typical application requirements. You can change the preconfigured values of these parameters to suit your requirements. To display the CoS Profiles page, in Build mode, select CoS under Profile and Configuration Management in the Tasks pane. The Manage CoS Profiles page appears.

If QoS is enabled on the service definition, configure the QoS Settings of the Site Settings panel of the service order creation wizard.

1. In the **QoS profile** field, select a profile from the list.

The **QoS profile** list displays the QoS profiles that are currently configured in the Manage CoS Profiles page of the Connectivity Services Director application.

A QoS profile classifies traffic into defined service groups to provide the special treatment of traffic across the network service.

Specifying Template Settings

The Template Settings page of the service order creation and modification wizards enables you to associate service templates with a point-to-point, VPLS, and Layer 3 VPN service order. You can apply only the templates that are previously configured in a service definition with the corresponding service order. The Template Settings page is available in the service order wizard only if the service definition that you selected to apply to the service order contains a service template. Otherwise, the Template Settings page is not displayed in the service order wizard. You can perform template operations for all endpoints in a service order.

If you defined a service template as the default service template, it is attached to the endpoint by default. You have the flexibility to create and provision a dynamic attribute in a service template. You can mark an attribute of a service template as dynamic, and you can obtain the values for these dynamic attributes from a specific device. To create a dynamic attribute, you must first mark an attribute of a service template as dynamic and then specify the device XPath for the dynamic attribute.

The Template Settings page is displayed before the Review page, which is the final step of the service order wizard.

In the Service Settings page of the Select Service Definition field of the service order creation wizard, you can double-click a service definition name displayed in the table to view the details of the definition in a popup dialog box. You can use this information to determine if the service definition is appropriate for your deployment needs. To filter and sort the display of service templates, enter the name of the template as a match criterion in the Search box and click the Search icon. The page refreshes to display only the template names that match with the search term. You can use the paging controls to navigate across multiple pages of templates as necessary.

All the tasks that you can perform with service templates are presented in the Template Settings page. The page is divided into three panes. The top half of the page displays a table of selected endpoints. All the endpoints or UNIs that you selected in the preceding pages of the service order wizard are displayed in this table. You can configure the template pertaining to only one endpoint at a point in time. If the selected endpoints (in previous pages of the wizard) contained a manually-entered unit number, that number is displayed in the table of selected endpoints. Otherwise, the Auto-pick label is displayed.

The lower half of the page is divided into two panes. The left pane displays the template selection table for the endpoint you selected. All the templates associated with the service definition are displayed. You can add and delete templates using the template selection table. The right pane displays all the parameters that you can modify for a selected service template. All such editable parameters are displayed in a consolidated form of a configuration page. This pane is displayed after you select a template. If any configuration parameter in template is set as a service-specific value, such attributes are not displayed in this pane.

To associate a service template with a service order:

1. Click **Add** to include a service template for the endpoint. A dialog box is displayed with the list of service templates associated with the service definition that is used to create the service order. The templates selected in this dialog box are displayed in the Template Selection table for the specified endpoint. Such templates are considered to be attached to that endpoint.

If you specified a template as a default template during the service definition creation, the template is displayed by default in the template selection table. You can associate non-default templates with the service order by clicking the **Add** button.

2. Click the link in the template name to open the Template Details dialog box. The template settings are displayed in the popup dialog box. For the selected template, the Configuration Page is displayed in the lower-right pane of the Template Settings page.
3. Modify any template-specific service components as necessary.
4. Click **Save** to submit the changes.
5. Select a template from the Template Selection table, and click Delete to remove the template from being associated with the service order for a particular endpoint.

Reviewing the Configured Settings

You can examine and modify the created service order parameters in the **Review** page of the **Create Layer 3 VPN Service Order** wizard.

If you want to modify a particular section in the review page, click the **Edit** button corresponding to that section.

Click **Done** to save the service order. The **Confirmation** dialogue box appears.

Deploying the New Service

From the **Confirmation** dialogue box that appears, you can choose one of the following options to deploy the service:

- Choose **Save & Validate** to validate the service.
- Choose **Save & Deploy** to deploy the service immediately.

The service order is now complete.

Related Documentation

- [Stitching a Pseudowire to an L3VPN Service on page 939](#)
- [Creating a Hub-and-Spoke Layer 3 VPN Service Order on page 964](#)
- [Selecting a Published L3VPN Service Definition for a Service Order on page 985](#)

Creating a Hub-and-Spoke Layer 3 VPN Service Order

Connectivity Services Director can configure and deploy Layer 3 VPN hub-and-spoke service orders. Creating a hub-and-spoke layer 3 service order involves the following tasks:

1. [Selecting the Service Definition on page 964](#)
2. [Configuring Service Parameters Information on page 965](#)
3. [Selecting N-PE Devices or Nodes on page 969](#)
4. [Setting Attributes for Endpoints or Nodes on page 970](#)
5. [Adding and Deleting UNI Interfaces on page 976](#)
6. [Setting Attributes for UNIs or Sites on page 976](#)
7. [Specifying QoS Settings on page 982](#)
8. [Specifying Template Settings on page 983](#)
9. [Reviewing the Configured Settings on page 984](#)
10. [Deploying the New Service on page 985](#)

Selecting the Service Definition

To select a service definition on which to base the new service order:

1. From the Connectivity Services Director application, select **Service View** from the Views list.

The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** tab in the Task Categories banner. The features that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, click the plus sign (+) to expand the tree and select the type of service.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
5. Select the **L3VPN Services** and from the Tasks pane, select **Service Provisioning > Manage Services**.

The Manage Network Services page is displayed in the top half of the right pane, which displays all of the configured services. The Manage Service Orders page is displayed in the bottom half of the right pane, which displays all of the service orders corresponding to a service.

- From the **Manage Network Services** page, select **New > Layer 3 VPN Service Order**.

The Service Settings page in the Create Layer 3 VPN Service Order wizard is displayed.

- From the Service Definition field, click **Select** to choose the service definition you want to base your service order on. The Choose Service Definition inventory page displays a view of only those published service definitions designed to work with the type of services you need.

Based on the fields or parameters that you defined in the service definition to be enabled for modification in the service order, the corresponding fields are available for editing. The fields that are disabled for modification in the service order can only be edited in the service definition.

- Select the check box beside the service definition that you want to associate with the service order, and click **OK**.

Configuring Service Parameters Information

In this topic you configure general settings, VPN settings that can be applied to all end points, and routing protocol settings for the provider edge (PE) and customer edge (CE) devices.

- [Specifying General Settings on page 965](#)
- [Specifying PE-CE Settings Information on page 968](#)

Specifying General Settings

To specify general information for a layer 3 VPN service order:

The screenshot shows the 'Create L3VPN Service Order' wizard with the 'Service Settings' tab selected. The page is divided into several sections:

- General Settings:**
 - Name:** A text input field.
 - Comments:** A text area.
 - Customer:** A dropdown menu with 'Demo' selected, and 'Select' and 'Clear' buttons.
 - Service Definition:** A dropdown menu with 'L3VPN-OSPF-Static(Hub-Spoke-1-1)' selected, and 'Select' and 'View' buttons.
 - Instance Type:** A dropdown menu with 'vrf' selected.
 - ☐ **Enable Distinct Instance Name**
- Connectivity Settings:**
 - ☒ **Policy Based Route Target**
 - ☒ **Auto pick Hub Route Target**
 - ☒ **Auto pick Spoke Route Target**
- VPN Settings:**
 - PE-CE Settings:**
 - Routing Protocol:** A dropdown menu with 'OSPF/Static Route' selected.
 - OSPF Domain ID:** A text input field.
 - OSPF Version:** A dropdown menu with 'Ver 2' selected.

At the bottom right, there are navigation buttons: **Back**, **Next**, **Done**, and **Cancel**.

1. Fill in the fields on the Service Settings page as indicated in [Table 116 on page 944](#).

Table 123: Layer 3 VPN Service Order - Service Settings

Field	Description
General Settings	
Name	<p>Type a unique name for the service. The service order name can consist of only letters, numbers, and underscores.</p> <p>NOTE: The name you specify for a Layer 3 VPN Service Order becomes the routing-instance name in the device configuration when you deploy the service.</p>
Comments	Type a description of the service.
Customer	<p>Click Select to select name of the enterprise customer that requests for a service.</p> <p>Click Clear to clear the current selection.</p>
Service Definition	<ul style="list-style-type: none"> Click Select to choose a service definition from the Choose Service Definition pop-up. The Service Order is created based on the service definition you choose. Select the check box beside the service definition that you want to associate with the service order, and click OK. Click View to view details of the service definition you selected. <p>The type of Service Definition you choose determines the fields that are available in the Connectivity Settings section, VPN Settings section, and the PE-CE Settings section of the Settings Page of the Layer 3 VPN Service Order wizard.</p>
Instance Type	The type of Service Definition you choose will determine the Instance Type displayed in the field.
Enable Distinct Instance Name	Select this check box to specify a distinct instance name for each device.
Connectivity Settings	
Policy Based Route Target	<p>Select this check box to create a policy-based vrf instance.</p> <p>Clear this check box to create a community-based vrf instance.</p> <p>For more information on creating policies for a Layer 3 VPN service, see "Creating Policies for a Layer 3 VPN Service" on page 998.</p>
Auto Pick Route Target	<p>Clear this check box, to enable the Route Target field.</p> <p>To override this setting in the service order, you can select the Editable in Service Order check box in the create Layer 3 full-mesh service definition wizard.</p>

Table 123: Layer 3 VPN Service Order - Service Settings (continued)

Field	Description
Route Target	<p>Specify the route target range in any of the following formats:</p> <ul style="list-style-type: none"> AS Number format: <ul style="list-style-type: none"> AS Number Range: 1 through 4294967295 IPv4 address format: <ul style="list-style-type: none"> If AS Number or IP is less than or equal to 65535, range is 0 through 65535. If AS Number or IP is greater than 65535, range is 0 through 4294967295. <p>NOTE: You must clear the Auto Pick Route Target check box to enable this field.</p>
Auto Pick Hub Route Target	<p>Select this check box to automatically generate a Hub Route Target.</p> <p>Clear this check box to manually enter a Hub Route Target.</p> <p>NOTE: The Auto Pick Hub Route Target check box is visible if the selected Instance Type is vrf.</p> <p>You can edit this field if you select the Editable in Service Order check box in the Create Layer 3 Hub-and-Spoke Service Definition wizard.</p>
Hub Route Target	<p>Specify the hub route target range in any of the following formats:</p> <ul style="list-style-type: none"> prefix-number:assigned-number Prefix-number can be any numeric value from 1 through 65535. Assigned-number can be any numeric value from 0 through 2147483647. IPV4-address:assigned-number IPV4-address can be any valid IPv4 address, and assigned-number can be any numeric value from 0 through 65635. <p>NOTE: To manually enter the Hub Route Target, clear the Auto Pick Hub Route Target check box.</p>
Auto Pick Spoke Route Target	<p>Select this check box to automatically generate a Spoke Route Target.</p> <p>Clear the Auto Pick Spoke Route Target check box to manually enter a Spoke Route Target.</p> <p>NOTE: The Auto Pick Spoke Route Target check box is visible only if Instance Type selected is vrf.</p> <p>You can edit this field if you select the Editable in Service Order check box in the Create Layer 3 Hub-and-Spoke Service Definition wizard.</p>
Spoke Route Target	<p>Specify the spoke route target range in any of the following formats:</p> <ul style="list-style-type: none"> prefix-number:assigned-number Prefix-number can be any numeric value from 1 through 65535. Assigned-number can be any numeric value from 0 through 2147483647. IPV4-address:assigned-number IPV4-address can be any valid IPv4 address, and assigned-number can be any numeric value from 0 through 65635.
VPN Settings	

Table 123: Layer 3 VPN Service Order - Service Settings (continued)

Field	Description
VRF Table Label	<p>Select this check box while creating a service definition to configure a separate label for each VRF to provide double lookup and egress filtering.</p> <p>This check box is visible only if the selected Instance Type is vrf.</p>
Export Direct Routes	Select this check box in the Create Layer 3 Full Mesh Service Definition wizard to export direct routes.
Enable Auto Export Routes	You can select this check box in the Create Layer 3 VPN Service Definition wizard to enable internal and external route leak as part of route target creation.
Import Internal Routes	Select this check box in the Create Layer 3 VPN Service Definition wizard to enable the internal route leak feature as part of route target policy creation.
Import External Routes	Select this check box in the Create Layer 3 VPN Service Definition wizard to enable the external route leak feature as part of route target policy creation.
Enable MVPN	<p>Select this check box to enable multicast VPN (MPVN) settings.</p> <p>If you select this check box, the Enable MC-LAG check box is disabled.</p>
Default UNI Settings	
MTU Factor	<p>Specify a value for MTU Factor in the range 1 through 1087902. The default value for MTU Factor is 10.</p> <p>The value you configure for MTU Factor should not exceed one tenth of the value you configured for burst size.</p> <p>NOTE: This field is enabled only if you select MTU Based as the Burst Size.</p>
Burst Period	<p>Specify a value for Burst Period in the range 10 through 1000. The default value for Burst Period is 10.</p> <p>NOTE: This field is enabled only when you select Line Rate Based as the Burst Size.</p>

Specifying PE-CE Settings Information

You configure VPN attributes that are usually common for all the endpoints in the service. Depending on the service definition on which the service order is based, the values that you provide vary.

If you do not expect these attributes to be the same on all endpoints, you can set them to be the same for now and then make changes later, or you can skip this step and apply the attribute values one at a time later.

Fill in the PE-CE Settings as indicated in [Table 124 on page 969](#):

Table 124: Layer 3 VPN Service Order - PE-CE Settings

Field	Description
PE-CE Settings	
Routing Protocol	The routing protocol in use is displayed.
AS Override	<p>Select this check box to allow a service provisioner to override the AS number.</p> <p>This check box is available if you select BGP as the routing protocol while creating the service definition.</p>
Maximum Prefixes	<p>Range: 1 through 4294967295</p> <p>This feature limits the number of unique destinations in a routing instance.</p>
OSPF Domain ID	<ul style="list-style-type: none"> • ID Range Prefix: 1 through 65535 • ID Range Postfix: 0 through 4294967295 <p>This check box is available only if you select OSPF as the routing protocol while creating the service definition.</p>
OSPF Version	<p>Choose an OSPF version from the OSPF Version list:</p> <ul style="list-style-type: none"> • Ver 2 • Ver 3 <p>Junos OS supports OSPF version 2 (OSPFv2) and OSPF version 3 (OSPFv3).</p> <p>This check box is available only if OSPF is selected as the routing protocol while creating the service definition.</p>

Click **Next**

The **Node Settings** page appears.

Selecting N-PE Devices or Nodes

In this topic you select the N-PE devices that you want to host the service endpoints.

To select endpoint N-PE devices:

1. Click **Add** in the **Node Settings** page of the **Create Layer 3 VPN Service Order** wizard to add a device.

A new row is added to the existing table.



NOTE: You can create a new policy by clicking **Create Policy**.

This option is available if you select **Policy Based Route Target** check box and clear the **Auto Pick Route Target** check box.

For more information on creating a policy, see [“Creating Policies for a Layer 3 VPN Service” on page 998](#)

2. Click the arrow in the name field.
3. From the list, select a device you want to add to the service.
You can select more than one device.
4. Click **OK**.

The device is added to the table.



NOTE: You can modify the device settings by selecting the check box next to the device and clicking **Edit**.

Click **Ok** to save your changes.

Continue with modifying or entering the node parameters.

Setting Attributes for Endpoints or Nodes

If a service template is attached to the service definition, there is a link to that template at the bottom of the **Endpoint Settings** section of the window. For instructions on working with service templates in service orders, see [“Creating a Service Order Based on a Service Definition with a Template” on page 990](#).

You set attributes for each endpoint in the service from the **Node Settings** page.

The screenshot shows the 'Create L3VPN Service Order' window with the 'Node Settings' tab selected. The breadcrumb trail indicates 'You are here: Node Settings'. The main area contains a table with the following columns: Name, IP Address, Stitching Point, Hub, and Route Distinguisher (Autopick, RD Value). A single row is listed with the name 'R260EL_1s'. The 'Stitching Point' and 'Hub' columns have checkboxes that are currently unchecked. The 'Autopick' checkbox is also unchecked, and the 'RD Value' is 'N/A'. At the bottom right, there are buttons for 'Back', 'Next', 'Done', and 'Cancel'.

For each endpoint, the **Node Settings** window shows the value for each UNI attribute.

You can enter topology settings, create static routes on the service, and enter MVPN/PIM settings in the Node Settings page. To specify these settings for a CE device on the Node Settings page:

1. Select the device and click **Edit**.

The Node Settings window appears.

2. Fill in the fields to configure or change topology settings as indicated in [Table 125 on page 971](#):

Table 125: Layer 3 VPN Service Order - Topology Settings

Field	Description
Topology	<p>The type of network circuit in use is displayed in this field:</p> <ul style="list-style-type: none"> • Full Mesh • Hub-and-spoke
Is Stitching Point	<p>Clear this check box.</p> <p>If you select the Is Stitching Point check box, all the parameters of that endpoint are disabled.</p>
Is Hub	<p>Select this check box to enable the node to function as a hub.</p> <p>Clear this check box if you want the device to function as a spoke.</p> <p>NOTE: This field is not applicable for full-mesh layer 3 VPN services.</p>

Table 125: Layer 3 VPN Service Order - Topology Settings (continued)

Field	Description
Import RT Policy	<p>Select a policy from the list.</p> <p>Policies associated with other devices and policies created as part of the service is listed. You can select more than one policy.</p> <p>You have the option to:</p> <ul style="list-style-type: none"> • Select a policy from the list. • Clear the current selection by clicking Clear. <p>NOTE: You can also add or delete a policy while modifying the service.</p>
Export RT Policy	<p>Select a policy from the list</p> <p>Policies associated with other devices and policies created as part of the service is listed. You can select more than one policy.</p> <p>You have the option to:</p> <ul style="list-style-type: none"> • Select a policy from the list. • Clear the current selection by clicking Clear. <p>NOTE: You can also add or delete a policy while modifying the service.</p>
Auto pick Route Distinguisher	<p>Select this check box to assign the Route Distinguisher automatically.</p> <p>This field is enabled if you have selected the Editable in Service Order check box in the service definition.</p>
Route Distinguisher	<p>Enter a valid Route Distinguisher range:</p> <ul style="list-style-type: none"> • as-number:id—Range: 1 through 65535 • ip-address:id—Range: <ul style="list-style-type: none"> • ip address: any unique unicast address • id: 1 through 65535 <p>Each routing instance must have a unique route distinguisher (RD) associated with it. The RD is used to place bounds around a VPN so that the same IP address prefixes can be used in different VPNs without any overlap.</p> <p>This field is available only if you have selected full-mesh as the service type while creating the service definition.</p>
Auto pick Hub Route Distinguisher	<p>Select this check box to assign the Hub Route Distinguisher automatically.</p> <p>This field is enabled if you selected the Editable in Service Order check box in the service definition.</p>

Table 125: Layer 3 VPN Service Order - Topology Settings (continued)

Field	Description
Hub Route Distinguisher	<p>Enter a valid Hub Route Distinguisher range:</p> <ul style="list-style-type: none"> as-number:id—Range: 1 through 65535 ip-address:id—Range: <ul style="list-style-type: none"> ip address: any unique unicast address id: 1 through 65535 <p>This field is available only if you selected hub-and-spoke as the service type while creating the service definition.</p>
Auto pick Spoke Route Distinguisher	<p>Select this check box to assign the Spoke Route Distinguisher automatically.</p> <p>This field is enabled only if you selected the Editable in Service Order check box in the service definition.</p>
Spoke Route Distinguisher	<p>Enter a valid Spoke Route Distinguisher range:</p> <ul style="list-style-type: none"> as-number:id—Range: 1 through 65535 ip-address:id—Range: <ul style="list-style-type: none"> ip address: any globally unique unicast address id: 1 through 65535 <p>This field is available only if you selected hub-and-spoke as the service type while creating the service definition.</p>

3. Fill in the fields to create static routes on the service as indicated in [Table 119 on page 952](#):

Table 126: Layer 3 VPN Service Order - Static Routes

Field	Action
Destination Prefix	<p>Enter the endpoint for the static route in this field.</p> <ul style="list-style-type: none"> IP address—Destination IP address that the router uses to identify packets. Network mask—Network mask for associated IP subnet. Netmask value: 0-32
Option Type	<p>Choose an option type from the Option Type list:</p> <ul style="list-style-type: none"> next-hop next-table community
Hop Address	<p>Enter a valid IP address in this field. You can have multiple hop for every destination prefix.</p> <p>This field is available only if you choose next-hop as the Option Type.</p>

Table 126: Layer 3 VPN Service Order - Static Routes (continued)

Field	Action
Route Table Name	<p>Choose one of the following options as the route table name:</p> <ul style="list-style-type: none"> inet.0 inet.3 <p>This field is available only if you choose next-table as the Option Type.</p>
Member	<p>Choose one of the following values as the member type:</p> <ul style="list-style-type: none"> no-export no-advertise no-export-subconfed <p>This field is available only if you choose community as the Option Type.</p>
Add	<p>Click Add to a static route to the Static Route Table.</p> <p>A new row is added to the table.</p>
Delete	<p>Select the row you want to delete and click Delete to remove the static route from the Static Route Table.</p>
Attribute	The Attribute column displays the Option Type you select
Attribute Value	The Attribute Value column displays the corresponding value for every Option Type you select.

4. Specify the MVPN and PIM Settings as indicated in [Table 127 on page 974](#):



NOTE: The MVPN and PIM Settings sections are displayed only if you select the **Enable MVPN** check box in the Service Settings page of the Create Layer 3 VPN Service Order wizard.

Table 127: Layer 3 VPN Service Order - MVPN and PIM Settings

Field	Description
PIM Settings	
PIM Mode	<p>Choose the PIM Mode from the list.</p> <p>Only sparse mode is currently supported.</p>
MVPN Settings	
MVPN Mode	<p>Choose one of the following MVPN mode from the MVPN Mode list:</p> <ul style="list-style-type: none"> rpt-spt spt-only

Table 127: Layer 3 VPN Service Order - MVPN and PIM Settings (continued)

Field	Description
Site Type	<p>Choose one of the following MBGP MVPN site type from the list:</p> <ul style="list-style-type: none"> • sender • receiver
Provider Tunnel Name	Specify the provider tunnel name to configure virtual private LAN service (VPLS) flooding of unknown unicast, broadcast, and multicast traffic using point-to-multipoint LSPs in this field. You can also configure point-to-multipoint LSPs for MBGP MVPNs.
Upstream Multicast Hop	Select this check box to configure the upstream multicast hop (UMH).
Import Target	<p>Specify the import targets for sender and receiver sites in this field.</p> <p>Select the Sender radio button to import targets for sender sites, select the Receiver radio button to import targets for receiver sites.</p>
Import Unicast Target	<p>Specify the import targets specifically for sender sites or receiver sites in this field. You can also borrow import targets from a configured unicast route target.</p> <p>NOTE: A sender site export route target is always advertised when security association routes are exported. By default, the VPN routing and forwarding (VRF) import and export route targets (configured either using VRF import and export policies or using the vrf-target statement) are used for importing and exporting routes with the MBGP MVPN network layer reachability information (NLRI).</p>
Export Unicast Target	Select this check box to specify the export target to enable you to override the Layer 3 VPN export route targets used for importing and exporting routes for the MBGP MVPN network layer reachability information (NLRI).
Auto pick Export Target	Select this check box to enable automatic selection of an export target if a configuration is not provided.
Target Community	<p>Specify the target community value to be used when exporting sender and receiver site routes in this field.</p> <p>You can specify this value manually if you clear the Autopick Export Target check box.</p>

Click **Ok** to accept all configured values.

Click **Cancel** to reject all configured values.

5. Click **Next** when you have finished configuring node settings.

The Site Settings page is displayed.

Adding and Deleting UNI Interfaces

In the Site Settings page, you can add or delete UNI interfaces on the PE devices that participate in a service.

To add a UNI interface on a selected device:

1. Click **Add** to add a new row to the table
2. From the newly added row, click the arrow in the **Device Name** field.

A list of UNI devices is displayed.

3. Select the check boxes beside the UNIs that you want to associate with the service order and click **Ok**. You can select more than one UNI.

The table now displays the UNI interfaces configured on the selected device.

To delete a UNI Interface from a selected device, select the check box next to the interface you want to delete, and click the **Delete** button above the table.



NOTE: If the deleted UNI is the only UNI selected from the device, then the device is deleted from the service configuration.

Setting Attributes for UNIs or Sites

If there is a service template attached to the service definition, there is a link to that template at the bottom of the Site Settings section of the screen. For instructions on working with service templates in service orders, see [“Creating a Service Order Based on a Service Definition with a Template” on page 990](#).

This part of the create Ethernet service order procedure sets the attributes for each UNI or interface in the service. Selection is made using the Site Settings screen.

The interface shown in the UNI Interface field is automatically selected by the Connectivity Services Director application, which chooses the UNI that has the highest available capacity among interfaces that are in the Up state. To calculate the available capacity of the interface, the system subtracts the bandwidth reserved for each service deployed on that interface from the total capacity of the interface.

For each endpoint, the Site Settings page shows the value for each UNI attribute.

To modify the values of a UNI interface:

1. To modify the device settings, select the device by clicking the check box next to it.

The row is highlighted in blue.

2. You can alter details in the row based on [Table 128 on page 977](#):

Table 128: Layer 3 VPN Service Order - Modify or alter UNI Interface

Field	Description
Device Name	Displays the name of the device associated with the UNI.
Interface Name	<p>Displays the selected interface name.</p> <p>To add a new interface:</p> <ol style="list-style-type: none"> Click the arrow in the Interface Name field. To select the interface, select the check box that corresponds to the interface. Click Ok. <p>The interface name is displayed and the corresponding fields are updated.</p>
Interface Status	<p>Displays the interface's status.</p> <ul style="list-style-type: none"> A Green Up arrow indicates devices that are up and running. A Red Down arrow indicates devices that are down.
Unit Autopick	<p>Select this check box to assign the Unit ID automatically.</p> <p>Clear this check box to assign the Unit ID manually.</p>
Unit ID	<p>Enter a value in this field.</p> <p>Range: 1 through 1073741823</p> <p>This field is available only if you clear the Unit Autopick checkbox.</p>
VLAN Tagging	<p>Select one of the following options from the list:</p> <ul style="list-style-type: none"> Port Dot1Q QinQ(All) QinQ(Single) <p>Specifying the Dot1Q Ethernet option enables you to apply a Unit ID, a single VLAN ID, a VLAN Range, or a VLAN list to the service order.</p> <p>Specifying the QinQ Ethernet option enables you to apply a single VLAN, a VLAN Range, or a VLAN list to the service order. For an L3VPN service deployed on a dual tagged interface, the inner tag determines the VPN routing and forwarding instance(VRF).</p>
VLAN Autopick	<p>Select this check box to assign the VLAN Outer ID automatically.</p> <p>Clear this check box to assign the VLAN Outer ID manually.</p>

Table 128: Layer 3 VPN Service Order - Modify or alter UNI Interface (continued)

Field	Description
VLAN Outer	Enter a value in this field. This field is available if you clear the Unit Autopick check box.
VLAN Inner	Enter a value in this field. This field is available if you choose Dot1Q or QinQ(All) as the VLAN Tagging value.
IP Autopick	Select this check box to assign the IP address automatically. Clear this check box to assign the IP address manually. You cannot edit this check box if you have not selected the Editable in Service Order check box in the service definition.
IP Address	You can enter an IP address in this field if you have cleared the IP Autopick check box. You can choose an IP address from the list if you have selected the IP Autopick check box.
IP Subnet	Enter a valid IP subnet in this field.

To configure or edit Site Settings:

1. Select the interface that you want to edit by clicking the check box next to it.
The selected row is highlighted in blue.
2. You can edit the interface details by following [Table 129 on page 978](#):

Table 129: Layer 3 VPN Service Order - Configure Site Settings

Field	Action
Site Settings	
Interface	The name of the interface you choose is displayed in this field.
Description	Type a description that describes the UNI Interface. Range: 0 to 128 characters.
UNI Settings	

Table 129: Layer 3 VPN Service Order - Configure Site Settings (continued)

Field	Action
Encapsulation	<p>Choose an encapsulation value from the Encapsulation list:</p> <ul style="list-style-type: none"> • Port • Dot1Q • QinQ(Single) • QinQ(All) <p>If you choose Port as the encapsulation value, no field in the UNI settings section is enabled.</p> <p>If you choose Dot1Q as the encapsulation value, Auto pick Interface Unit and Auto pick VLAN ID check boxes are enabled.</p> <p>If you choose QinQ(Single) or QinQ(All) as the encapsulation value, Customer VLAN Type and Outer TP ID fields are enabled.</p>
Auto pick Interface Unit	<p>Select this check box to automatically assign the Unit ID.</p> <p>Clear this check box to manually enter the Unit ID.</p>
Unit ID	<p>Enter a unit ID in this field.</p> <p>Range - 1 through 16385</p> <p>This field becomes available when you clear the Auto pick Interface Unit check box.</p>
Auto pick VLAN ID	<p>Select this check box to assign the VLAN ID automatically.</p> <p>Clear this check box to manually enter the VLAN ID.</p>
VLAN ID	<p>Enter a VLAN ID in this field.</p> <p>Range - 1 through 4094</p> <p>This field becomes available when you clear the Auto pick VLAN ID check box.</p>
Customer VLAN Type	<p>Choose a customer VLAN type from the Customer VLAN Type drop down box:</p> <ul style="list-style-type: none"> • Transport All Traffic—Transports traffic from all VLANs across the network • Transport Single VLAN—Transports traffic for a specific VLAN across the network. <p>This field is available only when the encapsulation value you selected is QinQ(Single) or QinQ(All)</p>
Customer VLAN ID	<p>Enter a Customer VLAN ID in this field.</p> <p>Range - 1 through 4094</p> <p>This field is available only when you select Transport Single VLAN as the Customer VLAN type.</p>
Outer TP ID	<p>Choose a value form the Outer TP ID list:</p> <ul style="list-style-type: none"> • empty (default) • 0x8100 • 0x88a8 • 0x9100

Table 129: Layer 3 VPN Service Order - Configure Site Settings (continued)

Field	Action
Inner TP ID	<p>Choose a value form the Inner TP ID list:</p> <ul style="list-style-type: none"> • empty (default) • 0x8100 • 0x88a8 • 0x9100 <p>This field is available when you select Transport Single VLAN as the customer VLAN type.</p>
IP Settings	
Autopick Interface IP	<p>Select this check box to choose an interface IP from IP Address Pool drop down list.</p> <p>Clear this check box to manually enter an interface IP in the Interface IP Address field.</p>
IP Pool Type	<p>Displays the IP Pool Type you have selected.</p> <ul style="list-style-type: none"> • Global • Customer • None
Interface IP Address	<p>Enter an interface IP address.</p> <p>This field is available only when you clear the Autopick Interface IP check box.</p>
IP Address Pool	<p>Choose an interface IP address from the IP Address Pool list.</p> <p>This field is available only if you select the Autopick Interface IP check box.</p>
IP Block size	<p>Enter a valid IP address block size value in this field.</p> <p>Range - 1 through 32</p>
PE-CE Settings	
Routing Protocol	<p>Select a protocol from the list:</p> <ul style="list-style-type: none"> • BGP • OSPF • Static
OSPF Area ID	<p>Enter an OSPF area id.</p> <p>Valid IP Range - 0.0.0.0 through 255.255.255.255</p> <p>This field is available only if OSPF is selected as the routing protocol in the service definition.</p>
OSPF Version	<p>Enter an OSPF version number.</p> <ul style="list-style-type: none"> • Ver 2 • Ver 3 <p>This field is available only if OSPF is selected as the routing protocol in the service definition.</p>

Table 129: Layer 3 VPN Service Order - Configure Site Settings (continued)

Field	Action
Group Name	<p>Enter a group name.</p> <p>Range - 0 to 255 characters</p> <p>This field is available only if BGP is selected as the routing protocol in the service definition.</p>
Local Address	<p>This field is available if BGP is selected as the routing protocol in the service definition.</p>
Autopick Neighbour IP	<p>Select this field if you want to automatically generate a Neighbour IP. You can edit this field if you select Editable in Service Order check box.</p> <p>This field is available only if BGP is selected as the routing protocol in the service definition.</p>
Neighbour IP	<p>Enter a valid IP address in this field.</p> <p>Range - 1.0.0.1 through 223.225.225.254, excluding 127.x.x.x</p> <p>This field is available if BGP is selected as the routing protocol in the service definition.</p>
Peer AS	<p>Enter a Peer AS range in this field.</p> <p>Range - 1 through 4294967295</p> <p>This field is available if BGP is selected as the routing protocol in the service definition.</p>
Import Policy	<p>Select the policy from the list.</p> <p>Policies associated with other devices and policies created as part of the service is listed. You can select more than one policy from the list.</p> <p>You also have the option to:</p> <ul style="list-style-type: none"> • Select a policy from the list. • Clear the current selection by clicking Clear. <p>You can also add or delete a policy while modifying the service.</p>
Export Policy	<p>Select the policy from the list.</p> <p>Policies associated with other devices and policies created as part of the service is listed. You can select more than one policy from the list.</p> <ul style="list-style-type: none"> • Select a policy from the list. • Clear the current selection by clicking Clear. <p>You can add or delete a policy while modifying the service.</p>
PIM Settings	
Add	<p>Click Add to add a new row in the PIM Settings table.</p>
Delete	<p>Click Delete to delete a row from the PIM Settings table.</p>
Rendezvous Point (device)	<p>Click the arrow in this field to select a device from the drop down list.</p>

Table 129: Layer 3 VPN Service Order - Configure Site Settings (continued)

Field	Action
Group Address	Enter a group IP address. Range - 224.0.1.0 through 239.255.255.255
Update or Cancel	Click Update to update the Rendezvous Point (device) and Group Address to the PIM Settings table. Click Cancel to cancel any updates.

- Click **Ok** after you enter the site settings details in the **Site Settings** window.

Alternatively, click **Cancel** if you do not want to make any change.

The site settings page is displayed.

- Click **Next**.

The **Review** page is displayed.

You can examine and modify the created service order parameters. Alternatively, you can click the corresponding buttons at the top of the wizard page to navigate to the specific pages.

- Click **Done**. The **Confirmation** dialogue box appears.

You can choose one of the following options:

- **Save & Validate**
- **Save & Deploy**

- Click **Ok** to confirm the deployment option.

Specifying QoS Settings

CoS profiles enable the grouping of class-of-service (CoS) parameters and apply them to one or more interfaces. Connectivity Services Director provides you with predefined traffic types for each CoS profile that you create. These traffic types represent the most common types of traffic for the device type. Each of these templates has preconfigured values for all CoS parameters based on the typical application requirements. You can change the preconfigured values of these parameters to suit your requirements. To display the CoS Profiles page, in Build mode, select CoS under Profile and Configuration Management in the Tasks pane. The Manage CoS Profiles page appears.

If QoS is enabled on the service definition, configure the QoS Settings of the Site Settings panel of the service order creation wizard.

1. In the **QoS profile** field, select a profile from the list.

The **QoS profile** list displays the QoS profiles that are currently configured in the Manage CoS Profiles page of the Connectivity Services Director application.

A QoS profile classifies traffic into defined service groups to provide the special treatment of traffic across the network service.

Specifying Template Settings

The Template Settings page of the service order creation and modification wizards enables you to associate service templates with a point-to-point, VPLS, and Layer 3 VPN service order. You can apply only the templates that are previously configured in a service definition with the corresponding service order. The Template Settings page is available in the service order wizard only if the service definition that you selected to apply to the service order contains a service template. Otherwise, the Template Settings page is not displayed in the service order wizard. You can perform template operations for all endpoints in a service order.

If you defined a service template as the default service template, it is attached to the endpoint by default. You have the flexibility to create and provision a dynamic attribute in a service template. You can mark an attribute of a service template as dynamic, and you can obtain the values for these dynamic attributes from a specific device. To create a dynamic attribute, you must first mark an attribute of a service template as dynamic and then specify the device XPath for the dynamic attribute.

The Template Settings page is displayed before the Review page, which is the final step of the service order wizard.

In the Service Settings page of the Select Service Definition field of the service order creation wizard, you can double-click a service definition name displayed in the table to view the details of the definition in a popup dialog box. You can use this information to determine if the service definition is appropriate for your deployment needs. To filter and sort the display of service templates, enter the name of the template as a match criterion in the Search box and click the Search icon. The page refreshes to display only the template names that match with the search term. You can use the paging controls to navigate across multiple pages of templates as necessary.

All the tasks that you can perform with service templates are presented in the Template Settings page. The page is divided into three panes. The top half of the page displays a table of selected endpoints. All the endpoints or UNIs that you selected in the preceding pages of the service order wizard are displayed in this table. You can configure the template pertaining to only one endpoint at a point in time. If the selected endpoints (in previous pages of the wizard) contained a manually-entered unit number, that number is displayed in the table of selected endpoints. Otherwise, the Auto-pick label is displayed.

The lower half of the page is divided into two panes. The left pane displays the template selection table for the endpoint you selected. All the templates associated with the service definition are displayed. You can add and delete templates using the template selection table. The right pane displays all the parameters that you can modify for a selected service template. All such editable parameters are displayed in a consolidated

form of a configuration page. This pane is displayed after you select a template. If any configuration parameter in template is set as a service-specific value, such attributes are not displayed in this pane.

To associate a service template with a service order:

1. Click **Add** to include a service template for the endpoint. The templates selected in this dialog box are displayed in the Template Selection table for the specified endpoint. Such templates are considered to be attached to that endpoint.

When you click **Add**, a dialog box is displayed with the list of service templates associated with the service definition that is used to create the service order. If you specified a template as a default template during the service definition creation, the template is displayed by default in the template selection table. You can associate non-default templates with the service order by clicking the **Add** button.

2. Click the link in the template name to open the Template Details dialog box. The template settings are displayed in the popup dialog box. For the selected template, the Configuration Page is displayed in the lower-right pane of the Template Settings page.
3. Modify any template-specific service components as necessary.
4. Click **Save** to submit the changes.
5. Select a template from the Template Selection table, and click Delete to remove the template from being associated with the service order for a particular endpoint.

Reviewing the Configured Settings

You can examine and modify the created service order parameters in the **Review** page of the **Create Layer 3 VPN Service Order** wizard.

Create L3VPN Service Order

Service Settings > Node Settings > Site Settings > Review

You are here: Review

General Settings

Service Order Name: tempSO
 Customer Name: Demo
 Service Definition Name: L3VPN-OSPF-Static-Hub-Spoke-1-Interface
 Service Type: L3 VPN (Hub-Spoke 1 Interface)
 Instance Type: vrf
 Enable Distinct Instance Name: false

Connectivity Settings

VPN Settings

PE-CE Settings

Node Settings

Name	IP Address	IsStitchingPoint	IsHub	RouteDistinguisher
R099EL_0	10.220.10.35	false	true	Autopick

Page 1 of 1

Displaying 1 - 1 of 1 | Show 10 Items

Back Next Done Cancel

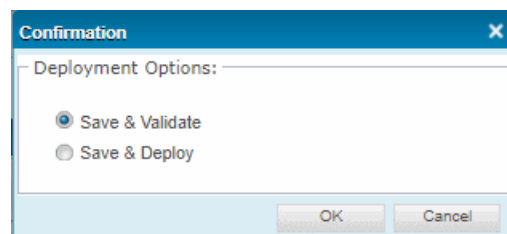
If you want to modify a particular section in the review page, click the **Edit** button corresponding to that section.

Click **Done** to save the service order. The **Confirmation** dialogue box appears.

Deploying the New Service

From the **Confirmation** dialogue box that appears, you can choose one of the following options to deploy the service:

- Choose **Save & Validate** to validate the service.
- Choose **Save & Deploy** to deploy the service immediately.



The service order is now complete.

Related Documentation

- [Stitching a Pseudowire to an L3VPN Service on page 939](#)
- [Creating a Full Mesh Layer 3 VPN Ethernet Service Order on page 941](#)
- [Selecting a Published L3VPN Service Definition for a Service Order on page 985](#)

Selecting a Published L3VPN Service Definition for a Service Order

To select a service definition on which to base the new service order:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the View pane, click the plus sign (+) to expand the tree and select the type of service.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.

5. From the Tasks pane, select **Service Provisioning > Deploy Services**.

The Manage Network Services page is displayed in the top half of the right pane, which displays all of the configured services. The Manage Service Orders page is displayed in the bottom half of the right pane, which displays all of the service orders corresponding to a service.

6. In the **Manage Network Services** page, select **New > L3 VPN Service Order**.

The **Choose Service Definition** inventory page, which opens when you click **Select** from the Service Definition Name field of the Service Settings page of the service order creation wizard, displays a view of only those published service definitions designed to work with Layer 3 VPN Ethernet services you need.

7. Select the service definition you want to base your service order on, then click **Next** to display the **Service Parameters** window.

Related Documentation

- [Stitching a Pseudowire to an L3VPN Service on page 939](#)
- [Creating a Full Mesh Layer 3 VPN Ethernet Service Order on page 941](#)
- [Creating a Hub-and-Spoke Layer 3 VPN Service Order on page 964](#)

Entering Layer 3 VPN Order Information

You, the Service Activator must set settings for a L3 VPN service order, including general settings, VPN settings that are applied to all end points, and routing protocol settings for the PE and CE devices.

1. [Setting General Settings on page 986](#)
2. [Entering VPN and Connectivity Settings Information on page 987](#)
3. [Entering PE-CE Settings on page 988](#)

Setting General Settings

Before You Begin

- You must add the customer to the database that requested the service order before proceeding. See [“Adding a New Customer” on page 737](#).

You must specify the following general information about the service order in the General Settings section of the Service Parameters page:

1. In the **Name** field, enter a unique name for the Layer 3 VPN service.

The service order name can consist of only letters, numbers, and underscores. It must be no longer than 50 characters.



NOTE: The name you specify for a Layer 3 VPN service order becomes the routing-instance name in the device configuration when you deploy the service. Consequently, you cannot use any Juniper Networks keywords, for example, “bgp” or “ospf”, as the name of a service order.

2. In the **Customer** drop-down list box, select the customer who requested the service.
If the customer is not in the list, you must add the customer to the database before proceeding. See [“Adding a New Customer” on page 737](#).
3. In the **Comments** field, enter a description of the service no longer than 200 characters. This description appears in information screens about the request or service instance created from the request.

You cannot change the **Route Target** field. Route targets are always selected automatically.

Entering VPN and Connectivity Settings Information

You must set VPN attributes that are usually common for all the endpoints in the service. The values that you enter vary, depending on the service definition on which the service order is based.

If these attributes will not be the same on all endpoints, you can set them to be the same for now and then make changes later, or you can choose to skip this step and apply the attribute values one at a time later.

To set attributes common to most endpoints on a service:

1. The **Autopick VLAN ID** option is automatically selected for Network Activate to automatically choose the VLAN ID. Deselect the check box if you want to manually assign the VLAN ID.

The **VLAN ID** text box appears.
2. If you deselected the **Autopick VLAN ID** option, enter a value in the **VLAN ID** field.
3. The **Autopick Route Target** option is selected, and you cannot deselect it. Network Activate automatically selects the route target.
4. The **Autopick Route Distinguisher** option is selected, and you cannot deselect it.
5. The **Autopick Interface IP Address** option is selected, and you cannot deselect it. Network Activate automatically selects the interface IP address.
6. The **VRF Table label** option is selected, and you cannot deselect it. Network Activate automatically selects the interface IP address.

Entering PE-CE Settings

In the **PE-CE Settings** section of the Service Parameters page, depending on the PE-CE routing protocol—OSPF/Static Route or BGP/Static Route—do one of the following:

- If **BGP/Static Route routing protocol** is specified in the service definition:
 - a. The **AS override** option is selected to allow a service provisioner to override the AS number. Clear the **AS override** check box to prevent a service provisioner from overriding the AS number.
 - b. Enter a value for the maximum number of prefixes accepted by a PE router from a CE router.
- If **OSPF/Static Route routing protocol** is specified in the service definition, in the **OSPF domain ID** field, enter a IP address.

You can enter from 1.0.0.1 to 223.255.255.254. excluding 127.x.x.x.

1. Click **Next**.

The **Node Parameters** page appears.

Related Documentation

- [Stitching a Pseudowire to an L3VPN Service on page 939](#)
- [Creating a Full Mesh Layer 3 VPN Ethernet Service Order on page 941](#)
- [Creating a Hub-and-Spoke Layer 3 VPN Service Order on page 964](#)
- [Selecting a Published L3VPN Service Definition for a Service Order on page 985](#)

Selecting Endpoint PE Devices or Nodes



NOTE: The Choose Endpoints window, which you can open by clicking **Add** above the Nodes table on the Node Parameters page of the Create L3VPN Service Order wizard, shows only assigned NPE devices that have an AS number configured. If you do not see the device you are looking for, use the CLI on the device to check for and assign an AS number.

N-PE devices that are L2VPN-only will not appear.

To select endpoint N-PE devices:

1. In the **Node Parameters** page, click **Add** in the Service Nodes table. From the Choose Endpoints dialog box that appears, select the devices that you want to participate in the service. Use the multiple selection feature to select one or more devices.

Figure 46: Choose Endpoints Dialog Box

<input type="checkbox"/>	Name	IP Address	State	Managed State	Platform	OS Version	Roles
<input checked="" type="checkbox"/>	960R2_EP_Alok_re	10.216.194.110	up	In Sync	MX960	14.2-20140916.0	N_PE
<input type="checkbox"/>	480R4_EP_Alok_re	10.216.194.105	up	In Sync	MX480	14.2-20140916.0	N_PE
<input type="checkbox"/>	480R3_EP_Alok_re	10.216.194.108	up	In Sync	MX480	14.2-20140916.0	N_PE
<input type="checkbox"/>	960R1_EP_Alok_re	10.216.194.118	up	In Sync	MX960	14.2-20140916.0	N_PE
<input type="checkbox"/>	RouterZ-re	10.92.35.185	down	In Sync	MX960	15.1-20141022_L...	N_PE
<input type="checkbox"/>	RouterY-re	10.92.35.187	up	In Sync	MX960	15.1-20141022_L...	N_PE
<input type="checkbox"/>	RouterX-re	10.92.35.189	up	In Sync	MX960	15.1-20141022_L...	N_PE
<input type="checkbox"/>	RouterXCore-re	10.92.35.183	down	In Sync	MX960	15.1-20141022_L...	-
<input type="checkbox"/>	Merg1_006_re	10.92.37.13	up	In Sync	MX960	15.1-20150727_...	N_PE

Page 1 of 3 Displaying 1 - 9 of 25 Show 9 items

<input type="checkbox"/>	Name	Status	Encapsulation	Index
<input type="checkbox"/>	ae0	down	none	508
<input type="checkbox"/>	ae1	down	none	509
<input type="checkbox"/>	em1	up	none	23
<input type="checkbox"/>	em2	up	none	116
<input type="checkbox"/>	ge-0/0/2	up	flexible-ethernet-services	533
<input type="checkbox"/>	ge-0/0/3	up	flexible-ethernet-services	539
<input type="checkbox"/>	ge-0/0/4	up	flexible-ethernet-services	542
<input type="checkbox"/>	ge-0/0/5	up	none	550
<input type="checkbox"/>	ge-0/0/6	up	none	551
<input type="checkbox"/>	ge-0/0/7	up	none	552
<input type="checkbox"/>	ge-0/0/8	up	none	553
<input type="checkbox"/>	ge-0/0/9	up	none	554

OK Cancel



NOTE: In the Choose Endpoints dialog box, you can sort and segregate the devices and their corresponding interfaces based on the roles of the devices to easily and quickly view only the devices of interest. Click the down arrow on the Filter Role menu, and select P2E to view only the provider edge devices, P to view only the provider devices, and L2E to view only Layer 2 Ethernet devices.

2. Based on the devices you select in the top half of the dialog box, the interfaces that are present in the selected device are displayed in the lower half of the dialog box. Select the check boxes next to the interfaces that you want to associate with the service.

3. Click **OK**.

The **Node Parameters** window appears.

4. Continue with modifying or entering the node parameters.

**Related
Documentation**

- [Stitching a Pseudowire to an L3VPN Service on page 939](#)
- [Creating a Full Mesh Layer 3 VPN Ethernet Service Order on page 941](#)
- [Creating a Hub-and-Spoke Layer 3 VPN Service Order on page 964](#)
- [Selecting a Published L3VPN Service Definition for a Service Order on page 985](#)

Creating a Service Order Based on a Service Definition with a Template

Creating a service order using a service definition with service templates attached to it facilitates endpoint configuration.

By means of a template, a number of service attributes identified by the service definition designer can be not only applied as a group to one or more endpoints in a service order, but also, in some cases, edited. Some attributes can only be set by service provisioners. For this reason, service definition designers can make these values editable by the service provisioner during service order creation.

A service definition can have multiple templates attached to it. If you use a definition with more than one template, you are not obliged to apply the same settings to all endpoints. You can create a service order in which each endpoint is configured using a different template. In other words, each endpoint can use a subset of templates defined in the service definition, and there, template choice is per service order.

From a service provisioner's perspective, the service template takes the form of a collection of flexible service attributes accessible through a link in the service order.

This topic describes how to work with a service template from within a service order, that is, while creating the service order.

These instructions assume that the service order is based on a service definition that has at least one template attached to it. The instructions apply to a definition with multiple templates, because the procedure for a definition with a single template is simpler.

To see if a definition has any templates before you begin creating a service order, view the details of the definition on the Service Settings page of the **Select Service Definition** field of **Create... Service Order**. The presence or absence of an attached Service Template is indicated below **Name** and **Type**.

To configure a service order based on a service definition with multiple templates:

1. To start creating a service order, follow the instructions in the topic listed below that is relevant to your service order type :
 - [Creating a Point-to-Point Service Order on page 829](#)
 - [Creating a Multipoint-to-Multipoint VPLS Service Order on page 881](#)
 - [Creating a Point-to-Multipoint VPLS Service Order on page 905](#)
 - [Creating a Full Mesh Layer 3 VPN Ethernet Service Order on page 941](#)
 - [Creating a Hub-and-Spoke Layer 3 VPN Service Order on page 964](#)
2. At the **Node Parameters** page, with an endpoint selected, make the appropriate selection or enter the appropriate data (guidelines for this are in [“Creating a Point-to-Point Service Order” on page 829](#)).
3. (Optional for a service definition containing multiple templates). Examine all the attributes in all the templates to determine whether to apply all templates to all endpoints. You can delete templates and add templates back at will.
4. To display and, if necessary, edit the attributes a page contains, select the page in the panel on the left.

On the right, underneath the name of the page, appear the attributes on the selected page of the template.

Usually the names of the attributes are ambiguous (for example, “description,”), therefore you must mouse over the field next to the name to see its context in the DMI schema hierarchy.
5. For each page in each applicable template, make the appropriate changes in the field on the right.
6. (Optional) If you determine that one of the templates contained in the definition is superfluous, select it in the panel on the left.

The name of the first page of the template appears at the top of the panel on the right.
7. Click the red “X” icon near the top of the panel on the left.

The template disappears.



NOTE: If you delete a template by mistake, you can add it again. Click the green “+” icon.

The Add Template window appears, displaying a list of all the templates previously deleted from the current endpoint's group of flexible service attributes.

Select the templates you want to add, and click Add Template.

The Flexible Service Attributes window reappears, displaying the newly added templates

-
8. When you have finished configuring the current endpoint's group of flexible service attributes, click **OK**.

The Endpoint Settings page reappears.

9. (Optional) Repeat the preceding steps for other endpoints.

To verify your work:

1. In Deploy mode, select a service from the Service View pane, and navigate to **Service Provisioning > Deploy Services** in the task pane, select the service you deployed, and select **View Service Configuration Change** from the **Actions** drawer.

The **Service Configuration** window opens.

2. Select the appropriate device from the panel on the left.

If a template was deployed to the device, the **Template Configuration** tab appears to the right of the **Service Configuration** tab.

3. Click the **Template Configuration** tab to display the configlet that was deployed as a result of the template.

Related Documentation

- [Stitching a Pseudowire to an L3VPN Service on page 939](#)
- [Creating a Full Mesh Layer 3 VPN Ethernet Service Order on page 941](#)
- [Creating a Hub-and-Spoke Layer 3 VPN Service Order on page 964](#)
- [Selecting a Published L3VPN Service Definition for a Service Order on page 985](#)
- [Entering Layer 3 VPN Order Information on page 986](#)
- [Selecting Endpoint PE Devices or Nodes on page 988](#)

Deploying a Layer 3 VPN Service Order

You must deploy a service for it to run on devices in the network.

To deploy the service, make selections from the **Manage Service Orders** window.

1. Select **Service View** from the View Selector. The workspaces that are applicable to network and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the View pane, click the plus sign (+) to expand the tree and select the type of service.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
5. From the Tasks pane, select **Service Provisioning > Deploy Services**.

The Manage Network Services page is displayed in the top half of the right pane, which displays all of the configured services. The Manage Service Orders page is displayed in the bottom half of the right pane, which displays all of the service orders corresponding to a service.

Figure 47: Manage Service Orders Page

The image shows a 'Confirmation' dialog box with a blue header. The main text reads 'Confirm Delete partial configuration of' followed by a text field containing 'ldp_fm_test1'. Below this is a section titled 'Deployment Options:' containing two radio buttons: 'Partial Delete Now' (which is selected) and 'Partial Delete Later'. Under 'Partial Delete Later', there are date and time pickers. The date is set to '2015-08-31' and the time is set to '12:00:00'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

6. Select the check box next to an L3VPN service in the Manage Network Services page. The corresponding service orders for the selected service are displayed in the Manage Service Orders page in the lower half of the main display area.
7. Select the check box next to the L3VPN service order you want to deploy.
8. Perform one of these actions from Deploy mode in the Service View of Connectivity Services Director :
 - To deploy the service immediately, select **Deploy now** and then click **OK**.
 - To deploy the service later, select **Schedule deployment**, select a date and time, and then click **OK**.
The time field specifies the time kept by the server, but in the time zone of the client.
 - To validate the service, click **Validate**.
9. Use the Deploy Configuration page to view the job and monitor the status of the service deployment.

Related Documentation

- [Stitching a Pseudowire to an L3VPN Service on page 939](#)
- [Creating a Full Mesh Layer 3 VPN Ethernet Service Order on page 941](#)
- [Creating a Hub-and-Spoke Layer 3 VPN Service Order on page 964](#)
- [Selecting a Published L3VPN Service Definition for a Service Order on page 985](#)
- [Entering Layer 3 VPN Order Information on page 986](#)

- [Selecting Endpoint PE Devices or Nodes on page 988](#)
- [Creating a Service Order Based on a Service Definition with a Template on page 990](#)

Creating a Multicast VPN Service Order

This topic describes how to use the Connectivity Services Director application to create a Multicast VPN (MVPN) service order.



NOTE: Multicast VPN services are supported on LN2600 and MX devices only.

1. Select **Service View** from the View Selector. The workspaces that are applicable to network and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the View pane, click the plus sign (+) to expand the tree and select the type of service.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
5. From the Tasks pane, select **Service Provisioning > Deploy Services**.
 The Manage Network Services page is displayed in the top half of the right pane, which displays all of the configured services. The Manage Service Orders page is displayed in the bottom half of the right pane, which displays all of the service orders corresponding to a service.
6. To select a service definition on which to base the new service order, from the Network Services page, select **New > L3VPN Service Order**.
7. In the **Service Parameters** window, from the **Select Service Definition** field, select the service definition upon which you want to base your service order.

8. In the **Service Parameters** window, enter the service attributes-related information in the relevant fields as described in the following table:

Field	Description
Service Definition	The service definition upon which this service order is based.
Name	Type a name for the service order.
Customer	Enter the customer for which you are creating the service order.
Comments	Enter comments to describe the service order (optional).
MVPN	If selected, this check box indicates that the service order is intended to function in a Multicast VPN. This check box is selected if it was selected in the service definition upon which this service order is based.
VPN Settings	The VPN settings listed in this panel correspond to the settings selected in the service definition upon which this service order is based.
Autopick VLAN ID	This check box is selected automatically if it was selected in the service definition upon which this service order is based.
Autopick Hub Route Target	This check box is selected automatically if it was selected in the service definition upon which this service order is based.
Autopick Spoke Route Target	This check box is selected automatically if it was selected in the service definition upon which this service order is based.
Autopick Hub Route Distinguisher	This check box is selected automatically if it was selected in the service definition upon which this service order is based.
Autopick Spoke Route Distinguisher	This check box is selected automatically if it was selected in the service definition upon which this service order is based.
Autopick Interface IP Address	This check box is selected automatically if it was selected in the service definition upon which this service order is based.
VRF Table Label	This check box is selected automatically if it was selected in the service definition upon which this service order is based.
Export Direct Routes	This check box is selected automatically if it was selected in the service definition upon which this service order is based.
PE-CE Settings	
Routing Protocol	OSPF/Static Route—This routing protocol corresponds to the protocol selected in the service definition upon which this service order is based.
OSPF domain ID	This field is optional. Range: 1.0.0.1 to 223.255.255.254 (excluding 127.x.x.x)

9. Click **Next**.
10. Select the device for which you want to implement the service order.
11. Click **Next**.
12. In the **Site Settings** window, enter information as described in the following table:

Field	Description
Choose Endpoints	
Device	Add the devices for which you intend to implement this service order.
UNI Interface	Select the interface on each device for which you intend to implement this service order.
UNI Description	<p>Enter the description for the selected UNI interface. The Description field is displayed in Modify Service Order, View Service Order Details, Modify Service, and View Service windows. You can edit this field while modifying a Layer 3 VPN service order or service.</p> <p>Range: 0 through 128 characters</p>
Set loopback	<p>Select this check box to create a loopback interface for the service order.</p> <p>NOTE: If you provision a loopback interface for an L3VPN service, an operator is able to identify a VRF routing instance. Thereafter, an operator can manually ping a remote CE router from a local PE router.</p>
Encapsulation	<p>VLAN</p> <p>This field displays the value specified in the service definition upon which you are basing this service order.</p>
UNI interface	Select the interface on the device for which you intend to implement this service order.
Autopick interface IP	This check box is selected automatically if it was selected in the service definition upon which this service order is based.
IP pool type	<p>Global</p> <p>This field displays the value specified in the service definition upon which this service order is based.</p>
IP address pool	Select the IP address pool from the list.
IP block size	This field displays the value specified in the service definition upon which this service order is based.
Autopick VLAN ID	This check box is selected automatically if it was selected in the service definition upon which this service order is based.

Field	Description
Routing protocol	BGP This field displays the value specified in the service definition upon which this service order is based.
Autopick neighbor IP	This check box is selected automatically if it was selected in the service definition upon which this service order is based.
Peer AS	The peer autonomous system number. Select a Peer AS from the list.

13. Click **Review**.

14. Click **Finish** to complete the creation of the service order.

Related Documentation

- [Stitching a Pseudowire to an L3VPN Service on page 939](#)
- [Creating a Full Mesh Layer 3 VPN Ethernet Service Order on page 941](#)
- [Creating a Hub-and-Spoke Layer 3 VPN Service Order on page 964](#)
- [Selecting a Published L3VPN Service Definition for a Service Order on page 985](#)
- [Entering Layer 3 VPN Order Information on page 986](#)
- [Selecting Endpoint PE Devices or Nodes on page 988](#)
- [Creating a Service Order Based on a Service Definition with a Template on page 990](#)

Creating Policies for a Layer 3 VPN Service

With Connectivity Services Director Release 2.0R4, you can create route target policies. Route target policies are also called protocol policies or PE–CE protocol policies. In releases earlier than Connectivity Services Director Release 2.0R4, the Connectivity Services Director application automatically generates route target policies. You can create these policies on the Node Settings page of the Create L3VPN Service Order wizard.

To create a route target policy, you must select the **Policy Based Route Target** check box in the Create Layer 3 VPN Definition wizard. If you have cleared the **Policy Based Route Target** check box, the Connectivity Services Director application does not generate the policy.

If you have selected the **Policy Based Route Target** check box, you have an option to create a policy on the Node Settings page of the Create Layer 3 VPN Service Order wizard. If you have not defined a policy in the Create Layer 3 VPN Service Order wizard, the Connectivity Services Director application automatically generates the necessary policy.

Creating PE–CE protocol policies is optional.

1. On the Node Settings page of the Create L3VPN Service Order wizard, click **Create Policy**.

The Policy Settings window appears.

2. Fill in the following fields in the Policy Settings window:

Field	Description
Device Name	This drop down menu lists the devices that are part of the Layer 3 VPN service. Select a device that you want to apply the policy.
Option Settings	
Option Type	<p>Select an option type:</p> <ul style="list-style-type: none"> • Community Specify the following attributes: <ul style="list-style-type: none"> • Community name—Specify the name of the community. Range: 0 through 255 characters • Member—Specify the member value in AS-number or IP address:ID format AS Number Range: 1 through 65535 IP address Range: Globally unique unicast address. • As-path Specify the following attributes: <ul style="list-style-type: none"> • AS-path name—Specify the name of the AS path. Range: 0 through 255 characters • Path—Specify the path. Range: Regular expressions • prefix-list Specify the following attributes: <ul style="list-style-type: none"> • Prefix List Name—Specify the name of the prefix list. Range: 0 through 255 characters • Prefix Address—Specify the prefix address. IP address Range: Globally unique address with subnet mask.
Add	Click Add to validate option attribute values. The attribute is listed in the table.
Delete	Select an attribute from the table and click Delete to delete an option attribute row.
Policy Settings	
Policy Name	<p>Specify the name of the policy.</p> <p>Range: 0 through 255 characters</p>

Field	Description
Name	Specify the name of the policy term. Range: 0 through 255 characters
Clause	Select one of the following clause: <ul style="list-style-type: none">• From• Then
Attribute selection	If the Clause type is From select one of the following attributes: <ul style="list-style-type: none">• route filter• community• protocol• family• as-path• prefix-list• prefix-list-filter If the Clause type is Then , select one of the following attributes: <ul style="list-style-type: none">• community• local-preference• accept• reject
Add	Click Add to validate policy setting values. The attribute is listed in the table.
Delete	Select an attribute from the table and click Delete to delete a policy term.

3. Click **Save**.

The policy is created.

Related •
Documentation

PART 11

Service Provisioning: Working with Services Deployment

- [Service Provisioning: Managing Deployed Services on page 1003](#)

Service Provisioning: Managing Deployed Services

- [Managing Service Configuration Deployment Jobs on page 1003](#)
- [Deploying Services Configuration to Devices on page 1005](#)
- [Deploy Configuration Window on page 1013](#)
- [Deleting a Partial Configuration of an LSP Service Order on page 1014](#)
- [Deleting a Service Order on page 1015](#)
- [Deploying a Service on page 1016](#)
- [Validating the Pending Configuration of a Service Order on page 1018](#)
- [Viewing the Configuration of a Pending Service Order on page 1020](#)
- [Viewing Decommissioned Point-to-Point, VPLS, and L3VPN Service Orders on page 1022](#)
- [Modifying a Point-to-Point Ethernet Service on page 1024](#)
- [Modifying a Multipoint-to-Multipoint Ethernet Service on page 1026](#)
- [Modifying a Point-to-Multipoint Ethernet Service on page 1033](#)
- [Modifying a Hub-and-Spoke Layer 3 VPN Service Order on page 1042](#)
- [Modifying a Full Mesh Layer 3 VPN Ethernet Service on page 1057](#)
- [Understanding Service Validation on page 1063](#)
- [Highlighting of Endpoints in the Layer 3 VPN, RSVP LSP, and VPLS Service Modification Wizards on page 1064](#)

Managing Service Configuration Deployment Jobs

When you Deployment Jobs changes or schedule a configuration deployment, a service configuration deployment job is created.

To start managing configuration deployment jobs:

1. Click **Deploy** in the Connectivity Services Director banner.
2. In the Tasks pane, select **View Deployment Jobs**.

The CSD Deployment Jobs page opens in the bottom part of the main window. The table on that page lists configuration deployment jobs.

This topic describes:

- [Selecting Service Configuration Deployment Job Options on page 1004](#)
- [Viewing Service Configuration Deployment Job Details on page 1005](#)
- [Canceling Service Configuration Deployment Jobs on page 1005](#)

Selecting Service Configuration Deployment Job Options

From the Deployment Jobs page, you can:

- View the details of a service configuration deployment job by clicking Show Details. See [“Viewing Configuration Deployment Job Details” on page 764](#) for more information.
- Cancel a scheduled service configuration deployment job by clicking Cancel Job. See [“Canceling Configuration Deployment Jobs” on page 764](#) for more information.

[Table 99 on page 763](#) describes the information provided on the Deployment Jobs page

Table 130: Deployment Jobs Table Description

Table Column	Description
Check box	Select to perform an action on the job in that row.
Job Id	An identifier assigned to the job.
Job Name	Job name (user-created).
Percent	Percentage of the job that is complete.
Status	Job status. The possible states are: <ul style="list-style-type: none"> • CANCELLED—The job was cancelled by a user. • FAILURE—The job failed. This state is applied if any of the devices in the job failed. But some of the devices might have completed successfully. View the job details for the status of each device. • INPROGRESS—The job is running. • SCHEDULED—The job is scheduled but has not run yet. • SUCCESS—The job completed successfully. This state is applied if all of the devices in the job completed successfully.
Summary	Job summary.
Scheduled Start Time	Job's scheduled start time
Actual Start Time	Time when the job started.
End Time	Time when the job ended
User	User who created the job
Recurrence	This field is not used for configuration deployment jobs.

Viewing Service Configuration Deployment Job Details

To view the details of a configuration deployment job:

1. Select the job in the table.
2. Click **Show Details**. The Deployment Jobs window opens. See *Deploy Configuration Window* for a description of the window.

Canceling Service Configuration Deployment Jobs

To cancel a configuration deployment job:

1. Select the job in the table.
2. Click **Cancel Job**.
3. Click **Yes** in the confirmation window that opens.

Deploying Services Configuration to Devices

When you make configuration changes in Build mode, the changes are not deployed to devices automatically. You must manually deploy the changes to devices in Deploy mode.

To start deploying configuration changes:

1. From the View selector, select **Service View**. The workspaces that are applicable to this view are displayed.
2. Click **Deploy** in the Connectivity Services Director banner.
3. Click the plus sign (+) beside Connectivity to expand the tree in the View pane and view the list of service types.
4. Select the type of service, such as P2P, L2VPN, or VPLS, for which you want to deploy the service order.
5. In the Tasks pane, select **Service Provisioning > Deploy Services**. The Manage Service Deployment window is displayed in the bottom part of the right pane.



TIP: From Build mode of Service View, in the View pane, if you select the Connectivity item in the tree under Network Services, without expanding the tree and selecting a specific service type, such as P2P Services, L3VPN Services, or VPLS Services, the top pane displays a set of five pie charts that enable you to view the different service orders configured, and their associated audit and monitoring statuses. The FA Status chart displays

the functional audit status for the service orders. The Device State graph displays the statuses of devices on which services are being provisioned and commissioned. The Fault Status chart displays the connectivity fault management details for the service orders. The SLA Status chart displays the service-level agreement details for the service orders. The PM Status chart displays the performance management details for the service orders. The count or percentage of service orders in the pie chart segments sum up to the total number of configured service orders. Mouse over each segment of the pie to view the number corresponding to the percentage of service orders for each of the charts. These charts provide a visual overview of customers and service orders on your network, and enables you to quickly access related and commonly needed information. For example, you can check for failed service orders and then access a list of failed requests so you can begin to take restoration measure.

In Build mode of Service View, from the View pane, if you select the Network Services node and do not expand the Network Services > Connectivity tree, the top pane displays a pie chart that enables you to view and examine the different services configured for devices, and the types of service protocols configured. The Services by Type graph displays the count of services for each type of service definition. Mouse over each segment of the pie to view the number corresponding to the percentage of service orders for each of the charts. This chart provides a visual overview of customers and service orders on your network, and enables you to quickly access related and commonly needed information. For example, you can check for failed service orders and then access a list of failed requests so you can begin to take restoration measure.

The following fields are displayed in this window:

- Name—Unique name assigned to the service.
- Customer—Name of the customer for which the service is provided.
- State—Status of the service order. Service orders can be one of the following states:
 - Completed—The service order has been successfully deployed.
 - Scheduled for deployment—The service provisioner has scheduled the service order for deployment.
 - Deployment Failed—An attempted service deployment was not successfully completed or failed an audit.
 - In Progress—The Connectivity Services Director application is in the process of deploying the service.
 - Requested—The service provisioner has created the service order, but has not yet attempted to deploy it or schedule it for deployment.
 - Invalid—The service order is not valid.
- Signaling—Type of signaling, namely, BGP or LDP.

- Created By—Name of the user that created the service order.
- Created Date—Date and time at which the service order was created.

This topic describes:

- [Selecting Configuration Deployment Options on page 1007](#)
- [Validating Configuration on page 1007](#)
- [Deleting the Partial Service Configurations on page 1009](#)
- [Discarding the Pending Configurations on page 1011](#)
- [Deploying Configuration Changes to Devices Immediately on page 1012](#)
- [Scheduling Configuration Deployment on page 1012](#)
- [Specifying Configuration Deployment Scheduling Options on page 1012](#)

Selecting Configuration Deployment Options

Based on the approval mode, you can choose to deploy the device configuration changes in the following ways:

- When you select the auto approval mode, the page **Devices with Pending Changes** open. From the **Devices with Pending Changes** page, you can:
 - Deploy configuration changes immediately by selecting one or more devices and clicking **Deploy Now**. For more information, see [“Deploying Configuration Changes to Devices Immediately” on page 759](#).
 - Schedule configuration deployment by selecting one or more devices and clicking **Schedule Deploy**. For more information, see [“Scheduling Configuration Deployment” on page 759](#).
 - View configuration changes that are pending on a device by clicking **View** in the **Configuration Changes** column.
 - Validate that the pending changes for a device are compatible with the device's configuration by selecting up to ten devices and clicking **Validate Pending Configuration Changes**. For more information, see [“Validating Configuration” on page 756](#).
 - Discard the pending configuration changes. For more information, see [“Discarding the Pending Configurations” on page 1011](#).

Validating Configuration

When you deploy configuration changes to a device, validation checks are performed to validate that the pending changes are compatible with the device. You can also perform this validation without deploying.



NOTE: You can also verify the configuration from the Build mode by clicking **Tasks > Domain Management > Validate Pending Configuration**.

To view the configuration of such service orders:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services > Connectivity** task pane, select **Service Provisioning > Deploy Services**. The Manage Service Deployment page is displayed on the right pane.



TIP: From Build mode of Service View, in the View pane, if you select the Connectivity item in the tree under Network Services, without expanding the tree and selecting a specific service type, such as P2P Services, L3VPN Services, or VPLS Services, the top pane displays a set of five pie charts that enable you to view the different service orders configured, and their associated audit and monitoring statuses. The FA Status chart displays the functional audit status for the service orders. The Device State graph displays the statuses of devices on which services are being provisioned and commissioned. The Fault Status chart displays the connectivity fault management details for the service orders. The SLA Status chart displays the service-level agreement details for the service orders. The PM Status chart displays the performance management details for the service orders. The count or percentage of service orders in the pie chart segments sum up to the total number of configured service orders. Mouse over each segment of the pie to view the number corresponding to the percentage of service orders for each of the charts. These charts provide a visual overview of customers and service orders on your network, and enables you to quickly access related and commonly needed information. For example, you can check for failed service orders and then access a list of failed requests so you can begin to take restoration measure.

In Build mode of Service View, from the View pane, if you select the Network Services node and do not expand the Network Services > Connectivity tree, the top pane displays a pie chart that enables you to view and examine the different services configured for devices, and the types of service protocols configured. The Services by Type graph displays the count of services for each type of service definition. Mouse over each segment of the pie to view the number corresponding to the percentage of service orders for each of the charts. This chart provides a visual overview of customers and service orders on your network, and enables you to quickly access related and commonly needed information. For example, you can check for failed service orders and then access a list of failed requests so you can begin to take restoration measure.

4. Select a service order that is in either of the following states:

- Requested
- Invalid
- Scheduled
- Failed deployment

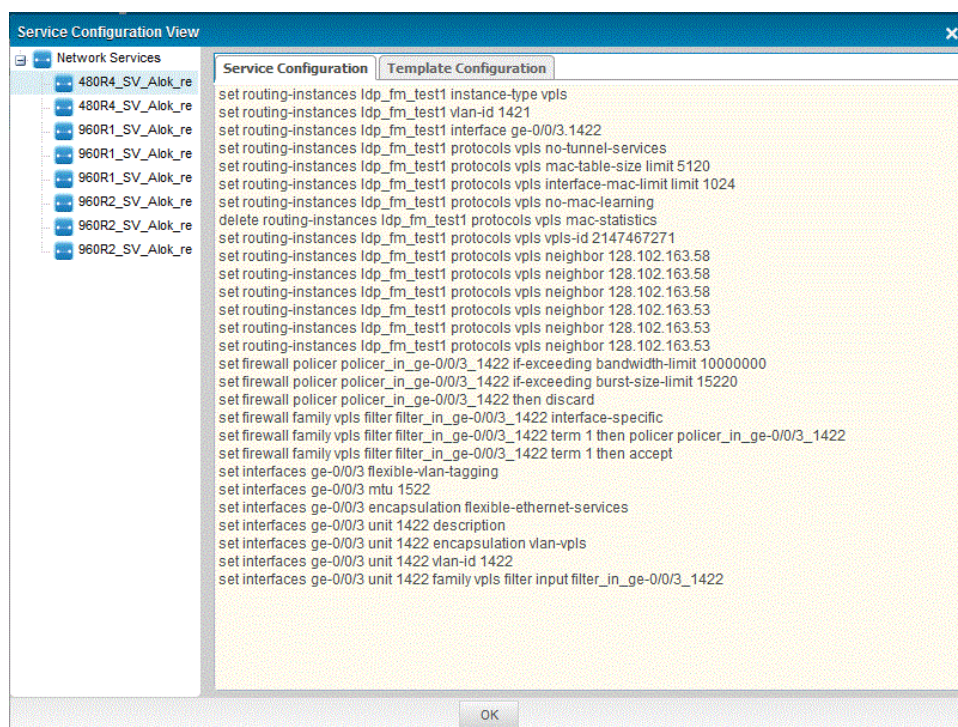


NOTE: The Order State column displays the state of the service order.

- Right-click the service order and select the **View Pending Order Configuration**. The **Pending Order Configuration** window is displayed. The configuration is displayed in xml format.



NOTE: The View Pending Order Configuration appears to be dimmed if the service order state is Completed.



- Select a device to view the configuration details. You can also view the template configuration if a template is attached to the service order.

Deleting the Partial Service Configurations

A failed service order of type Provisioning can leave parts of the service configuration on the devices.

To remove the partial configuration of services that are present on the associated devices of the service order:

1. From the View selector, select **Service View**. The workspaces that you can configure in this view are displayed.
2. Click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that are applicable to this lifecycle mode are displayed.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
5. From the task pane, select **Service Provisioning > Deploy Services**. The top part of the right pane displays the Manage Network Services page, with the table of services, and the bottom part of the right pane displays the Manage Service Orders page, with the table of service orders.
6. From the Manage Service Orders page, select the services for which you want to delete the partial configuration and click **Delete Partial Configuration** from the Actions menu.

A dialog box is displayed, prompting you to specify whether you want to delete the partial service configuration immediately or schedule the partial deletion for a future specified time.
7. To delete the pending changes of the service immediately, select **Partial Delete Now**, and click **OK**. To discard the pending changes of the service at a later time, select **Partial Delete Later**, select a date and time for deletion, then click **OK**. The time field specifies the time kept by the server, but in the time zone of the client. After scheduling the service order for deployment, the provisioning software begins validating the service order.

Figure 48: Delete Partial Configuration Confirmation

Name	Customer	State	Service Type	Signaling	Latest Job	Created Date	Created By
ldp_fm_test1	test	Validated	VPLS	LDP	1310908	August 28, 2015...	super

You are returned to the Manage Service Orders page.

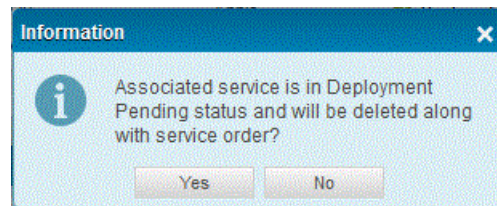
Discarding the Pending Configurations

Use the Discard Local Configuration Changes Results window to discard all the pending service configurations that were made on a device. Once you discard the local configuration changes on a device, the configuration state of the device changes to In Sync or Out of Sync based on the system of record (SOR) mode set for the Junos Space Network Management Platform. If the SOR mode is set to Network as system of record (NSOR), then the configuration state changes to In Sync and if the SOR mode is set to Junos Space as system of record (SSOR), then the configuration state changes to Out of Sync.

To discard the configuration changes:

1. From the View selector, select **Service View**. The workspaces that you can configure in this view are displayed.
2. Click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that are applicable to this lifecycle mode are displayed.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
5. From the task pane, select **Service Provisioning > Deploy Services**. The top part of the right pane displays the Manage Network Services page, with the table of services, and the bottom part of the right pane displays the Manage Service Deployment page, with the table of service orders.
6. From the Manage Service Deployment page, select the services for which you want to discard the pending configuration and click **Discard Pending Configuration** from the Actions menu.
7. You are prompted to confirm whether you want to discard the service order, which causes the associated service to be deleted along with it. Click **OK** to confirm the deletion.

Figure 49: Discard Pending Configuration Confirmation



8. Click **OK** to close the dialog box that displays the job ID. The Manage Service Orders page appears.

Deploying Configuration Changes to Devices Immediately

To deploy configuration changes to devices immediately:

1. Select the check box next to the service you want to deploy from the Manage Service Deployment page.

2. Click **Deploy Now**.

The Deploy Options window opens.

3. In the Deploy Options window, enter a job name in the Deployment Job Name field, then click **OK**.

The configuration deployment job runs. The Deploy Configuration window opens and shows the results of the deployment job.

Scheduling Configuration Deployment

To schedule configuration deployment to devices:

1. Select the check box next to the service you want to deploy from the Manage Service Deployment page.

2. Click **Schedule Deploy**.

The Deploy Options window opens.

3. Use the Deploy Options window to schedule the configuration deployment. See [“Specifying Configuration Deployment Scheduling Options” on page 760](#) for a description of the window.

Specifying Configuration Deployment Scheduling Options

Use the Deploy Options window to schedule configuration deployment jobs.

[Table 98 on page 760](#) describes the actions for the fields in this window.

Table 131: Deploy Options Window

Field	Action
Deployment Job Name	Enter a job name.
Date and Time	Enter the job's start date and time.
OK	Click to accept changes and exit the window.
Cancel	Click to cancel changes and exit the window.

Deploy Configuration Window

The Deploy Configuration window shows the results of a completed deployment job or information about a scheduled job. See [Table 100 on page 764](#) for a description of the fields in this window.

Table 132: Deploy Configuration Window

Field	Description
Job Name	Job name.
Job Start Time	Time when job started or will start.
Job End Time	Time when job ended.
Percentage Completed	Percentage of the job that is complete.
Number of Devices	Number of devices in the deployment job.
Deployed Devices table	
Name	Device name.
IP Address	Device IP address.
Deployment Status	Status of configuration deployment on device: <ul style="list-style-type: none"> • Scheduled—Job is scheduled for future deployment. • In Progress—Deployment is in progress. • Success—Deployment completed successfully. • Failed—Deployment failed.
Configuration	Click View to see the configuration changes that were deployed to the device. See “Deploying Services Configuration to Devices” on page 758 for more information. For a scheduled job, this column does not contain a link. See “Deploying Services Configuration to Devices” on page 1005 for information about viewing pending configuration changes for a device.
Result Details	Click View to see the results of configuration deployment for the device.

Table 132: Deploy Configuration Window (continued)

Field	Description
Close	Click to close the window.

Deleting a Partial Configuration of an LSP Service Order

A failed service order of type Provisioning can leave parts of the service configuration on the devices. To remove this partial configuration:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
5. From the task pane, select **Service Provisioning > Deploy Services**. The top part of the right pane displays the Manage Network Services page, with the table of services, and the bottom part of the right pane displays the Manage Service Deployment page, with the table of service orders.
6. From the **Network Services > Connectivity** task pane, select **Service Provisioning > Deploy Services > service order name**.
7. In the **Manage Service Deployment** page, select the failed service order for which you want to delete the partial configuration.
8. Open the **Actions** menu and select **Delete Partial Configuration**.
9. In the confirmation screen, select **Delete**.

Related Documentation

- [Managing Service Configuration Deployment Jobs on page 1003](#)
- [Deploying Services Configuration to Devices on page 1005](#)
- [Deploy Configuration Window on page 764](#)

- [Managing Jobs on page 118](#)

Deleting a Service Order

You can delete a service order that is in the requested state, the scheduled state, the invalid state, or the failed deployment state.

To delete a service order from the database:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services** task pane, select **Connectivity** or **Tunnel**.
4. In the **Tasks** task pane, select **Decommissioned Service Orders**.
5. In the **Decommissioned Service Orders** page, select the service order to be deleted from the Connectivity Services Director application database.
6. Click **Delete**.

The **Manage Service Deployment** page reappears with the deleted service orders removed.

To delete a service order from a service, which is not decommissioned:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services** task pane, select a service in **Connectivity** or **Tunnel**.
4. In the **Tasks** task pane, select **Service Provisioning > Manage Services**.
5. In the **Manage Network Service** page, select a service from which the service order must be deleted.
6. In the **Manage Service Order** page, select the service order.
7. Click **Actions** menu, and select **Discard pending Configuration**.

The selected service order along with the associated service is deleted.

**Related
Documentation**

- [Creating a Point-to-Point Service Order on page 829](#)
- [Creating a Multipoint-to-Multipoint VPLS Service Order on page 881](#)
- [Creating a Point-to-Multipoint VPLS Service Order on page 905](#)

Deploying a Service

This procedure schedules a service for deployment on the network. Use this procedure to perform the following tasks:

- Deploy a new service.
- Deploy a modified service.
- Redeploy a service order that failed deployment.

You cannot deploy an invalid service order.

To schedule a service for deployment:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services > Connectivity** task pane, select **Service Provisioning > Deploy Services**. The Manage Service Deployment page is displayed on the right pane.



TIP: From Build mode of Service View, in the View pane, if you select the Connectivity item in the tree under Network Services, without expanding the tree and selecting a specific service type, such as P2P Services, L3VPN Services, or VPLS Services, the top pane displays a set of five pie charts that enable you to view the different service orders configured, and their associated audit and monitoring statuses. The FA Status chart displays the functional audit status for the service orders. The Device State graph displays the statuses of devices on which services are being provisioned and commissioned. The Fault Status chart displays the connectivity fault management details for the service orders. The SLA Status chart displays the service-level agreement details for the service orders. The PM Status chart displays the performance management details for the service orders. The count or percentage of service orders in the pie chart segments sum up to the total number of configured service orders. Mouse over each segment of the pie to view the number corresponding to the percentage of service orders for each of the charts. These charts provide a visual overview of customers and service orders on your network, and enables

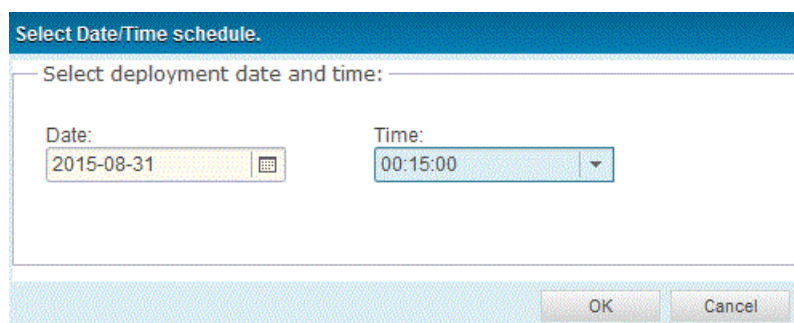
you to quickly access related and commonly needed information. For example, you can check for failed service orders and then access a list of failed requests so you can begin to take restoration measure.

In Build mode of Service View, from the View pane, if you select the Network Services node and do not expand the Network Services > Connectivity tree, the top pane displays a pie chart that enables you to view and examine the different services configured for devices, and the types of service protocols configured. The Services by Type graph displays the count of services for each type of service definition. Mouse over each segment of the pie to view the number corresponding to the percentage of service orders for each of the charts. This chart provides a visual overview of customers and service orders on your network, and enables you to quickly access related and commonly needed information. For example, you can check for failed service orders and then access a list of failed requests so you can begin to take restoration measure.

4. In the **Manage Service Deployment** page, select the service order that you want to deploy.
5. Click the **Deploy Service Order** button at the top of the page.
The **Deploy Service** window appears.
6. To deploy the service immediately, select **Deploy now**, and click **OK**.



To deploy the service at a later time, select **Schedule Deploy**, and select a date and time for deployment, then click **OK**.



The time field specifies the time kept by the server, but in the time zone of the client.

After scheduling the service order for deployment, the provisioning software begins validating the service order.

7. Use the Jobs workspace to monitor the outcome of the deployment.

**Related
Documentation**

- [Validating the Pending Configuration of a Service Order on page 1018](#)
- [Viewing the Configuration of a Pending Service Order on page 1020](#)

Validating the Pending Configuration of a Service Order

This procedure validates a service order but does not push the configuration to the device. Use this procedure to perform the following tasks:

- Validate a service request in the REQUESTED state.
- Validate a service request in the INVALID state after making necessary configuration changes on one or more PE devices associated with the service order.

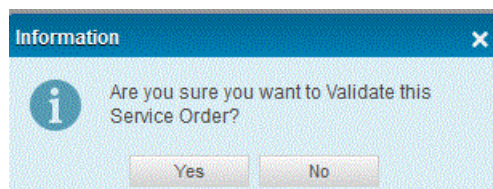
When you create a service order, it is automatically validated in Connectivity Services Director. However, if subsequent changes to service configuration attributes and settings have occurred for the devices or endpoints to which they are associated, you can use the functionality to validate pending service order configuration. You can validate the configuration of a service order that is in the requested state, the scheduled state, the invalid state, or the failed deployment state

To schedule a service order for validation, follow these steps:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
5. From the task pane, select **Service Provisioning > Deploy Services**. The top part of the right pane displays the Manage Network Services page, with the table of services, and the bottom part of the right pane displays the Manage Service Deployment page, with the table of service orders.

6. From the Manage Service Deployment page, select the service order you want to validate and save.
7. Open the **Actions** menu and click **Validate Pending Configuration**.

The **Schedule Service Request Validation** window appears.



8. You can validate a service now or at some future time:
 - To validate the service immediately, select **Validate now**, and click **OK**.
 - To validate the service at a later time, select **Validate later**, select a date and time for deployment, and then click **OK**.



NOTE: When specifying a time to validate the service, the time field specifies the time kept by the server, but in the time zone of the client.

After scheduling the service order for validation, the provisioning software begins validating the service order.

9. You can use the **Job Management** window to view details about the service validation.



NOTE: Alternatively, to display the Job Management page, click the **System** icon on the Connectivity Services Director banner, and select **Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

Related Documentation

- [Deleting a Partial Configuration of an LSP Service Order on page 1014](#)
- [Deleting a Service Order on page 1015](#)
- [Deploying a Service on page 1016](#)

Viewing the Configuration of a Pending Service Order

You can view the configuration of a service order that is in the requested state, the scheduled state, the invalid state, or the failed deployment state.

To view the configuration of such service orders:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the **Network Services > Connectivity** task pane, select **Service Provisioning > Deploy Services**. The Manage Service Deployment page is displayed on the bottom part of the right pane.



TIP: From Build mode of Service View, in the View pane, if you select the Connectivity item in the tree under Network Services, without expanding the tree and selecting a specific service type, such as P2P Services, L3VPN Services, or VPLS Services, the top pane displays a set of five pie charts that enable you to view the different service orders configured, and their associated audit and monitoring statuses. The FA Status chart displays the functional audit status for the service orders. The Device State graph displays the statuses of devices on which services are being provisioned and commissioned. The Fault Status chart displays the connectivity fault management details for the service orders. The SLA Status chart displays the service-level agreement details for the service orders. The PM Status chart displays the performance management details for the service orders. The count or percentage of service orders in the pie chart segments sum up to the total number of configured service orders. Mouse over each segment of the pie to view the number corresponding to the percentage of service orders for each of the charts. These charts provide a visual overview of customers and service orders on your network, and enables you to quickly access related and commonly needed information. For example, you can check for failed service orders and then access a list of failed requests so you can begin to take restoration measure.

In Build mode of Service View, from the View pane, if you select the Network Services node and do not expand the Network Services > Connectivity tree, the top pane displays a pie chart that enables you to view and examine the different services configured for devices, and the types of service protocols configured. The Services by Type graph displays the count of services for each type of service definition. Mouse over each segment of the pie to view the number corresponding to the percentage of service orders for each of the charts. This chart provides a visual overview of customers and service orders on your network, and enables

you to quickly access related and commonly needed information. For example, you can check for failed service orders and then access a list of failed requests so you can begin to take restoration measure.

4. Select a service order that is in either of the following states:

- Requested
 - Invalid
 - Scheduled
 - Failed deployment
-



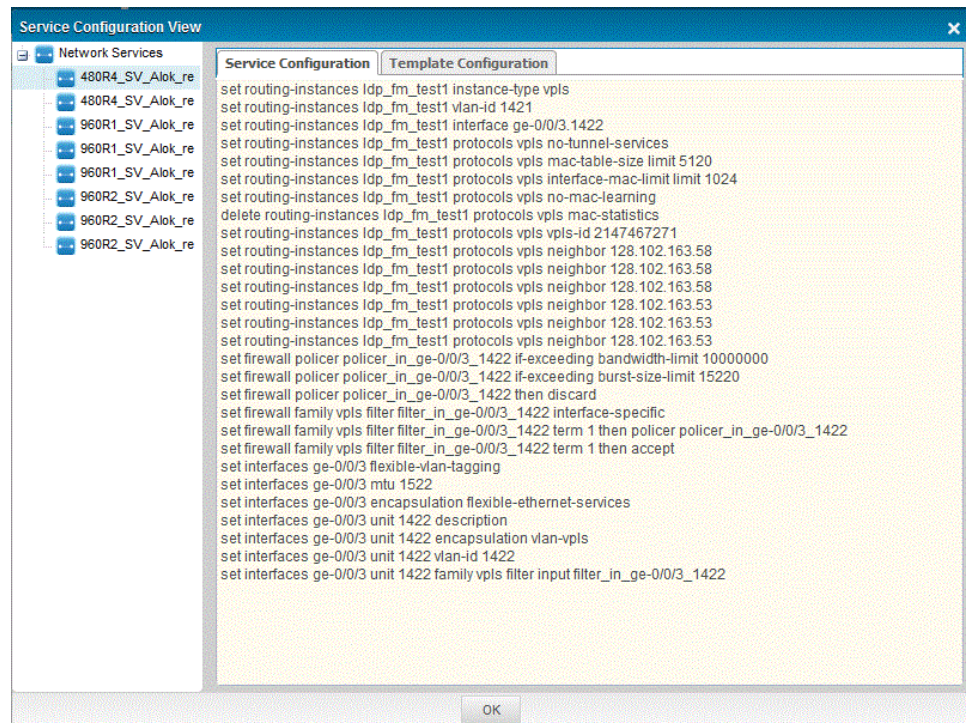
NOTE: The **Order State** column displays the state of the service order.

5. Select the service order for which you want to view the configuration details.

6. Open the **Actions** menu and select the **View Pending Order Configuration** option. The **Pending Order Configuration** window is displayed. The configuration is displayed in xml format.



NOTE: The **View Pending Order Configuration** appears to be dimmed if the service order state is **Completed**.



7. Select a device to view the configuration details. You can also view the template configuration if a template is attached to the service order.

Based on the application's settings, the configuration is displayed in xml format or in set format. To view the configuration in set format:

1. Select **Platform > Administration > Applications > Connectivity Services Director**.
2. Right-click the Connectivity Services Director application and select **Modify Application Settings**. The Modify Connectivity Services Director Settings window is displayed.
3. Select the **show configuration in set format** check box.

Related Documentation

- [Deleting a Partial Configuration of an LSP Service Order on page 1014](#)
- [Deleting a Service Order on page 1015](#)
- [Deploying a Service on page 1016](#)
- [Validating the Pending Configuration of a Service Order on page 1018](#)

Viewing Decommissioned Point-Point, VPLS, and L3VPN Service Orders

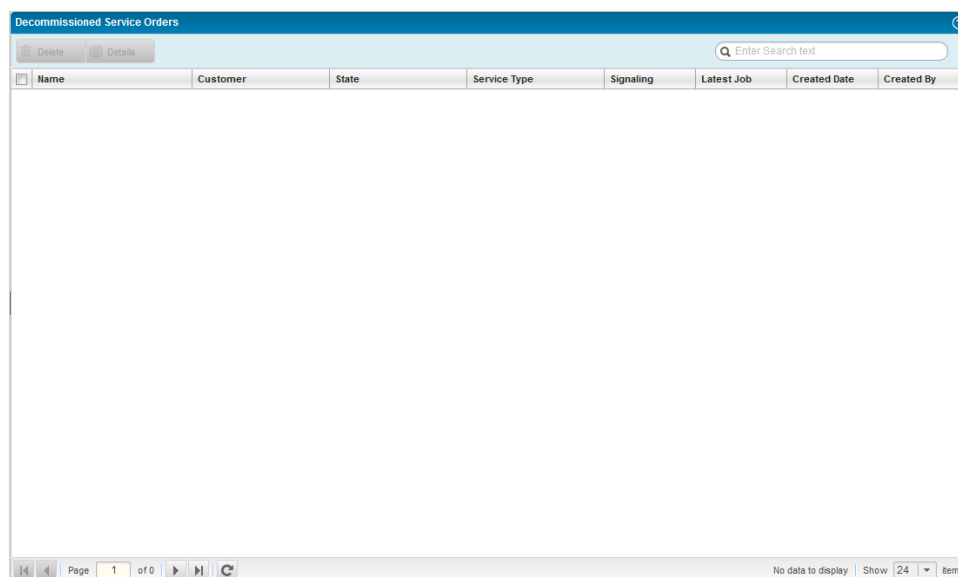
In certain situations, you might decommission a service that a customer no longer needs. You cannot decommission a service if a service order requesting action on that service is in the Requested, Scheduled, In Progress, or Invalid state. You can view the

decommissioned service orders in a separate page to determine whether you want to delete it completely.

To view and determine the status of decommissioned service orders in a tabular form:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the View pane, click the plus sign (+) to expand the Network Services tree, and select the Connectivity node.
4. In the Network Services > Connectivity view pane, select **Service Provisioning > Decommissioned Service Orders**.

The Decommissioned Service Orders page is displayed on the right pane.



A table of service orders on the system appears in the main display area. The following fields are displayed on this page:

- Name—Unique name assigned to the service.
- Customer—Name of the customer for which the service is provided.
- State:
 - Completed—Service order has been successfully deployed.
 - Deploy failed—Device is down or the Connectivity Services Director application was unable to push the service configuration to a device configured for the service.

- In-progress—Connectivity Services Director application is in the process of deploying the service.
- Invalid—Service order contains invalid data.
- Requested—Service provisioner has created the service order, but has not yet attempted to deploy it or schedule it for deployment.
- Scheduled—Service provisioner has scheduled the service order for deployment.
- Service Type:
 - Point-to-point pseudowire (LDP)
 - Point-to-point pseudowire (BGP)
 - VPLS (MultiPoint-to-MultiPoint)
 - VPLS (Point-to-MultiPoint)
 - L3VPN (Full Mesh)
 - L3VPN (Hub-Spoke 1 Interface)
- Latest Job—Unique identifier assigned by the system for a deployment job. Click the link in the job ID to open the CSD Deployment Jobs. The table on that page lists configuration deployment jobs.
- Signaling Type:
 - BGP
 - LDP
- Created By—The screen name of the user who created the service order
- Created Date—The date and when you created the service order.

From this page, you can delete a decommissioned service order and view the details of a service order.

5. Select the check box beside a decommissioned service order that you want to delete, and click **Delete** above the table of listed service orders.

You are prompted to confirm the deletion. Click **OK** to confirm the deletion. The deleted service order is removed from the list of decommissioned service orders.

6. To view details of a specific service order, double-click the table row that summarizes the service order.

Modifying a Point-to-Point Ethernet Service

You can modify the following entities of a point-to-point Ethernet service:

- MTU across the network
- Rate limiting bandwidth of an endpoint

- MTU of an endpoint

After modifying a service, the configuration audit and functional audit information is cleared and the functional audit status is set to pending.

To modify the attributes of a service:



NOTE: When you modify a service or a service order, the read-only fields in the different pages of the wizard for service or service order modification are grayed out to indicate that you cannot modify those attributes.

1. In the **Network Services > Connectivity** task pane, select **Service Provisioning > Manage Services**.
2. In the **Manage Services** page, select the service you want to modify.
3. Click the **Modify** icon at the top of the page.
A graphical image of the service appears, showing device images that represent the service endpoints. The General Settings box contains a unique name for the service order that will request the change.
4. In the **Name** field, change the name of the modification service order, if desired.
5. Change the MTU setting, as required.
6. If you have configured the CFM, the **General/Connectivity Settings** panel provides an option to disable the CFM service. You can select the **Disable CFM** check box to disable the CFM service, if desired.
If you have not configured the CFM, the **General/Connectivity Settings** panel provides an option to enable the CFM service. You can select the CFM definition from the **OAM Profile** list, if desired.
7. Click **Next**.
The service order endpoint settings information for endpoint A appears in the right panel.
8. Change the bandwidth or MTU setting as required.
9. Change the **Revert time (sec)** and **Switch Over Delay (sec)** as required.
10. Select or clear the **Enable send-oam config** check box.
11. Click **Next** and make any required changes to endpoint Z.

12. Click **Modify**.

The Connectivity Services Director application modifies the service.

13. Use the **System > Manage Jobs > Job Management** workspace to check for successful completion of the action.



NOTE: Alternatively, to display the Job Management page, access the Jobs workspace from the Junos Space Network Management Platform UI, and select **Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

Related Documentation

- [Creating a Multipoint-to-Multipoint VPLS Service Order on page 881](#)
- [Creating a Point-to-Multipoint VPLS Service Order on page 905](#)
- [Creating a Point-to-Point Service Order on page 829](#)

Modifying a Multipoint-to-Multipoint Ethernet Service

For a multipoint-to-multipoint service, you can change the bandwidth or MTU of a specific UNI, add or delete a UNI, change C-VLAN range values, and change advanced settings for a device endpoint or add a new device endpoint.

You cannot change the interface of an existing UNI. Neither can you change the service VLAN ID.

To perform the equivalent of changing the interface on an existing UNI, add a new UNI with the desired interface, and then delete the old UNI.

After modifying a service, the configuration audit and functional audit information is cleared and the functional audit status is set to pending.

Modifying a service creates a new service order based on the attribute settings of the existing service.



NOTE: When you modify a service or a service order, the read-only fields in the different pages of the wizard for service or service order modification are grayed out to indicate that you cannot modify those attributes.

The following topics provide instructions for modifying a multipoint-to-multipoint (full mesh) Ethernet service:

- [Adding an Endpoint on page 1027](#)
- [Adding a UNI Interface on page 1028](#)

- [Deleting a UNI Interface and Deleting an Endpoint on page 1030](#)
- [Changing the Endpoint Bandwidth on page 1031](#)
- [Changing Advanced Settings for an Endpoint on page 1032](#)

Adding an Endpoint

To add an endpoint to a multipoint-to-multipoint Ethernet service:

1. In the Network Services > Connectivity view pane, select **Service Provisioning > Manage Services**.
2. In the **Manage Services** page, select the service to which you want to add an endpoint.
3. Click **Modify** at the top of the table of listed service orders.

Current service settings appear in the main display area. The **General Information** box contains a unique name for the service order that will request the change.

4. In the service **Order name** field, change the name of the modification service order, if desired.
5. If you have configured the CFM, the **Service Parameters** panel provides an option to disable the CFM service. You can select the **Disable CFM** check box to disable the CFM service, if desired.

If you have not configured the CFM, the **Service Parameters** panel provides an option to enable the CFM service. You can select the CFM definition from the **OAM Profile** list, if desired.

6. Click the **Node Settings** button to view the endpoints or devices that are associated with the service.
7. In the **Service Nodes** table, click **Add**.

The **Choose Endpoints** window shows available N-PE devices that are not part of the service.

8. Select the devices on which you want to add new endpoints, then click **OK**. You are returned to the Node Settings page of the Manage Service Orders wizard.

To filter and sort the display of objects, enter the name of the object as a match criterion in the Search box and click the Search icon. The page refreshes to display only the object names that match with the search term. You can use the paging controls to navigate across multiple pages of objects as necessary.

Based on the devices you select in the top half of the dialog box, the interfaces that are present in the selected device are displayed in the lower half of the dialog box. Select the check boxes next to the interfaces that you want to associate with the service.

The service modification window shows the added devices with system recommended choices for UNI. To select a different UNI, see [“Adding a UNI Interface” on page 1028](#). To select a different bandwidth than the applied default, see [“Changing the Endpoint Bandwidth” on page 1031](#).

9. Click **Finish** to complete the modification of the service order and save the settings.
10. In Deploy mode of the Service View of the Connectivity Services Director, select one of the following from the Manage Services page:
 - Schedule the change for immediate deployment.
 - Schedule the change for later deployment.
11. Click **OK**.
12. Use the **System > Manage Jobs > Job Management** workspace to monitor the progress and status of the deployment.



NOTE: Alternatively, to display the Job Management page, from the Junos Space Platform UI, select **Jobs > Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

Adding a UNI Interface

To add a UNI on a device that is already part of a multipoint-to-multipoint Ethernet service:

1. In the Network Services > Connectivity view pane, select **Service Provisioning > Manage Services**.
2. In the **Manage Services** page, select the service to which you want to add a UNI.
3. Click **Modify** at the top of the table of listed service orders.

Current service settings appear in the main display area. The **Service Parameters** box contains a unique name for the service order that will request the change.
4. In the service **Order name** field, change the name of the modification service order, if desired.
5. Click the **Site/Endpoint Settings** button to view the interfaces on endpoints or devices that are associated with the service.
6. In the **User-to-Network Interfaces** table, click **Add**.

The **Choose Endpoints** window shows available N-PE devices that are not part of the service.

7. Select the devices on which you want to add new interfaces. The window refreshes to display all the user-to-network (UNI) or ingress interfaces for the selected device in the lower part of the window as a tabular grid. Select the interfaces that you want to assign to the service order, and then click **OK**.

To filter and sort the display of objects, enter the name of the object as a match criterion in the Search box and click the Search icon. The page refreshes to display only the object names that match with the search term. You can use the paging controls to navigate across multiple pages of objects as necessary.

You are returned to the Node Settings page of the Manage Service Orders wizard.

The service modification window shows the added devices with system recommended choices for UNI. To select a different bandwidth than the applied default, see [“Changing the Endpoint Bandwidth” on page 1031](#).

8. If the interface you selected in the previous step is already configured (duplicate) you must either manually enter a different value in the service VLAN ID fields, or check the **Autopick VLAN ID** field.
9. Select an interface from the UNI Interface column.
10. Click **Finish** to complete the modification of the service order and save the settings.
11. In Deploy mode of the Service View of the Connectivity Services Director, select one of the following from the Manage Services page:
 - Schedule the change for immediate deployment.
 - Schedule the change for later deployment.
12. Click **OK**.
13. Use the **System > Manage Jobs > Job Management** workspace to monitor the progress and status of the deployment.



NOTE: Alternatively, to display the Job Management page, from the Junos Space Platform UI, and select **Jobs > Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

Deleting a UNI Interface and Deleting an Endpoint

To delete a UNI from a multipoint-to-multipoint Ethernet service:

1. In the Network Services > Connectivity view pane, select **Service Provisioning > Manage Services**.
2. In the **Manage Services** page, select the service from which you want to delete a UNI.
3. Click **Modify** at the top of the table of listed service orders.

Current service settings appear in the main display area. The **Service Parameters** page contains a unique name for the service order that will request the change.
4. In the service **Order name** field, change the name of the modification service order, if desired.
5. Click the **Site/Endpoint Settings** button to view the interfaces on endpoints or devices that are associated with the service.
6. In the **User-to-Network Interfaces** table, select the interfaces that you want to remove from being assigned to the service order, and click **Delete** at the top of the table.

The selected UNI is removed from the table. If the deleted UNI was the only UNI selected on that device, then the device is deleted from the Endpoint Settings table.
7. Click **Finish** to save the modified service order.
8. In Deploy mode of the Service View of the Connectivity Services Director, select one of the following from the Manage Services page:
 - Schedule the change for immediate deployment.
 - Schedule the change for later deployment.
9. Use the **System > Manage Jobs > Job Management** workspace to monitor the progress and status of the deployment.



NOTE: Alternatively, to display the Job Management page, from the Jobs workspace of the Junos Space Platform UI, select **Manage Jobs** from the **Tasks** pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

Changing the Endpoint Bandwidth

To change the rate limit or bandwidth for an endpoint of a multipoint-to-multipoint Ethernet service:

1. In the Network Services > Connectivity view pane, select **Service Provisioning > Manage Services**.
2. In the **Manage Services** page, select the service on which you want to change the bandwidth of an endpoint.
3. Click **Modify** at the top of the table of listed service orders.
Current service settings appear in the main display area. The **Service Parameters** page of the wizard contains a unique name for the service order that will request the change.
4. In the service **Order name** field, change the name of the modification service order, if desired.
5. Click the **Site/Endpoint Settings** button to navigate to the corresponding page of the wizard. Click on the **Bandwidth** entry for the UNI on which you want to change the bandwidth.
6. From the list of valid bandwidth settings, select the setting you want, then click **Finish**.
7. In Deploy mode of the Service View of Connectivity Services Director, select one of the following:
 - Schedule the change for immediate deployment.
 - Schedule the change for later deployment.
8. Click **OK**.
9. Use the **System > Manage Jobs > Job Management** workspace to monitor the progress and status of the deployment.



NOTE: Alternatively, to display the Job Management page, from the Junos Space Platform UI, select **Jobs > Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

Changing Advanced Settings for an Endpoint

To change advanced settings for an endpoint of a multipoint-to-multipoint Ethernet service:

1. In the Network Services > Connectivity view pane, select **Service Provisioning > Manage Services**.
2. In the **Manage Services** page, select the service on which you want to change one or more advanced settings for an endpoint.

3. Click **Modify** at the top of the table of listed service orders.

Current service settings appear in the main display area. The **General Settings** box contains a unique name for the service order that will request the change.

4. In the service **Order name** field, change the name of the modified service order, if desired.

5. In the **Endpoint Settings** page of the wizard, find the device endpoint you want to modify, and click **Advanced** for that table row.

The **Advanced Setting** window displays the security and advanced settings that you can configure for a device.

See the *Service Attributes Overview* for more information about configuring MAC security settings and advanced settings.

6. In the **MAC Security Settings** box, make selections for MAC learning and MAC statistics and enter values for Interface MAC limit, MAC table size, and MAC table aging time.
7. Enable or disable tunnel services by selecting or clearing the **disable-tunnel-service** check box.
8. Enable or disable local switching by selecting or clearing the **disable-local-switching** check box.
9. In the **Fast reroute priority** field, specify the reroute priority for a VPLS routing instance.
10. In the **Label block size** field, specify the label block size for VPLS labels.
11. In the **Connectivity type** field, select a connection-type to specify when a VPLS connection is taken down, depending on whether or not the interface for the VPLS routing instance is customer-facing or integrated routing and bridging (IRB)
12. Click **OK** to save all your changes in the Advanced Setting window.

13. Click **Finish**.
14. In Deploy mode of the Service View, select one of the following:
 - Schedule the change for immediate deployment.
 - Schedule the change for later deployment.
15. Click **OK**.
16. Use the **System > Manage Jobs > Job Management** workspace to monitor the progress and status of the deployment.



NOTE: Alternatively, to display the Job Management page, from the Junos Space Platform UI, select **Jobs > Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

Related Documentation

- [Creating a Full Mesh Layer 3 VPN Ethernet Service Order on page 941](#)
- [Creating a Hub-and-Spoke Layer 3 VPN Service Order on page 964](#)

Modifying a Point-to-Multipoint Ethernet Service

For a point-to-multipoint service, you can add a spoke or a hub, change the role of a device from hub to spoke or spoke to hub, change the bandwidth or MTU of a specific UNI, or add or delete a UNI.

You cannot change the interface of an existing UNI or the service VLAN ID.

To perform the equivalent of changing the interface on an existing UNI, add a new UNI with the desired interface, and then delete the old UNI.

After modifying a service, the configuration audit and functional audit information is cleared and the functional audit status is set to pending.

Modifying a service creates a new service order based on the attribute settings of the existing service.

The following topics provide instructions for modifying a multipoint Ethernet (VPLS) service:



NOTE: When you modify a service or a service order, the read-only fields in the different pages of the wizard for service or service order modification are grayed out to indicate that you cannot modify those attributes.

- [Adding a Spoke on page 1034](#)
- [Adding a Hub on page 1035](#)
- [Changing a Spoke to a Hub on page 1036](#)
- [Changing a Hub to a Spoke on page 1037](#)
- [Adding a UNI Interface on page 1038](#)
- [Deleting a UNI Interface or Deleting an Endpoint on page 1039](#)
- [Changing the Endpoint Bandwidth on page 1040](#)
- [Changing Advanced Settings for an Endpoint on page 1041](#)

Adding a Spoke

To add an endpoint configured as a spoke to a multipoint Ethernet service:

1. In the Network Services > Connectivity view pane, select **Service Provisioning > Manage Services**.
2. In the **Manage Services** page, select the point-to-multipoint service to which you want to add a spoke.
3. Click the **Modify** icon at the top of the table of previously created service orders.
Current service settings appear in the main display area. The **General Settings** box contains a unique name for the service order that will request the change.
4. In the service **Order name** field, change the name of the modification service order, if desired.
5. If you have configured the CFM, the **General Settings** panel provides an option to disable the CFM service. You can select the **Disable CFM** check box to disable the CFM service, if desired.

If you have not configured the CFM, the **General Settings** panel provides an option to enable the CFM service. You can select the CFM definition from the **OAM Profile** list, if desired.
6. Click the **Node Settings** button to view the endpoints or devices that are associated with the service.
7. In the **Service Nodes** table, click **Add**.

The **Choose Endpoints** dialog box shows available N-PE devices that are not part of the service.

The dialog box is divided into two halves. The top half of the dialog box displays the devices that you can associate with the service. Based on the devices you select in the top half of the dialog box, the interfaces that are present in the selected device are displayed in the lower half of the dialog box. Select the check boxes next to the interfaces that you want to associate with the service.

8. In the **Endpoint Settings** table, check **Spoke** for the device you just added.
9. Click **Finish** to complete the modification of the service order and save the settings.
10. In Deploy mode of the Service View of Connectivity Services Director, select one of the following from the Manage Services page:
 - Schedule the change for immediate deployment.
 - Schedule the change for later deployment.

Adding a Hub

To add an endpoint to a multipoint Ethernet service:

1. In the Network Services > Connectivity view pane, select **Service Provisioning > Manage Services**.
2. In the **Manage Services** page, select the service to which you want to add a hub.
3. Click the **Modify** icon at the top of the table of previously created service orders.

Current service settings appear in the main display area. The **General Information** box contains a unique name for the service order that will request the change.
4. In the service **Order name** field, change the name of the modification service order, if desired.
5. Click the **Node Settings** button to view the endpoints or devices that are associated with the service.
6. In the **Service Nodes** table, click **Add**.

The **Choose Endpoints** window shows available N-PE devices that are not part of the service.

The dialog box is divided into two halves. The top half of the dialog box displays the devices that you can associate with the service. Based on the devices you select in the top half of the dialog box, the interfaces that are present in the selected device

are displayed in the lower half of the dialog box. Select the check boxes next to the interfaces that you want to associate with the service.

7. In the **Endpoint Settings** table, check **Spoke** for the device you just added.
8. Use the **System > Manage Jobs > Job Management** workspace to monitor the progress and status of the deployment.



NOTE: Alternatively, to display the Job Management page, from the Junos Space Platform UI, select **Jobs > Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

Changing a Spoke to a Hub

To change a spoke to a hub in a point-to-multipoint Ethernet service:

1. In the Network Services > Connectivity view pane, select **Service Provisioning > Manage Services**.
2. In the **Manage Services** page, select the point-to-multipoint service for which you want to change a spoke to a hub.
3. Click the **Modify** icon at the top of the table of previously created service orders.
Current service settings appear in the main display area. The **General Settings** box contains a unique name for the service order that will request the change.
4. In the service **Order name** field, change the name of the modification service order, if desired.
5. In the **Device** column of the **Endpoint Settings** table, find the spoke endpoint you want to change to a hub and select the **Hub** check box.
6. Click **Finish** to save the modified service order properties.
7. In Deploy mode of the Service View of Connectivity Services Director, select one of the following:
 - Schedule the change for immediate deployment.
 - Schedule the change for later deployment.
8. Use the **System > Manage Jobs > Job Management** workspace to monitor the progress and status of the deployment.



NOTE: Alternatively, to display the Job Management page, from the Junos Space Platform UI, select **Jobs > Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

Changing a Hub to a Spoke



NOTE: You cannot change the only hub of a point-to-multipoint service to a spoke. You will receive an error message when you try to save such a service configuration.

To change a hub to a spoke in a point-to-multipoint Ethernet service:

1. In the Network Services > Connectivity view pane, select **Service Provisioning > Manage Services**.
2. In the **Manage Services** page, select the point-to-multipoint service for which you want to change a hub to a spoke.
3. Click the **Modify** icon at the top of the table of previously created service orders.
Current service settings appear in the main display area. The **General Settings** box contains a unique name for the service order that will request the change.
4. In the service **Order name** field, change the name of the modification service order, if desired.
5. In the **Device** column of the **Endpoint Settings** table, find the spoke endpoint you want to change to a hub and clear the **Hub** check box.
6. Click **Finish** to save the modified service order properties.
7. In Deploy mode of the Service View of Connectivity Services Director, select one of the following:
 - Schedule the change for immediate deployment.
 - Schedule the change for later deployment.
8. Use the **System > Manage Jobs > Job Management** workspace to monitor the progress and status of the deployment.



NOTE: Alternatively, to display the Job Management page, from the Junos Space Platform UI, select **Jobs > Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

Adding a UNI Interface

To add a UNI on a device that is already part of a multipoint Ethernet service:

1. In the Network Services > Connectivity view pane, select **Service Provisioning > Manage Services**.
2. In the **Manage Services** page, select the service to which you want to add a UNI.
3. Click the **Modify Service** icon at the top of the page of previously defined service orders.
Current service settings appear in the main display area. The **General Settings** box contains a unique name for the service order that will request the change.
4. In the service **Order name** field, change the name of the modification service order, if desired.
5. Click the **Site/Endpoint Settings** button to view the interfaces on endpoints or devices that are associated with the service.
6. In the **User-to-Network Interfaces** table, click **Add**.

The **Choose Endpoints** window shows available N-PE devices that are not part of the service.

7. Select the devices on which you want to add new interfaces. The window refreshes to display all the user-to-network (UNI) or ingress interfaces for the selected device in the lower part of the window as a tabular grid. Select the interfaces that you want to assign to the service order, and then click **OK**.

To filter and sort the display of objects, enter the name of the object as a match criterion in the Search box and click the Search icon. The page refreshes to display only the object names that match with the search term. You can use the paging controls to navigate across multiple pages of objects as necessary.

You are returned to the Node Settings page of the Manage Service Orders wizard.

The service modification window shows the added devices with system recommended choices for UNI.

8. If the interface you selected in the previous step is already configured (duplicate) you must either enter a different value in the service **VLAN ID** field manually, or check the **Autopick VLAN ID** field.
9. Click **Modify**.
10. In the **Deployment Options** window, select one of the following:
 - Save the change without scheduling it.
 - Schedule the change for immediate deployment.
 - Schedule the change for later deployment.
11. Click **OK**.
12. Use the **System > Manage Jobs > Job Management** workspace to monitor the progress and status of the deployment.



NOTE: Alternatively, to display the Job Management page, from the Junos Space Platform UI, select **Jobs > Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

Deleting a UNI Interface or Deleting an Endpoint



NOTE: You cannot delete the last endpoint on the only hub device in the service. You will receive an error message when you try to save such a service configuration.

To delete a UNI from a multipoint Ethernet service:

1. In the **Network Services > Connectivity** view pane, select **Service Provisioning > Manage Services**.
2. In the **Manage Services** page, select the service from which you want to delete a UNI.
3. Click the **Delete** icon at the top of the page.
Current service settings appear in the main display area. The **General Settings** box contains a unique name for the service order that will request the change.
4. In the service **Order name** field, change the name of the modification service order, if desired.

5. Click the **Site/Endpoint Settings** button to view the interfaces on endpoints or devices that are associated with the service.
6. In the **User-to-Network Interfaces** table, select the interfaces that you want to remove from being assigned to the service order, and click **Delete** at the top of the table.

The selected UNI is removed from the table. If the deleted UNI was the only UNI selected on that device, then the device is deleted from the Endpoint Settings table.
7. Click **Finish** to save the modified service order.
8. In Deploy mode of the Service View of Connectivity Services Director, select one of the following from the Manage Services page:
 - Schedule the change for immediate deployment.
 - Schedule the change for later deployment.
9. Use the **System > Manage Jobs > Job Management** workspace to monitor the progress and status of the deployment.



NOTE: Alternatively, to display the Job Management page, from the Junos Space Platform UI, select **Jobs > Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

Changing the Endpoint Bandwidth

To change the rate limit or bandwidth for an endpoint of a multipoint Ethernet service:

1. In the Network Services > Connectivity view pane, select **Service Provisioning > Manage Services**.
2. In the **Manage Services** page, select the service on which you want to change the bandwidth of an endpoint.
3. Open the **Actions** menu and select **Modify Service**.

Current service settings appear in the main display area. The **General Settings** box contains a unique name for the service order that will request the change.
4. In the service **Order name** field, change the name of the modification service order, if desired.
5. Click the **Site/Endpoint Settings** button to navigate to the corresponding page of the wizard. Click on the **Bandwidth** entry for the UNI on which you want to change the bandwidth.

6. From the list of valid bandwidth settings, select the setting you want, then click **Modify**.
7. In Deploy mode of the Service View of Connectivity Services Director, select one of the following:
 - Schedule the change for immediate deployment.
 - Schedule the change for later deployment.

Changing Advanced Settings for an Endpoint

To change advanced settings for an endpoint of a point-to-multipoint Ethernet service:

1. In the Network Services > Connectivity view pane, select **Service Provisioning > Manage Services**.
2. In the **Manage Services** page, select the service on which you want to change one or more advanced settings for an endpoint.
3. Click the **Modify** icon at the top of the page.

Current service settings appear in the main display area. The **General Settings** box contains a unique name for the service order that will request the change.
4. In the service **Order name** field, change the name of the modified service order, if desired.
5. In the **Action** column of the **Endpoint Settings** table, find the device endpoint you want to modify, and click **Advanced** for that table row.

The **Advanced Setting** window displays the security and advanced settings that you can configure for a device.
6. In the **MAC Settings** box, make selections for MAC learning and MAC statistics and enter values for Interface MAC limit, MAC table size, and MAC table aging time.
7. Enable or disable tunnel services by selecting or clearing the **disable-tunnel-service** check box.
8. Enable or disable local switching by selecting or clearing the **disable-local-switching** check box.
9. In the **Fast reroute priority** field, specify the reroute priority for a VPLS routing instance.
10. In the **Label block size** field, specify the label block size for VPLS labels.

11. In the **Connectivity type** field, select a connection-type to specify when a VPLS connection is taken down, depending on whether the interface for the VPLS routing instance is customer-facing or integrated routing and bridging (IRB)
12. Click **OK** to save all your changes in the **Advanced Setting** window.
13. In Deploy mode of the Service View in the Connectivity Services Director GUI, select one of the following:
 - Schedule the change for immediate deployment.
 - Schedule the change for later deployment.
14. Click **OK**.
15. Use the **System > Manage Jobs > Job Management** workspace to monitor the progress and status of the deployment.



NOTE: Alternatively, to display the Job Management page, from the Junos Space Platform UI, select **Jobs > Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

Related Documentation

- [Creating a Multipoint-to-Multipoint VPLS Service Order on page 881](#)
- [Creating a Point-to-Multipoint VPLS Service Order on page 905](#)
- [Creating a Point-to-Point Service Order on page 829](#)

Modifying a Hub-and-Spoke Layer 3 VPN Service Order

You can modify and deploy previously configured Layer 3 VPN hub-and-spoke service orders. Modifying a service order involves the following tasks:



NOTE: When you modify a service or a service order, the read-only fields in the different pages of the wizard for service or service order modification are grayed out to indicate that you cannot modify those attributes.

1. [Viewing the Service Definition on page 1043](#)
2. [Configuring Service Parameters Information on page 1044](#)
3. [Selecting N-PE Devices or Nodes on page 1049](#)
4. [Setting Attributes for Endpoints or Nodes on page 1050](#)
5. [Adding and Deleting UNI Interfaces on page 1053](#)

- 6. [Setting Attributes for UNIs or Sites on page 1054](#)
- 7. [Deploying the New Service on page 1057](#)

Viewing the Service Definition

To view the service definition on which the service order is based:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon on the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
5. Select L3VPN Services to manage Layer 3 VPN Ethernet service orders.

6. You can modify a service order or a deployed service in either of the following ways:

From the Manage Network Services page, do the following:

- a. Select the check box beside the service that you want to modify.
- b. Click **Edit** at the top of the table of the listed services.

The Edit Service Order wizard is displayed. You can navigate to the various pages of the wizard by clicking the buttons at the top of the page or the navigation buttons at the bottom of the page.

From the Manage Service Deployment page, do the following:

- a. From the Manage Service Deployment page, select the check box beside the service you want to modify.
- b. Click **Edit** at the top of the table of the listed services.

The Review page or step of the Edit Service Order wizard is displayed. You can click **Edit** beside the sections in the page for which you want to update the configuration parameters. The settings that you can configure in the service order are organized in separate pages of the wizard, which you can launch by clicking the appropriate buttons at the top of the Edit Service Order page. Alternatively, you can proceed to the corresponding setting-related pages by clicking the Back and Next buttons at any point in the wizard.

7. From the Service Definition field, click **View** to open a popup dialog box that displays the details of the selected service definition. The service definition properties, such as the name, signaling type (LDP or BGP), service type (point-to-point psuedowire,

ATM, or TDM), are displayed. The interface-specific attributes, such as rate-limiting details, encapsulation, and VLAN tags, are also displayed in the dialog box. Close the dialog box to return to the service order modification wizard.

Based on the fields or parameters that you defined in the service definition to be enabled for modification in the service order, the corresponding fields are available for editing. The fields that are disabled for modification in the service order can only be edited in the service definition.

Configuring Service Parameters Information

In this topic you configure general settings, VPN settings that can be applied to all end points, and routing protocol settings for the provider edge (PE) and customer edge (CE) devices.

- [Specifying General Settings on page 1044](#)
- [Specifying PE-CE Settings Information on page 1048](#)

Specifying General Settings

You configure general information about the service order in the General Settings box of the Enter Order Information window.

If a service template is attached to the service definition, there is a link to that template at the bottom of the Endpoint Settings section of the window. For instructions on working with service templates in service orders, see [“Creating a Service Order Based on a Service Definition with a Template” on page 990](#).

You must add the customer to the database before proceeding. See [“Adding a New Customer” on page 737](#).

To enter general settings information:

1. In the **Name** field, type a unique name for the full mesh service.

The service order name can consist of only letters, numbers, and underscores.



NOTE: The name you specify for a Layer 3 VPN service order becomes the routing-instance name in the device configuration when you deploy the service. Consequently, you cannot use any Juniper Networks keywords, for example, “bgp” or “ospf”, as the name of a service order.

2. In the **Customer** field, select the customer who is requesting the service.
3. In the **Comments** field, type a description of the service.

This description appears in information windows about the request or service instance created from the request.

To enter connectivity settings information:

1. Specify whether the **Autopick Route Target** can be selected automatically or manually.

- To assign the **Route Target** automatically, select the **Auto Pick Route target** check box.
- To assign the **Route Target**, clear the **Auto Pick Route Target** check box.

The window expands to include the **Route Target** field. In the **Route Target** field, type a value.



NOTE: For Hub-and-Spoke service order, clear the **Auto Pick Hub Route Target** and **Autopick Spoke Route Target** check boxes to activate the **Hub Route Target** and **Spoke Route Target** fields, respectively.

When you manually type a route target, Junos Space accepts either of the following two formats:

- *prefix-number:assigned-number*

Where *prefix-number* can be any numeric value from 1 through 65,535. The *assigned-number* can be any numeric value from 0 through 2,147,483,647.

- *IPV4-address:assigned-number*

Where *IPV4-address* can be any valid IPv4 address, and *assigned-number* can be any numeric value from 0 through 65,535.



NOTE: You cannot edit this field if you have not selected the **Editable in Service Order** check box in the service definition.

2. Specify whether the **Auto Pick Route Distinguisher** can be selected automatically or manually.

- To assign the **Route Distinguisher** automatically, select the **Auto Pick Route Distinguisher** check box.
- To assign the **Route Distinguisher** manually, clear the **Auto Pick Route Distinguisher** check box.

The window expands to include the **Route Distinguisher** field. In the **Route Distinguisher** field, type a value.

When you manually type route distinguishers, Junos Space accepts either of the following two formats:

- *prefix-number: assigned-number*

Where *prefix-number* can be any numeric value from 1 through 65,535. The *assigned-number* can be any numeric value from 0 through 2,147,483,647.

- *IPV4-address: assigned-number*

Where *IPV4-address* can be any valid IPv4 address, and *assigned-number* can be any numeric value from 0 through 65,535.



NOTE: You cannot edit this field if you have not selected the **Editable in Service Order** check box in the service definition.

3. Select the **Autopick Hub Route Target** and **Autopick Spoke Route Target** check boxes if you want the Route target chosen automatically by the Connectivity Services Director application.



NOTE: You cannot edit this field if you have not selected the **Editable in Service Order** check box in the service definition.

To manually assign a Route target:

1. Clear the **Autopick Hub Route Target** and **Autopick Spoke Route Target** check boxes to activate the **Hub Route Target** and **Spoke Route Target** fields respectively.
2. In the **Route Target** field, enter a value.

When you manually enter route target, Junos Space accepts either of the following two formats:

- *<prefix-number>: <assigned-number>*

Where *<prefix-number>* can be any numeric value from 1 to 65535, inclusive.
The *<assigned-number>* can be any numeric value from 0 to 2,147,483,647, inclusive.

- *<IPV4-address>: <assigned-number>*

Where *<IPV4-address>* can be any valid IPv4 address (in W.X.Y.Z "dot" notation), and *<assigned-number>* can be any numeric value from 0 to 65535, inclusive.

- 4.
5. Select the **Autopick Hub Route Distinguisher** and the **Autopick Spoke Route Distinguisher** check boxes if you want the Route distinguisher chosen automatically by the Connectivity Services Director application.

To manually assign a Route distinguisher:

1. Clear the **Autopick Hub Route Distinguisher** and the **Autopick Spoke Route Distinguisher** check boxes to activate the **Hub Route distinguisher** and **Spoke Route distinguisher** fields respectively.
2. In the **Route distinguisher** field, enter a value.

When you manually enter route distinguishers, Junos Space accepts either of the following two formats:

- *<prefix-number>: <assigned-number>*

Where *<prefix-number>* can be any numeric value from 1 to 65535, inclusive.
 The *<assigned-number>* can be any numeric value from 0 to 2,147,483,647, inclusive.

- *<IPV4-address>*: *<assigned-number>*

Where *<IPV4-address>* can be any valid IPV4 address (in W.X.Y.Z "dot" notation), and *<assigned-number>* can be any numeric value from 0 to 65535, inclusive.

To enter VPN settings details:

1. To configure a separate label for each VRF to provide double lookup and egress filtering, select the **VRF Table label** check box.



NOTE: You cannot edit this field if you have not selected the **Editable in Service Order** check box in the service definition.

The **Export Direct Routes** check box is not editable in the service order.

2. Select the **Enable MVPN** check box to enable multicast virtual private network (MVPN).

To enter default UNI settings information:

1. Select a value for **Ethernet Option**:

- **Port**
- **Dot1Q**

Specifying the **Dot1Q** Ethernet option enables you to apply a Unit ID, a single VLAN ID, a VLAN Range, or a VLAN list to the service order.

- **QinQ**

Specifying the **QinQ** Ethernet option enables you to apply a single VLAN, a VLAN Range, or a VLAN list to the service order. For an L3VPN service deployed on a dual tagged interface, the inner tag determines the VPN routing and forwarding instance(VRF).

2. Select or clear the **Autopick Interface IP** check box.

- To specify the **Interface IP address**, clear the **Autopick interface IP** check box.
- To specify the **IP Address Pool** and **IP Block Size** field values in the Site Settings page of the service order creation wizard, select the **Autopick interface IP** check box.

If you have selected the **Enable MC- LAG** check box in the Service Settings section, the maximum and minimum values for **IP block size** are 29 and 28, respectively.



NOTE: You cannot edit the **Autopick Interface IP** check box if you have not selected the **Editable in Service Order** check box in the service definition.



NOTE: The fields specified in the Default UNI Settings section are based on the Ethernet Option type. The Logical IF Settings box is not available if you have selected the Ethernet Option as *Port*.

3. Specify whether the **Autopick Interface Unit** can be selected automatically or manually.

- To assign the **Unit ID** automatically, select the **Autopick Interface Unit** check box.
- To assign the **Unit ID** manually, clear the **Autopick Interface Unit** check box.

The window expands to include the **Unit ID** field. In the **Unit ID** field, type a value.

Range: 1 through 1073741823



NOTE: You can edit this field only if you have selected the **Editable in Service Order** check box for the VLAN ID selection in the service definition.

4. Specify whether the **Autopick VLAN ID** can be selected automatically or manually.

- To assign the **VLAN ID** automatically, select the **Autopick VLAN ID** check box.
- To assign the **VLAN ID** manually, clear the **Autopick VLAN ID** check box.

The window expands to include the **VLAN ID** field. In the **VLAN ID** field, type a value.



NOTE: You cannot edit this field if you have not selected the **Editable in Service Order** check box in the service definition.

Specifying PE-CE Settings Information

You configure VPN attributes that are usually common for all the endpoints in the service. The values that you provide vary, depending on the service definition on which the service order is based.

If you do not expect these attributes to be the same on all endpoints, you can set them to be the same for now and then make changes later, or you can skip this step and apply the attribute values one at a time later.

In the **PE-CE Settings** section of the Service Parameters page, depending on the PE-CE routing protocol—OSPF/Static Route or BGP/Static Route—do one of the following:

- If **BGP/Static Route routing protocol** is specified in the service definition:
 - a. The **AS override** option is selected to allow a service provisioner to override the AS number. Clear the **AS override** check box to prevent a service provisioner from overriding the AS number.
 - b. Enter a value for the maximum number of prefixes accepted by a PE router from a CE router.
- If **OSPF/Static Route routing protocol** is specified in the service definition, in the **OSPF domain ID** field, enter a IP address.

You can enter from 1.0.0.1 to 223.255.255.254, excluding 127.x.x.x.

1. Click **Next**.

The **Node Parameters** page appears.

Selecting N-PE Devices or Nodes

In this topic you select the N-PE devices that you want to host the service endpoints. The selection is made from the **Select Endpoint PE Devices** window.



NOTE: The **Choose Endpoints** window, which you can view by clicking the **Add** icon on the **Node Parameters** page, shows only assigned N-PE devices that have an AS number configured. If you do not see the device you are looking for, use the CLI on the device to check for and assign an AS number.

N-PE devices that have L2VPN only do not appear.

To select endpoint N-PE devices:

1. In the **Node Parameters** page, click **Add** in the Service Nodes table. From the **Choose Endpoints** dialog box that appears, select the devices that you want to participate in the service. Use the multiple selection feature to select one or more devices.



NOTE: In the **Choose Endpoints** dialog box, you can sort and segregate the devices and their corresponding interfaces based on the roles of the devices to easily and quickly view only the devices of interest. Click the down arrow on the **Filter Role** menu, and select **P2E** to view only the provider edge devices, **P** to view only the provider devices, and **L2E** to view only Layer 2 Ethernet devices.

2. Click **OK**.

The **Node Parameters** window appears.

3. Continue with modifying or entering the node parameters.

Setting Attributes for Endpoints or Nodes

If a service template is attached to the service definition, there is a link to that template at the bottom of the Endpoint Settings section of the window. For instructions on working with service templates in service orders, see [“Creating a Service Order Based on a Service Definition with a Template” on page 990](#).

You set attributes for each endpoint in the service from the Endpoint Settings window.

The interface shown in the UNI Interface field is automatically selected by the Connectivity Services Director application, which chooses the UNI that has the highest available capacity among interfaces that are in the Up state. To calculate the available capacity of the interface, the system subtracts the bandwidth reserved for each service deployed on that interface from the total capacity of the interface.

For each endpoint, the Endpoint Settings window shows the value for each UNI attribute.

As a service provider, you can create static routes on the service. To specify static routes for a CE device on the Node Parameters page:

1. Click the **Add** icon above the Static Routes table. A new row is added to the table and highlighted in yellow to denote that you can enter the destination prefix and next-hop address.
2. In the Destination Prefix field, enter the endpoint for the static route.
3. In the Next-Hop field, enter the IP address of the next-hop. You can enter a dotted decimal notation, between 1.0.0.1 and 223.255.255.254 except 127.x.x.x.
4. Insert as many static routes as you require. To delete an existing route, select the check box beside the route, and click **Delete** above the listed routes.

The MVPN and PIM Settings sections are displayed only if you selected the **Enable MVPN** check box in the Service Parameters page of the creation of service order wizard. To specify PIM settings for the service order:

1. From the **PIM Mode** list, specify the mode of PIM. Only PIM sparse mode is currently supported.



NOTE: A Protocol Independent Multicast (PIM) sparse-mode domain uses reverse-path forwarding (RPF) to create a path from a data source to the receiver requesting the data. When a receiver issues an explicit join request, an RPF check is triggered. A (*G) PIM join message is sent toward the RP from the receiver's designated router (DR). (By definition, this message is actually called a join/prune message, but for clarity in this description, it is called either join or prune, depending on its context.) The join message is multicast hop by hop upstream to the ALL-PIM-ROUTERS group (224.0.0.13) by means of each router's RPF interface until it reaches the RP. The RP router receives the (*G) PIM join message and adds the interface on which it was received to the outgoing interface list (OIL) of the rendezvous-point tree (RPT) forwarding state entry. This builds the RPT connecting the receiver with the RP. The RPT remains in effect, even if no active sources generate traffic.

2. From the **Interface** list, select the interface to be used for PIM. When you modify a UNI from the list of interfaces on the Site Settings page, the GUI does not automatically delete the UNI from the Endpoint list. However, the newly added UNIs are added to the **Interface** list for the selected device or node.

To specify rendezvous point (RP) settings:

1. Click the **Add** icon above the table of RP addresses. The Add Rendezvous Point Address dialog box is displayed.
2. In the Rendezvous Point (device) field, configure the routing device as an actual or potential rendezvous point (RP). A routing device can be an RP for more than one group.
3. In the Interface field, specify the name of the interface on which PIM must be enabled. Specify the full interface name, including the physical and logical address components. UNIs for the selected device include lo0 if the selected device is enabled with loopback.
4. In the Group Address field, configure the address ranges of the multicast groups for which this routing device can be a rendezvous point (RP). By default, the routing device is eligible to be the RP for all IPv4 or IPv6 groups (224.0.0.0/4 or FF70::/12 to FFF0::/12).
5. Click **OK** to add the RP addresses to the table on the Node Parameters page.
6. To modify an added RP address, select the check box beside the row and click **Edit**. The dialog box is displayed to enable you modify the settings.
7. To delete an added RP address, select the check box beside the row and click **Delete**. The selected RP address is removed from the table.

To define MVPN settings for the service order:

1. From the **MVPN mode** list, indicate whether the shared-tree data distribution mode (**RPT-SPT**) or the shortest path tree only (**SPT-only**) mode of MVPN must be enabled to learn about active multicast sources using multicast VPN source-active routes. the default mode of operation is shortest path tree only (SPT-only) mode. In SPT-only mode, the active multicast sources are learned through multicast VPN source-active routes. This mode of operation is described in section 14 of the BGP-MVPN draft (draft-ietf-l3vpn-2547bis-mcast-bgp-00.txt). If the default mode is not suitable for your environment, you can configure RPT-SPT mode (also known as shared-tree data distribution), as documented in section 13 of the BGP-MVPN draft (draft-ietf-l3vpn-2547bis-mcast-bgp-00.txt). RPT-SPT mode supports the native PIM model of transmitting (*G) messages from the receiver to the RP for intersite shared-tree join messages. This means that the type 6 (*G) routes get transmitted from one PE router to another. In RPT-SPT mode, the shared-tree multicast routes are advertised from an egress PE router to the upstream router connected to the VPN site with the C-RP
2. In the Provider Tunnel Name field, specify the provider tunnel name to configure virtual private LAN service (VPLS) flooding of unknown unicast, broadcast, and multicast traffic using point-to-multipoint LSPs. Also configure point-to-multipoint LSPs for MBGP MVPNs.
3. From the **Site Type** list, specify the site type of the MBGP MVPN. An MBGP MVPN defines two types of site sets, a sender site set and a receiver.
4. Select the **Upstream Multicast Hop** check box to configure the upstream multicast hop (UMH) to denote a router to use the unicast route preference to determine the single forwarder election.
5. In the **Import Unicast Target** field, specify the import targets specifically for sender sites or receiver sites, or can be borrowed from a configured unicast route target. Note that a sender site export route target is always advertised when security association routes are exported. By default, the VPN routing and forwarding (VRF) import and export route targets (configured either using VRF import and export policies or using the **vrf-target** statement) are used for importing and exporting routes with the MBGP MVPN network layer reachability information (NLRI). You can use the **export-target** and **import-target** options to override the default VRF import and export route targets. Select the **Sender** radio button to import unicast targets for sender sites, select the **Receiver** radio button to import unicast targets for receiver sites, or select **None** to disable the import of unicast targets.
6. In the **Import Target** field, specify the import targets for sender and receiver sites. Select the **Sender** radio button to import targets for sender sites, select the **Receiver** radio button to import targets for receiver sites.

7. Select the **Export Unicast Target** check box to specify the export target to enable you to override the Layer 3 VPN export route targets used for importing and exporting routes for the MBGP MVPN network layer reachability information (NLRI).
8. In the Target Community field, specify the target community value to be used when exporting sender and receiver site routes. You can specify this value manually if you deselect the **Autopick Export Target** check box.
9. Select the **Autopick Export Target** check box to specify that you want to enable automatic selection of an export target if a configuration is not provided. An imported automatic discovery route is treated as belonging to both the sender site set and the receiver site set.

If you select the **Is Stitching** check box, all the parameters of that endpoint are disabled.

To configure or change the topology settings on the Node Parameters page:

1. The type of network circuit is displayed in the Topology field as full-mesh or hub-and-spoke.
2. Make sure the **Is Stitching Point** check box is not selected.
3. To add the loopback interface for a Layer 3 VPN service, select the **Add Loopback** check box.



NOTE: If you provision a loopback interface for an L3VPN service, an operator is able to identify a VRF routing instance. Thereafter, an operator can manually ping a remote CE router from a local PE router.

4. Select the **Is Hub** check box to enable the node to function as a hub. Deselect the check box if you want the device to function as a spoke. This field is not applicable for full-mesh Layer 3 VPN services.
5. When you have finished configuring the endpoint settings, click **Next**.

The Site Settings page of the Create L3VPN Service Order wizard appears.

Adding and Deleting UNI Interfaces

You can add or delete UNI interfaces on the PE devices that participate in a service:

To add a UNI interface on a selected device:

1. Select the **Add** icon in above the table of listed UNI interfaces, and from the **Choose Endpoints** window, select the device from which you want to retrieve the UNI interface to associate with the service order. The window refreshes to display all the UNI interfaces configured on the selected device.
2. Select the check boxes beside the UNIs that you want to associate.
3. Click **Add** to close the window. You are returned to the Site Settings page, and the selected UNIs are displayed in the table.
4. If the interface you selected in the previous step is already configured (duplicate) either type a different value in the VLAN ID field manually, or check the **Autopick VLAN ID** field.

To delete a UNI interface from a selected device:

- Select the check box adjacent to the interface you want to delete, and click the **Delete** icon above the list of displayed interfaces.

If the deleted UNI is the only UNI selected from the device, then the device is deleted from the service configuration.

You can set or modify attributes for a UNI endpoint.

To modify a UNI interface for a selected device:

1. Select the row for the UNI endpoint that you want to modify.
The **UNI Settings** dialog box appears.
2. Modify the **UNI Settings** fields.
3. Either apply the attributes you already specified or add values that you did not configure for different attributes of a UNI.
4. When you have finished modifying the endpoint settings, click **OK**.

The **Site Settings** page appears.

Setting Attributes for UNIs or Sites

If there is a service template attached to the service definition, there is a link to that template at the bottom of the Site Settings section of the screen. For instructions on working with service templates in service orders, see [“Creating a Service Order Based on a Service Definition with a Template” on page 990](#).

This part of the create Ethernet service order procedure sets the attributes for each UNI or interface in the service. Selection is made using the Site Settings screen.

The interface shown in the UNI Interface field is automatically selected by the Connectivity Services Director application, which chooses the UNI that has the highest available capacity among interfaces that are in the Up state. To calculate the available capacity of the interface, the system subtracts the bandwidth reserved for each service deployed on that interface from the total capacity of the interface.

For each endpoint, the Site Settings page shows the value for each UNI attribute.

To configure or change the site or UNI settings:

1. Select a value for **Encapsulation**.

- **Port**
- **Dot1Q**

Specifying the **Dot1Q** Ethernet option enables you to apply a Unit ID, a single VLAN ID, a VLAN Range, or a VLAN list to the service order.

- **QinQ**

Specifying the **QinQ** Ethernet option enables you to apply a single VLAN, a VLAN Range, or a VLAN list to the service order. For an L3VPN service deployed on a dual tagged interface, the inner tag determines the VPN routing and forwarding instance(VRF).

- **Flexible UNI**

Specifying the **Flexible UNI** Ethernet option enables you to apply different values for the Unit ID and vlan-tags.



NOTE: Prior to release 13.1P6.1, Network Activate set the unit and vlan-id parameters to the same value.

To create a service order that specifies the Flexible UNI Ethernet option, you must complete two preliminary tasks. First you must create a service template in which you specify both outer and inner vlan tags. Then you must create a service definition that associates the service template with the service definition.

2. To select a different UNI on a device, click the **UNI interface** and choose another interface from the list.
3. In the **UNI Description**, you can enter the description for the selected **UNI interface**. The **Description** field is displayed in Modify Service Order, View Service Order Details, Modify Service, and View Service windows. You can edit this field while modifying a Layer 3 VPN service order or service.

Range: 0 through 128 characters

4. Specifying the encapsulation settings for a particular UNI:



NOTE: The fields specified in the Encapsulation Settings box are based on the Encapsulation type. The Encapsulation Settings box is not available if you have selected the Encapsulation as *Port*.

- If you have selected the **Encapsulation** as *Dot1Q*, or *QinQ*, or *Flexible UNI*, specify whether the **Autopick Interface Unit** can be selected automatically or manually.

- To assign the **Unit ID** automatically, select the **Autopick Interface Unit** check box.
- To assign the **Unit ID** manually, clear the **Autopick Interface Unit** check box.

The window expands to include the **Unit ID** field. In the **Unit ID** field, type a value.

Range: 1 through 1073741823



NOTE: The unit ID value that you have specified in the Enter Order Information page is displayed in the Unit ID field.

- If you have selected the **Encapsulation** as *Dot1Q*, or *QinQ*, or *Flexible UNI*, specify whether the **Autopick VLAN ID** can be selected automatically or manually.

- To assign the **VLAN ID** automatically, select the **Autopick VLAN ID** check box.
- To assign the **VLAN ID** manually, clear the **Autopick VLAN ID** check box.

The window expands to include the **VLAN ID** field. In the **VLAN ID** field, type a value.



NOTE: The unit ID value that you have specified in the Enter Order Information page is displayed in the UNIT ID field.

- If you have selected the **Encapsulation** as *QinQ*, select the **Customer VLAN Type**.

If the **Customer VLAN type** is *Transport all traffic*, select the **Outer TP ID**.

If the **Customer VLAN type** is *Transport single vlan*, select the **Customer VLAN**, **Inner TP ID**, and **Outer TP ID**.



NOTE: You can optionally specify Inner TP ID and Outer TP ID.

5. In the IP section of the Site Settings page, clear the **Autopick Interface IP** check box to specify the **Interface IP address**.

Select the **Autopick Interface IP** check box to specify the **IP Address Pool** and **IP Block Size**.



NOTE: You cannot edit the **Autopick Interface IP** check box if you have not selected the **Editable in Service Order** check box in the service definition.

6. In the Routing Protocol section of the Site Settings page, select the **Protocol** type.

If the **Protocol** type is **BGP**, specify the following information:

- **Neighbor IP address**



NOTE: You need to clear the **Autopick neighbor IP** check box to specify the **Neighbor IP** address.

- **Peer AS**

If the **Protocol** type is **OSPF**, specify the following information:

- **OSPF area ID**—Specify any valid IPV4 address in W.X.Y.Z "dot" notation.

Range: 0.0.0.0 through 225.255.255.255

- **OSPF version**—Select the OSPF version from the list.

7. When you have finished configuring the endpoint settings, click **Review** to examine the defined settings. You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages pertain to the settings you want to modify. Click **Back** to return to the previous page of the wizard; else click **Cancel** to discard the changes.

Deploying the New Service

To deploy the service:

1. From the **Manage Deploy Services** window in Deploy mode of Service View of Connectivity Services Director, perform one of these actions:
 - To deploy the service immediately, select **Deploy now** and then click **OK**.
 - To deploy the service later, select **Schedule deployment**, select a date and time, and then click **OK**.
The time field specifies the time kept by the server, but in the time zone of the client.
 - To validate the service, click **Validate**.
2. Navigate to the Deployment Configuration Changes window to view the status of the deploy job.

The service order is now complete.

Related Documentation

- [Stitching a Pseudowire to an L3VPN Service on page 939](#)
- [Creating a Full Mesh Layer 3 VPN Ethernet Service Order on page 941](#)
- [Selecting a Published L3VPN Service Definition for a Service Order on page 985](#)

Modifying a Full Mesh Layer 3 VPN Ethernet Service

For a full mesh Layer 3 VPN service, you can add a new device endpoint, add or delete a UNI, change routing protocol parameters, remove or add static routes, change IP addresses, swap between BGP and static routing protocols (if service definition specifies

BGP and Static), swap between OSPF and static routing protocols (if service definition specifies OSPF and Static).



NOTE: You cannot change the interface of an existing UNI. To perform the equivalent of changing the interface on an existing UNI, add a new UNI with the desired interface, and then delete the old UNI.

After modifying a service, the configuration audit and functional audit information is cleared and the functional audit status is set to pending.

If there is a service template attached to the service definition, there is a link to that template at the bottom of the **Endpoint Settings** section of the window. For instructions on working with service templates in service orders, see [“Creating a Service Order Based on a Service Definition with a Template” on page 990](#).

Modifying a service creates a new service order based on the attribute settings of the existing service.



NOTE: When you modify a service or a service order, the read-only fields in the different pages of the wizard for service or service order modification are grayed out to indicate that you cannot modify those attributes.

- [Adding an Endpoint on page 1058](#)
- [Adding a UNI Interface on page 1060](#)
- [Deleting a UNI Interface and Deleting an Endpoint on page 1062](#)

Adding an Endpoint

To add an endpoint to a multipoint-to-multipoint Ethernet service:

1. In the **Network Services > Connectivity** task pane, select **Service Provisioning > Manage Services**.
2. In the **Manage Services** page, select the service to which you want to add an endpoint.
3. Click the **Modify** icon at the top of the page that displays the previously created service orders.

The **Modify Service** page appears.

Current service settings appear in the main display area. The **General Information** box contains a unique name for the service order that will request the change.

4. In the **Order name** field, change the name of the modification service order, if desired.
5. Click the **Node Settings** button to view the endpoints or devices that are associated with the service.

- In the **Service Nodes** table, click **Add**.

The **Choose Endpoints** window shows available N-PE devices that are not part of the service.

- Select the devices and the interfaces corresponding to the selected devices on which you want to add new endpoints, then click **OK**. You are returned to the Node Settings page of the Manage Service Orders wizard.

Name	Service Type	Customer	State	Status	Fault Status	Definition	Activation Date	Last Modified Date
ldp_fm_test1	VPLS	test	DeploymentPending	Down		ldp_fm_test1	August 28, 2015, 1...	August 28, 2015, 1...
p2p_121	P2P	test	Deployed-Active	Down		ELine-QinQ-AirVLA...	August 27, 2015, 1...	August 28, 2015, 2...
p2p_noservice...	P2P	test	Deployed-Active	Down		p2p_eccc	August 28, 2015, 1...	August 28, 2015, 1...
p2p_existingser...	P2P	test	DeploymentPending	Down		p2p_eccc	August 28, 2015, 1...	August 28, 2015, 1...
Raj-P2P-1055	P2P	test	Deployed-Active	Up		ELine-Dot1q-Single...	August 29, 2015, 2...	August 29, 2015, 2...
Apple-P2P-1075	P2P	Apple	Deployed-Active	Down		ELine-Dot1q-Single...	August 29, 2015, 2...	August 29, 2015, 2...
p2p_cfm	P2P	test	Deployed-Inactive	Down		ELine-Dot1q-Single...	August 29, 2015, 3...	August 29, 2015, 3...
P2P_Traffic_R1-R4	P2P	Apple	Deployed-Active	Up		ELine-Dot1q-Single...	August 29, 2015, 1...	August 29, 2015, 1...
p2p_template	P2P	Apple	DeploymentPending	Down		P2P_template	August 30, 2015, 4...	August 30, 2015, 4...
ldp9131313	P2P	test	Deployed-Active	Down		ldp1	August 30, 2015, 9...	August 30, 2015, 9...
vpls_pr	VPLS	test	Deployed-Active	Up		ldp_fm_test1	August 28, 2015, 1...	August 28, 2015, 1...
VPLS-Traffic-R1...	VPLS	Apple	Deployed-Active	Down		ELAN-BGP-Dot1Q...	August 29, 2015, 1...	August 29, 2015, 1...
new_so1	VPLS	Apple	Deployed-Active	Up		ELAN-BGP-Dot1Q...	August 30, 2015, 2...	August 30, 2015, 2...
vpls_ldp_324321...	VPLS	test	Deployed-Active	Down		vpls_ldp090097097	August 30, 2015, 9...	August 30, 2015, 9...
QinQTagging	L3VPN	Apple	DeploymentPending	Down		L3VPN-OSPF-Static	August 30, 2015, 1...	August 30, 2015, 1...

To filter and sort the display of objects, enter the name of the object as a match criterion in the Search box and click the Search icon. The page refreshes to display only the object names that match with the search term. You can use the paging controls to navigate across multiple pages of objects as necessary.

The service modification window shows the added devices with system recommended choices for UNI.

- Select the devices on which you want to add new endpoints, and then click **Next**.

The service modification window shows the added devices with system recommended choices for UNI. To select a different UNI, see [“Adding a UNI Interface” on page 1060](#).

- Click **Finish** to save the modified service order. You are returned to the Manage Service Orders page.
- In Deploy mode of the Service View of Connectivity Services Director, select one of the following:
 - Deploy now to deploy modified service immediately when you click, OK
 - Schedule deployment to specify a date and time to deploy the modified service later. The default time is the current date and time when you select the option.

11. Click **OK**.

The service modification deployment job ID is assigned.

12. Click the Job ID.

You see the service modification deployment job details in the **System > Manage Jobs > Job Management** page. The **Job Management** page presents the job information by job ID, Name, Percent complete, State, Job Type, Summary, Scheduled Start, Username, and Recurrence. The State column indicates whether the modified service deployment is successful.



NOTE: Alternatively, to display the Job Management page, from the Junos Space Platform UI, select **Jobs > Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

Adding a UNI Interface

To add a UNI on a device that is already part of a multipoint-to-multipoint Ethernet service:

1. In the **Network Services > Connectivity** task pane, select **Service Provisioning > Manage Services**.

2. In the **Manage Services** page, select the service to which you want to add a UNI.

3. Click the **Modify** icon at the top of the page that displays the previously created service orders.

Current service settings appear in the main display area. The **General Settings** box contains a unique name for the service order that will request the change.

4. In the service **Order name** field, change the name of the modification service order, if desired.

5. Click the **Site/Endpoint Settings** button to view the interfaces on endpoints or devices that are associated with the service.

6. In the **User-to-Network Interfaces** table, click **Add**.

The **Choose Endpoints** window shows available N-PE devices that are not part of the service.

7. Select the devices on which you want to add new interfaces. The window refreshes to display all the user-to-network (UNI) or ingress interfaces for the selected device

in the lower part of the window as a tabular grid. Select the interfaces that you want to assign to the service order, and then click **OK**.

To filter and sort the display of objects, enter the name of the object as a match criterion in the Search box and click the Search icon. The page refreshes to display only the object names that match with the search term. You can use the paging controls to navigate across multiple pages of objects as necessary.

Based on the devices you select in the top half of the dialog box, the interfaces that are present in the selected device are displayed in the lower half of the dialog box. Select the check boxes next to the interfaces that you want to associate with the service.

You are returned to the Node Settings page of the Manage Service Orders wizard.

8. The **Interface IP** field displays the interface IP address.
9. The **Autopick VLAN ID** check box is selected by default to allow Network Activate to select a VLAN ID. If you deselect the **Autopick VLAN ID** check box, you must either enter a different value in the service **VLAN ID** field manually.
10. Select a routing protocol from the drop-down list box.
11. Click **Modify**.
12. Click **Modify**.

You can now deploy the modified service.

13. In the **Deployment Options** dialog box, select one of the following:
 - Save only and Validate to save the service modification and validate it.
 - Deploy now to deploy modified service immediately when you click, OK
 - Schedule deployment to specify a date and time to deploy the modified service later. The default time is the current date and time when you select the option.
14. Click **OK**.

The service modification deployment Job ID link appears.

15. Click the Job ID.

You see the service modification deployment job details in the **System > Manage Jobs > Job Management** page. The **Job Management** page presents the job information by job ID, Name, Percent complete, State, Job Type, Summary, Scheduled Start, Username, and Recurrence. The State column indicates whether the modified service deployment is successful.



NOTE: Alternatively, to display the Job Management page, from the Junos Space Platform UI, select **Jobs > Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

Deleting a UNI Interface and Deleting an Endpoint

To delete a UNI from a multipoint-to-multipoint Ethernet service:

1. In the **Network Services > Connectivity** task pane, select **Service Provisioning > Manage Services**.
2. In the **Manage Services** page, select the service from which you want to delete a UNI.
3. Click the **Modify** icon at the top of the page that displays the previously created service orders.

Current service settings appear in the main display area. The **General Settings** box contains a unique name for the service order that will request the change.

4. In the service **Order name** field, change the name of the modification service order, if desired.
5. Click the **Site/Endpoint Settings** button to view the interfaces on endpoints or devices that are associated with the service.
6. In the **User-to-Network Interfaces** table, click **Add**.

The **Choose Endpoints** window shows available N-PE devices that are not part of the service.

7. Select the devices on which you want to add new interfaces. The window refreshes to display all the user-to-network (UNI) or ingress interfaces for the selected device in the lower part of the window as a tabular grid. Select the interfaces that you want to assign to the service order, and then click **OK**.

To filter and sort the display of objects, enter the name of the object as a match criterion in the Search box and click the Search icon. The page refreshes to display only the object names that match with the search term. You can use the paging controls to navigate across multiple pages of objects as necessary.

Based on the devices you select in the top half of the dialog box, the interfaces that are present in the selected device are displayed in the lower half of the dialog box. Select the check boxes next to the interfaces that you want to associate with the service.

You are returned to the Node Settings page of the Manage Service Orders wizard.

The service modification window shows the added devices with system recommended choices for UNI.

8. Click **Finish** to complete the modification of the service order and save the settings.
9. In Deploy mode of the Service View of the Connectivity Services Director, select one of the following from the Manage Services page:
 - Schedule the change for immediate deployment.
 - Schedule the change for later deployment.
10. You see the service modification deployment job details in the **System > Jobs > Job Management** page. The **Job Management** page presents the job information by job ID, Name, Percent Complete, State, Job Type, Summary, Scheduled Start, Username, and Recurrence. The State column indicates whether the modified service deployment is successful.



NOTE: Alternatively, to display the Job Management page, from the Junos Space Platform UI, select **Jobs > Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

Related Documentation

- [Modifying a Multipoint-to-Multipoint Ethernet Service on page 1026](#)
- [Modifying a Point-to-Multipoint Ethernet Service on page 1033](#)
- [Modifying a Hub-and-Spoke Layer 3 VPN Service Order on page 1042](#)

Understanding Service Validation

You can use a functional audit and a configuration audit to monitor the health of a service for any of the following reasons:

- You have just deployed a service and want to verify that it works before your customer starts to use it.
- You want to perform periodic verification that a service is functioning correctly.
- A customer has reported that a service is not functioning correctly and you need to find out what the problem is and fix it.

The following sections provide instructions for functional audit and configuration audit:

- [Performing a Functional Audit on page 1067](#)
- [Performing a Configuration Audit on page 1077](#)

- Related Documentation**
- [Viewing Configuration Audit Results on page 1098](#)
 - [Viewing Functional Audit Results on page 1102](#)

Highlighting of Endpoints in the Layer 3 VPN, RSVP LSP, and VPLS Service Modification Wizards

In the Edit VPLS Service and Edit L3VPN Service wizards that you use to modify the corresponding service types, the Node Settings and Site Settings pages that display the endpoints and interfaces associated with a service are enhanced to provide an easily-identifiable color-coding format for quickly understanding the changes made to these pages of the wizards. A new row that you add to these pages is displayed in blue. An existing row that is deleted from these pages is displayed in red. An existing row that you update on these pages is shaded in gray. Similarly, the Node Parameters page of the Edit RSVP LSP Service wizard uses this color-coding format to denote added, modified, and deleted nodes.

For the modified and deleted endpoints or nodes that are highlighted in gray and red, respectively, you can select the check boxes beside such rows and click **Revert** to cancel the changes and deletions made to these nodes. You can click Revert only for the modified and deleted nodes, which restores the nodes in the states in which they were present in the service before you changed or deleted them.

PART 12

Auditing Services and Viewing Audit Results

- [Service Provisioning: Auditing Services on page 1067](#)
- [Troubleshooting Devices and Services on page 1113](#)

Service Provisioning: Auditing Services

- [Performing a Functional Audit on page 1067](#)
- [Performing a Configuration Audit on page 1077](#)
- [Troubleshooting N-PE Devices Before Provisioning a Service on page 1080](#)
- [Modifying the Application Settings of Connectivity Services Director on page 1082](#)
- [Troubleshooting the Endpoints of Services on page 1088](#)
- [Basic Requirements of Operational Scripts on page 1095](#)
- [Viewing Configuration Audit Results on page 1098](#)
- [Viewing Functional Audit Results on page 1102](#)
- [Viewing Functional Audit Results for an Inverse Multiplexing for ATM Service on page 1106](#)
- [Modifying a Saved Service Order on page 1107](#)
- [Viewing Service-Level Alarms on page 1110](#)

Performing a Functional Audit

A functional audit determines whether a deployed service instance is functioning. It checks the control plane to ensure connectivity among endpoints and that the UNIs are functioning correctly. It also checks the data plane to verify packet transmission between each valid pair of endpoints in the service.

The functional audit provides both a CLI verification and a troubleshooting feature that allows you to check the status of interfaces, LDP sessions, neighbor links, and endpoints of point-to-point services. The **Functional Audit Results** window displays information about the service statistics for the link you are monitoring. When you click **Troubleshoot** button in the Functional Audit Results window, the **Troubleshooting** page displays status of the interfaces, LDP sessions, neighbor links, and endpoints.

Functional Audit Result

Last Run Time: 29-Aug-2015 05:34:22 Status: DONE [Rerun Functional Audit](#) [Reload Result](#) [Troubleshoot](#)

Service Status

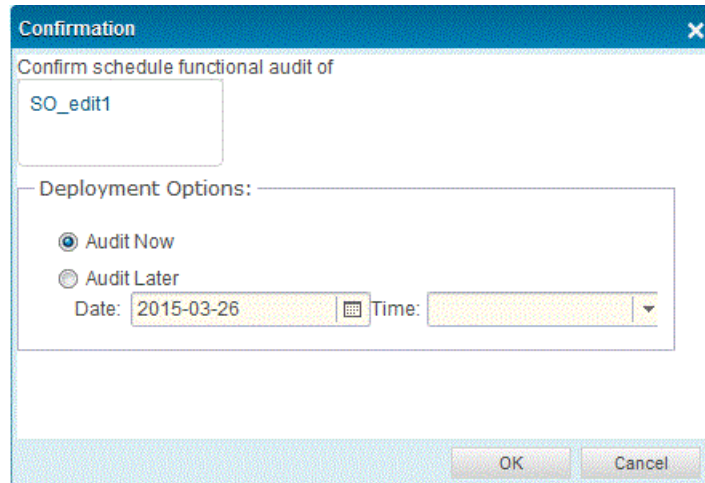
Service Name: P2P_Traffic_R1-R4
 Service Type: ELINEMarlini
 Operation State: Up
 UNIs Up/Down: 2 / 0

Device Name	Interface Name	Topology	Operation State	Up Remote UNI	Down Remote UNI	Troubleshoot St...
960R1_SV_Alok_re	ge-0/0/2.1	P2P	Up	1	0	-
480R4_SV_Alok_re	ge-0/0/2.1	P2P	Up	1	0	-

Performing the Functional Audit

To perform a functional audit:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
4. In the **Network Services > Connectivity** task pane, select **Audit Results > Functional Audit**. Alternatively, you can select a service order, click the **Audit** button at the top of the table of listed service orders from the Manage Network Services page and select **Run Functional Audit**.



5. In the **Schedule Functional Audit** dialog box, do one of the following:

- a. Select **Audit Now**, then click **OK**.

The **Job Details** dialog box appears for you to click the Job ID link to see the functional results. The **Job Management** page displays the functional audit details by job ID, name, percentage complete, state, job type, summary, scheduled start time, user, and recurrence.



NOTE: Alternatively, to display the Job Management page, click the **System** icon on the Connectivity Services Director banner, and select **Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

- b. Select **Audit Later**, enter a date and time, then click **OK**.

To monitor the progress of an audit after selecting **Audit Later**, after the scheduled time of the audit:

- a. On the Junos Space Network Management Platform user interface, select **Jobs**.
- b. On the **Jobs** statistics page, select the **Functional Audit** segment of the Job Types pie chart.

The **Job Management** page appears filtered by functional audit jobs.

- c. Select the functional audit job that you want.

Summary information about the audit appears in the quick look panel.

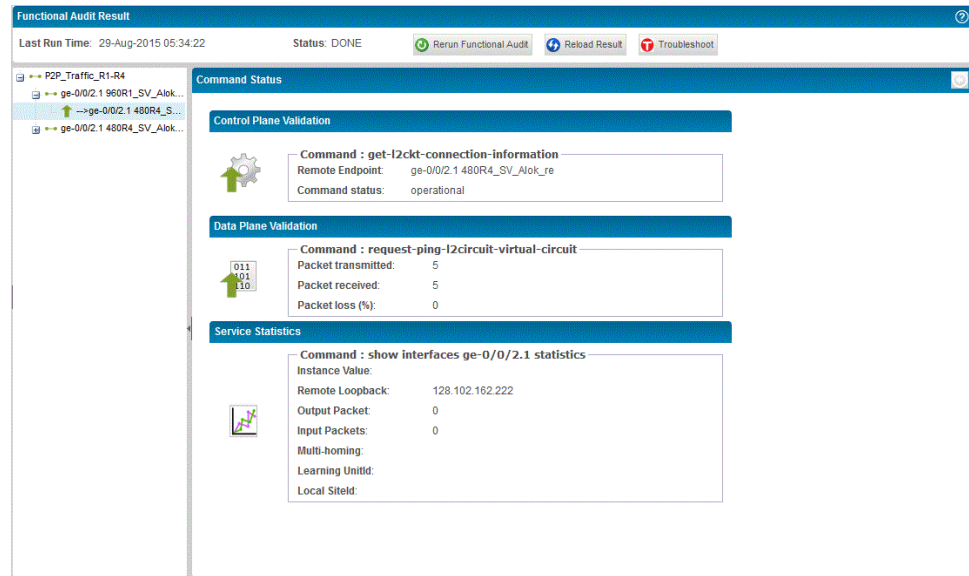
- d. In the filter bar, select the table view icon to see additional information about the job. If the service failed the audit, information about the failure appears in the **Summary** field.



NOTE: Functional audit can be run for multiple services from Build mode of Service View of the Connectivity Services Director GUI. From the Manage Network Services page, select the check boxes beside multiple services, and click the Audit/Results button at the top of the table of configured services. When the Audit/Results button is clicked, the Schedule Functional Audit window is displayed, which enables you to perform the audit immediately or schedule it to be run at a later time. You can view detailed, ingrained information about the output of the functional audit that you performed for a service from the Functional Audit Results window. Select the Service-name > Interface-name Device-name > Remote Interface - Remote Device in the left pane of the window. The control plane and data plane statuses are displayed by running service-specific commands in the right pane of the window. Click Rerun Functional Audit at the top-right corner of the window to perform the audit again. If the Status field displays as Completed, an audit can be run again; else, if the Status field displays as Ongoing, it denotes that an audit is currently in progress, you must wait for the running instance to be completed to perform a functional evaluation again.

Click Reload Result at the top-right corner of the window to refresh the results of the audit and display the updated information. You can refresh the results only for completed audit instances. When you select Service-name in the left pane of the window, service status information is displayed in the right pane. The Service Status window displays details such as the operational status of the service, the device name, the topology used in the service are displayed in a tabular format. The number of UNI interfaces and PE devices that are up and down is also shown. When you select Service-name > Interface-name Device-name > Remote Interface - Remote Device in the left pane of the window, endpoint status information is shown in the right pane. The Endpoint Status window displays details of the device name, the topology used in service, remote UNIs status, and device status of the selected service.

The Service Status field corresponding to the service for which polled data is not available is displayed as NA. The Service Status field represents the overall status of a service. To calculate the overall service status, a polling mechanism is used to retrieve data from devices by Connectivity Services Director. Because the overall status of a service involves multiple devices, it is possible to calculate and update service statuses, based on an event from one of the devices because the status of all endpoints of a service needs to be determined to compute the overall service status. It is an expensive operation to send requests to all endpoints, based on an event from a single device. As a result, a polling method is used to obtain the overall status of the device. Because the polled data represents a snapshot at a point in time, a delay occurs in updating the status of a service. Also, while polling, if service information from one of the devices is not available, the service is marked as down.



6. To view additional details about the functional audit, including results from checking the control plane and the data plane, see [“Viewing Functional Audit Results” on page 1102](#).

CLI Verification

The CLI verification feature of a functional audit works by running commands that perform verification and reporting relevant information.

The following table shows the commands that are used for each service type.

	XML Commands		CLI Commands	
Service Type/ Device Type	Control Plane	Data Plane	Control Plane	Data Plane
ELINE Martini/ M Series and MX Series	<pre><get-l2ckt-connection-information> <neighbor>neighborIP</neighbor> <interface>interfaceName </interface> </get-l2-ckt-connection-information></pre>	<pre><request-ping-l2circuit-virtual-circuit> <neighbor>neighborIP</neighbor> <virtual-circuit-id>VCID</virtual-circuit-id> </request-ping-l2circuit-virtual-circuit></pre>	<pre>show l2circuit connections neighbor neighborIP interface interfaceName show ppp interface mlppp group1 members</pre>	<pre>ping mpls l2circuit virtual-circuit VCID neighbor neighborIP</pre>
<p>Where:</p> <p><i>neighborIP</i> = Address of remote neighbor</p> <p><i>VC ID</i> = Virtual Circuit ID</p> <p><i>interfaceName</i> = Name of interface</p>				

	XML Commands		CLI Commands	
Service Type/ Device Type	Control Plane	Data Plane	Control Plane	Data Plane
BX Series	Not supported.	<pre><get-l2circuit-information> <l2circuit-name> name<l2circuit-name> <brief/> </get-l2circuit-information></pre>	Not supported.	show l2circuit <i>name</i> brief
Where: Name = name of the l2 circuit ID				
VPLS/ M Series	<pre><get-vpls-connection-information> <instance> routing_instance_name </instance> <local-site> local-siteID </local-site> <remote-site> remote-siteID </remote-site> </get-vpls-connection-information></pre>	<pre><request-ping-vpls-instance> <instance-name> routing_instance_name </instance-name> <destination-mac> destMacValue </destination-mac> <source-ip> sourceIP </source-ip> <learning-vlan-id> learning-vlan-id </learning-vlan-id> </request-ping-vpls-instance></pre>	<pre>show vpls connections instance routing_instance_name local-site local-siteID remote-site remote-siteID</pre>	<pre>ping vpls instance routing_instance_name destination-mac destMacValue source-ip sourceIPValue learning-vlan-id learningVlanID</pre>
Where: <i>routing_instance_name</i> = Routing instance name <i>destMacValue</i> = Destination MAC address <i>sourceIP</i> = Source IP address <i>local-SiteID</i> = Name or ID of VPLS local site <i>remote-SiteID</i> = ID of VPLS remote site <i>learning-vlan-id</i> = Learning VLAN identifier				
L3VPN/ Junos	<pre><get-route-information> <table> bgp.l3vpn.0</table> <rd-prefix>destinationRDPrefix</rd-prefix> </get-route-information></pre>	<pre><ping><routing-instance> routingInstanceValue </routing-instance> <count>5 </count></pre>	<pre>show route table bgp.l3vpn.0 rd-prefix destinationRDPrefix</pre>	<pre>ping routing-instance routingInstanceValue count</pre>
Where: <i>routingInstanceValue</i> = Routing instance name <i>destinationRDPrefix</i> = Route Distinguisher: remote UNI IP address <i>destinationUniInterfaceIP</i> = Destination UNI IP address				

For the data plane, the Junos Space software places a static MAC address in the forwarding table of the remote endpoint, which it uses to verify correct packet transfer.



NOTE: Data plane validation of a VPLS service works for MX Series devices running Junos Release 9.4 or later. If the service under audit contains an M Series device or an N-PE device running Junos Release 9.2 or 9.3, the functional audit does not complete successfully and generates a message stating that functional audit is not supported on that platform.

The following table shows the commands for VPLS service type:

Service Type	Device Family	XML Commands	CLI Commands	Category
VPLS	M Series	<get-vpls-connection-information> <instance> <i>instanceValue</i> </instance> </get-vpls-connection-information>	show vpls connection instance <i>instanceValue</i>	Route
		<get-mpls-lsp-information> <ingress/> </get-mpls-lsp-information>	show mpls lsp ingress	MPLS
		<get-mpls-lsp-information> <egress/> </get-mpls-lsp-information>	show mpls lsp egress	MPLS
		<get-mpls-static-lsp-information> <ingress/> </get-mpls-static-lsp-information>	show mpls static-lsp ingress	MPLS
		<get-rsvp-session-information> </get-rsvp-session-information>	show rsvp session	Route
		<get-route-information> <table>inet.3</table> </get-route-information>	show route table inet.3	Route
		<get-interface-information> <terse/><interface-name> <i>interfaceValue</i> </interface-name> </get-interface-information>	show interface <i>interfaceValue</i> terse	UNI
		<get-interface-information> <statistics/> <interface-name> <i>interfaceValue</i> </interface-name> </get-interface-information>	show interface <i>interfaceValue</i> statistics	UNI
		<get-route-information> <table> <i>instanceValue</i> </table> <protocol> <i>bgp</i> </protocol> </get-route-information>	show route protocol bgp table <i>instanceValue</i> .l2vpn.0	Route
Where:				
<i>instanceValue</i> = Name of the service				
<i>neighborIP</i> = Address of the remote neighbor				
<i>interfaceValue</i> = Name of the interface				

The following table shows the commands for L3VPN service type:

Service Type	Device Family	XML Commands	CLI Commands	Category
--------------	---------------	--------------	--------------	----------

L3VPN	M Series	<get-mpls-lsp-information> <ingress/> </get-mpls-lsp-information>	show mpls lsp ingress	MPLS
		<get-mpls-lsp-information> <egress/> </get-mpls-lsp-information>	show mpls lsp egress	MPLS
		<get-interface-information> <terse/> <interface-name> </get-interface-information>	show interfaces <i>instance</i> <i>value</i> .initvalue terse	Route
		<get-forwarding-table-information> <vpn> <i>instance</i> </vpn> </get-forwarding-table-information>	show route forwarding-table vpn <i>instance</i>	Route
		<get-rsvp-session-information> </get-rsvp-session-information>	show rsvp session	Route
		<get-interface-information> <statistics/> <interface-name> </get-interface-information>	show interfaces <i>instance</i> statistics	UNI
		<get-mpls-static-lsp-information> <ingress/> </get-mpls-static-lsp-information>	show mpls static-lsp	MPLS
		<get-ospf-neighbor-information> </get-ospf-neighbor-information>	show ospf neighbor	Route
		<get-route-information> <table> <i>bgp.l3vpn.0</i> </table> <rd-prefix> <i>destination</i> </rd-prefix> </get-route-information>	show route table bgp.l3vpn.0	Route
		<get-lacp-interface-information> <interface-name> <i>lag</i> / <i>Interface</i> </interface-name> </get-lacp-interface-information>	show lacp interfaces	UNI
		<get-mc-ae-interface-information> </get-mc-ae-interface-information>	show interfaces mc-ae	UNI
		<get-vrrp-interface-information> <interface-name> <i>Interface</i> </interface-name> </get-vrrp-interface-information>	Show vrrp <i>interfaceName</i>	UNI
			Show bridge domain <i>domainName</i>	UNI

```
<get-bridge-instance-information>  
<bridge-domain-name>  
  domainName  
</bridge-domain-name>  
</get-bridge-instance-information>
```

Where:

instanceValue= Name of the service

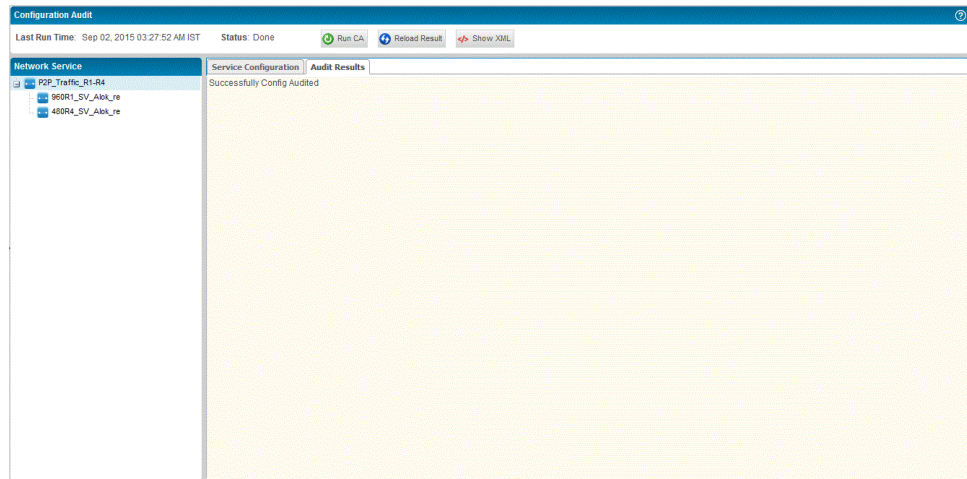
neighborIP= Address of the remote neighbor

interfaceValue= Name of the interface

- Related Documentation**
- [Performing a Configuration Audit on page 1077](#)
 - [Troubleshooting N-PE Devices Before Provisioning a Service on page 1080](#)
 - [Modifying the Application Settings of Connectivity Services Director on page 1082](#)
 - [Troubleshooting the Endpoints of Services on page 1088](#)
 - [Viewing Configuration Audit Results on page 1098](#)
 - [Viewing Functional Audit Results on page 1102](#)
 - [Viewing Functional Audit Results for an Inverse Multiplexing for ATM Service on page 1106](#)

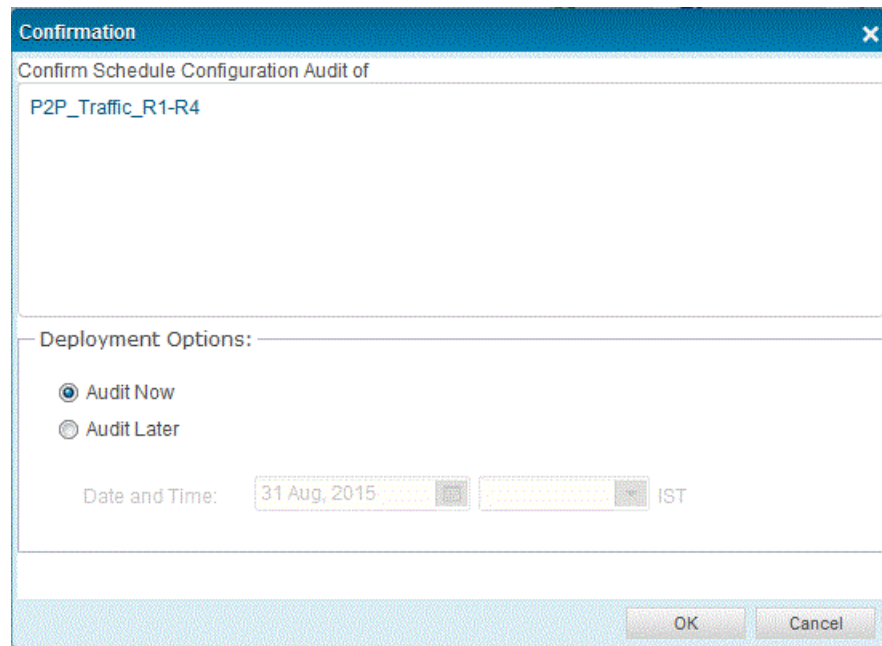
Performing a Configuration Audit

A configuration audit can help you determine whether the service configuration on the device has been changed out of band. To this end, you can compare the results of a configuration audit with the service configuration in the Junos Space database. The following example shows a sample comparison.



To perform a configuration audit:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
4. In the **Network Services > Connectivity** task pane, select **Audit Results > Configuration Audit**, and from the Configuration Audit page that is launched, click the **Run Configuration Audit** button. Alternatively, you can select a service order, and click the **Audit** button at the top of the table of listed services from the Manage Network Services page and select **Run Configuration Audit**.



5. In the **Schedule Configuration Audit** window, either:
 - Select **Audit Now**, then click **OK**.
An informational dialog appears, stating that the configuration audit job is successfully triggered with the job ID, and an **OK** button.
 - Select **Audit Later**, enter a date and time, then click **OK**.
6. To monitor the progress of an audit after selecting **Audit Now**, click the Job ID in the **Audit Information** window. The **Job Management** page shows information about the configuration audit job.



NOTE: Alternatively, to display the Job Management page, click the **System** icon on the Connectivity Services Director banner, and select **Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

The **State** field indicates whether the service passed or failed the audit. If the service failed the audit, then the **Summary** field provides information about the failure.

To monitor the progress of an audit after selecting **Audit Later**, after the scheduled time of the audit:

- a. On the Junos Space Network Management Platform user interface, select **Jobs**.
- b. In the **Job Types** chart, select the **Configuration Audit** segment of the pie chart.

- c. Select the configuration audit of interest from the list on the **Job Management** page.
Summary information about the audit appears in the quick look panel.

- d. In the filter bar, select the table view icon to see additional information about the job. If the service failed the audit, information about the failure appears in the **Summary** field.

- 7. In the **Audit Information** window, click the job ID of the configuration audit.

The **Job Management** window appears and shows a filtered view of the job inventory, showing only the configuration audit job.



NOTE: If a resynchronization between a device and the Junos Space database is ongoing when the configuration audit job starts, the configuration audit job suspends until the resynchronization job finishes. If the resynchronization job fails to complete, the audit could be suspended indefinitely. To allow the audit to proceed, go to the **Job Management** workspace and cancel the resynchronization job, as described in *Canceling a Job*.

- 8. In the **Status** column, check the status of the audit to determine whether it succeeded or failed.

Check the **Summary** column, which contains useful service information such as the VC ID and endpoint information. For some failed deployments, this column also contains information about why the deployment failed.



NOTE: When a configuration audit is performed, the XPATH attributes that are present in the service configuration are used. Only the addition, modification, or deletion of the XPATH attributes is detected, and the creation of a new attribute (child XPATH) on a device is not determined. The audit operation disregards such attributes and does not identify them. This behavior is expected and occurs because Junos Space Platform software audits only the settings present a user template. If the template has a container, Junos Space Platform only audits to determine whether the device is configured with this container. If a user wants to audit any container child, the user needs add it into the template. This scenario is similar to an out-of-band configuration change on the device, which Junos Space Platform can determine only if the system of record (SOR) mode is set for the Junos Space Network Management Platform application.

Related Documentation

- [Performing a Functional Audit on page 1067](#)
- [Troubleshooting N-PE Devices Before Provisioning a Service on page 1080](#)

- [Modifying the Application Settings of Connectivity Services Director on page 1082](#)
- [Troubleshooting the Endpoints of Services on page 1088](#)
- [Viewing Configuration Audit Results on page 1098](#)
- [Viewing Functional Audit Results on page 1102](#)
- [Viewing Functional Audit Results for an Inverse Multiplexing for ATM Service on page 1106](#)

Troubleshooting N-PE Devices Before Provisioning a Service

You can use the **Troubleshoot** option to check PE router configurations before you deploy a new service or troubleshoot PE router configurations if you are unable to deploy a new service.

To check the configuration on a PE router, follow these steps:

1. In the **Network Services > Connectivity** task pane, select **Prestage Devices > Manage Device Roles**

The **Manage Device Roles** page appears displaying all devices on the network that are assigned the N-PE role

2. Select the device that you want to troubleshoot.

3. In the **Actions** menu, select **Troubleshoot**.

The **Troubleshoot Device** window appears. The table here describes the show commands that you can run to check the configuration on a N-PE device.

Table 133: Commands Available in the Troubleshoot Device Window

Command	Description	Fields Displayed
show mpls lsp ingress	Display whether ingress LSP is up and running.	<ul style="list-style-type: none"> • Device name • LSP State • Destination Address
show mpls lsp egress	Display whether egress LSP is up and running.	<ul style="list-style-type: none"> • Device name • LSP State • Destination Address
show bgp summary	Display summary information about BGP and its neighbors to determine if routes are received from peers in the autonomous system (AS). When a BGP session is established, the peers exchange update messages.	<ul style="list-style-type: none"> • Peer Address • Peer State
show ospf neighbor	Display information about OSPF neighbors.	<ul style="list-style-type: none"> • Interface Name • Neighbor Address • OSPF Neighbor State

Table 133: Commands Available in the Troubleshoot Device Window (continued)

show bgp neighbor	Display information about all BGP peers.	<ul style="list-style-type: none"> • Peer Address • Peer State • Local AS
show ldp interface	Display standard status information about all LDP-enabled interfaces for all routing instances.	<ul style="list-style-type: none"> • Interface Name • LDP Neighbor Count
show ldp neighbor	Display standard information about LDP neighbors for all routing instances.	<ul style="list-style-type: none"> • Interface Name • Neighbor Address • Remaining Time—remaining hold time before the neighbor expires, in seconds.
show rsvp session	Display information about Resource Reservation Protocol (RSVP) sessions.	<ul style="list-style-type: none"> • Name • LSP State • Destination Address <p>For complete information about the fields displayed for the show rsvp session command, see the <i>Junos Software Routing Protocols and Policies Command Reference</i>.</p>
show rsvp interface	Display the status of Resource Reservation Protocol (RSVP)-enabled interfaces and packet statistics.	<ul style="list-style-type: none"> • Interface Name • RSVP Status • Static Bandwidth • Available Bandwidth • Total Reserved Bandwidth
show isis adjacency	Display information about intermediate System-to-Intermediate System (*IS-IS) neighbors.	<ul style="list-style-type: none"> • Interface Name • Adjacency State • System Name <p>For complete information about the fields displayed for the show isis adjacency command, see the <i>Junos Software Routing Protocols and Policies Command Reference</i>.</p>

4. Select on any show command to view device-specific configuration information.



NOTE: For additional information about a PE device configuration, you can explicitly run a show command with the extensive option, for example, **show mpls lsp extensive**.

Related Documentation

- [Performing a Functional Audit on page 1067](#)
- [Performing a Configuration Audit on page 1077](#)
- [Modifying the Application Settings of Connectivity Services Director on page 1082](#)
- [Troubleshooting the Endpoints of Services on page 1088](#)
- [Viewing Configuration Audit Results on page 1098](#)

- [Viewing Functional Audit Results on page 1102](#)
- [Viewing Functional Audit Results for an Inverse Multiplexing for ATM Service on page 1106](#)

Modifying the Application Settings of Connectivity Services Director

To modify the configuration settings of services activation-related capabilities of Connectivity Services Director, perform the following steps:

1. To open the Preferences page, click  in the Connectivity Services Director banner and select **Preferences** as shown in [Figure 18 on page 123](#).

Figure 50: Accessing the Preferences Page



The Preferences page appears, with **User Preferences** as the default tab.

2. Click the **Services Activation** tab.
3. Click any parameter, or specify a different value for parameters that accept values, to modify it.



NOTE: You cannot modify the application settings if another user is currently modifying them.

4. Click **OK** to save the changes that you made in the **Connectivity Services Director** application or click **Cancel** to retain the original settings.

Also, you can modify the configuration settings for the Connectivity Services Director application using the Junos Space Platform GUI.

To modify the configuration settings of Connectivity Services Director using the Junos Space Platform GUI, perform the following steps:

1. From the **Network Management Platform** task pane, select **Administration** > **Applications**.
The **Applications** page that appears displays a list of the applications in the Network Management platform.
2. Right-click **Network Activate** and select **Modify Applications Settings**.

The **Modify Application Settings** page that appears displays a list of the parameters that can be modified.

3. Click any parameter to modify it.



NOTE: You cannot modify the application settings if another user is currently modifying them.

4. Click **Modify** to save the changes that you made in the **Connectivity Services Director** application or click **Cancel** to retain the original settings.

To understand the parameters of the Connectivity Services Director application settings, refer to [Table 14 on page 123](#).

Table 134: Parameters in Connectivity Services Director Application Settings

Fields	Description
Deployment	
Check service version	Select this check box to validate the version of the service being configured.
Deploy configuration to the device	Select this check box to deploy the configuration to the device.
Enable service alarms	Select this check box to enable the service alarms. Enabling the service alarms causes a GUI impact on the Connectivity Services Director application. When you select the check box and deploy the service, the interface goes down, resulting in the failure to update the fault status. When you right-click Service and select View Service Alarms , the latter does not appear in the results.
Save configuration in XML format	Select this check box to save the configuration of the device in XML format.
Show configuration in set format	Select this check box to display the configuration in set format.
Use two-phase commit for service provisioning	Select this check box to push the configuration on all the network elements automatically, making either one or all successful.
Use vlan maps for E-Line services	When this check box is selected, normalization of VLAN tags is performed using the input or output VLAN maps. This check box is selected by default.
Use vlan maps for flexible tagged services instead of normalized vlan (VPLS)	When this check box is cleared, normalization of VLAN tags is performed using normalized tags under routing instance. This check box is cleared by default.
Audit	

Table 134: Parameters in Connectivity Services Director Application Settings (continued)

Fields	Description
Enable Functional Audit after deployment	Select this check box to perform the functional audit automatically, after the service is deployed successfully. By default, the functional audit is not checked. Extra time is taken to complete both the functional audit and deployment.
Functional Audit Waiting Time after deployment	<p>Specify the initial wait time to auto-schedule a functional audit job after deployment.</p> <p>If the entered value is greater than 30 minutes, it is reset to 30 minutes. If the entered value is less than 1 minute, the wait time is ignored.</p> <p>The range is from 1 minute through 30 minutes.</p>
Perform Functional Audit on Control plane only	Select this check box to make the functional audit ignore the data plane verification and to consider only the control plane.
User Interface	
Allow template modification for service	Select this check box to allow the templates to be changed during the service modification.
Bandwidth Combo Items Count	<p>Specify the bandwidth combo items count.</p> <p>In Create P2P service order page, if the bandwidth range exceeds the bandwidth combo items count, then the bandwidth input is taken in text field.</p> <p>The default value is 100.</p>
Service Detail Wait Time (sec)	Specify the period of time in seconds as the wait period for retrieving service details during service template modification.
Monitoring	
Perform Monitoring on Failed Functional Audit	Select this check box to perform monitoring if the functional audit fails.
Pseudowire Redundancy Transition TimeDelay	<p>Select this check box to dump the configuration files.</p> <p>Specify the time delay to issue the remote procedure call (RPC) call for redundancy service. Since there is no support for the fault management for redundancy service, it should not update the fault status as down, when the interface goes down as the service will be running with the help of backup device. The RPC is issued to check the status of the service. If the value of this time delay is 2 seconds and the interface goes down, it waits for 2 seconds to check whether the service is up, with the help of the backup device and correspondingly updates the fault status.</p> <p>The default value is 2 seconds.</p>
Statistics Aggregation Reporting	<p>Specify the manner in which the aggregated results are returned for a query that polls and retrieves data from devices. Two aggregation values are supported:</p> <ul style="list-style-type: none"> • Total: Sum of the number of packets received in the interval • Average: Average of the total number of packets received in the interval

Table 134: Parameters in Connectivity Services Director Application Settings (continued)

Fields	Description
Logging	
Dump Configuration Files	By default, the configuration files are not dumped into the log directory. This is enabled, if there is a need to provide troubleshooting to Juniper Networks Technical Assistance Center (JTAC).
Dump Deployment Data	Select this check box to write the configlets and error response from the JUNOS devices into the log directory..
Log Directory	Specify the default path of the log directory: <code>/var/tmp/jboss</code>
Prestage Devices	
Pre-stage Wait Time (Sec)	Specify the number of seconds for which the task to trigger a job for prestaging devices must wait after receiving the first notification for prestaging devices. For example, if you specify the prestage wait time as 20 seconds, the prestaging task waits for a period of 20 seconds, after receiving the first notification for prestaging devices, and then initiates the prestaging-devices job.
Pre-stage Idle Time (Sec)	Specify the number of seconds after which the job for prestaging devices is initiated, if no notification is received during the idle period. For example, if you specify the prestage idle time as 10 seconds and if no notification for prestaging devices is received within this period, the job for prestaging devices is triggered immediately after 10 seconds. The prestage idle time value takes precedence over the prestage wait time value.
Loopback Unit	Specify the logical unit of the loopback interface that must be used as the default loopback logical interface for all provisioning tasks that are initiated from Connectivity Services Director. The default logical unit for the loopback interface is 0.
Route Target	
BeginIndex	<p>Specify the least value in the preferred range of numbers, among which a certain number is assigned for each BGP service. Route target allows you to distribute VPN routes to only the routers that need them. When a route target value is entered manually, it should be either of the following two formats: Autonomous System number format or IPv4 format. For Autonomous System number format, the pattern is as-number:2-byte-number. For example, target:100:200.</p> <p>Range: The Autonomous System number format number can be in the range from 1 through 65,535.</p> <p>The IPv4 format is ip-address:2-byte-number. For example, target:10.1.1:2.</p>

Table 134: Parameters in Connectivity Services Director Application Settings (continued)

Fields	Description
EndIndex	<p>Specify the greatest value in the preferred range of numbers, among which a certain number is assigned for each BGP service. Route target allows you to distribute VPN routes to only the routers that need them. When a route target value is entered manually, it should be either of the following two formats: Autonomous System number format or IPv4 format. For Autonomous System number format, the pattern is as-number:2-byte-number. For example, target:100:200.</p> <p>Range: The Autonomous System number format number can be in the range from 1 through 65,535.</p> <p>The IPv4 format is ip-address:2-byte-number. For example, target:10.1.1:2. The EndIndex value should be lesser than the maximum assigned value.</p>
Virtual Circuit ID	
BeginIndex	<p>Specify the least value in the preferred range of numbers, among which a certain number is assigned as the VirtualCircuitID to the new circuit created. This VCID can be manually chosen by the customer or auto-generated by the system. For example, if BeginIndex = 100 and EndIndex = 200, then the VCID would be somewhere between 100 and 200.</p> <p>Minimum: 1</p> <p>The value of BeginIndex should be less than or equal to EndIndex value.</p> <p>The range is from 0 through 200000.</p>
EndIndex	<p>Specify the greatest value in the preferred range of numbers, among which a certain number is assigned as the VirtualCircuitID to the new circuit created. This VCID can be manually chosen by the customer or auto-generated by the system. For example, if BeginIndex = 100 and EndIndex = 200, then the VCID would be somewhere between 100 and 200.</p> <p>Maximum: 2147483647.</p> <p>The range is from 0 through 200000.</p>
Performance Monitoring	
DataSetSize	<p>DataSetSize is the size of the performance monitoring data set in days. This field indicates the number of days of performance monitoring data could be stored for display.</p> <p>The default value is 2880.</p>
Enable Performance Monitoring through scripts	<p>Select the check box to collect the performance data through scripts and opennms will store the data in its database. If this check box is not selected, then performance data such as one-way delay, two-way delay, and frame loss are collected through RPC and stored in the application database.</p>
OSS Config Parameters	
Alcatel Primary Server IP	Specify the IP address of the primary server.
Alcatel Primary Server Port	Specify the port number of the primary server.

Table 134: Parameters in Connectivity Services Director Application Settings (continued)

Fields	Description
Backup Server IP	Specify the IP address of the backup server.
Backup Server Port	Specify the port number of the backup server.
HTTP Connection Timeout	Specify the duration of HTTP connection before the time-out elapses.
Maximum API Requests	Specify the maximum number of simultaneous API requests permitted.
OSS Log Directory	Specify the directory path of the OSS log directory.
OSS Log Filename	Specify the OSS log filename.
OSS User Name	Specify the user name for accessing the OSS server.
OSS User Password	Specify the hashed password for accessing the OSS server.
Synchronize OSS Inventory daily at given time	Sets the daily time at which the CPP system synchronizes third-party devices, added or deleted from the CPP system, with the OSS server.
Use primary server	If the check box is enabled, the CPP system communicates with the primary OSS server.
Service Decommission	
Service Recovery	
OutofBand Notification	<p>Select either of the following options from the OutofBand Notification Action list to specify the action you want to be performed when an OutOfBand notification is received by Connectivity Services Director:</p> <ul style="list-style-type: none"> • Make Device OutOfSync—Causes the device to be made OutOfSync and disables subsequent provisioning on that device until it changes to the In Sync state again • Ignore Notification—Causes the notification to be ignored and device will remain InSync
Store OutofBand Notification XML	Select the check box to enable the storage of OutOfBand notification XML in the Connectivity Services Director database. By default, this check box is not selected, which disables the saving of OutofBand notification XML in the Connectivity Services Director database.
Device Sync Wait Time	<p>Specify the device synchronization waiting time. This is the maximum wait time to complete the device synchronization. After this time duration, irrespective of the device synchronization status, the resources are released.</p> <p>The default value is 60 seconds.</p> <p>The range is from 30 seconds through 300 seconds.</p>
Reports (accessible from the Modify Connectivity Services Director Settings page in the Administration workspace of the Junos Space Platform GUI)	

Table 134: Parameters in Connectivity Services Director Application Settings (continued)

Fields	Description
Retention period for generated Reports days	Move the slider right or left to specify the time period for which the generated reports must be retained in the Connectivity Services Director database. By default, Connectivity Services Director keeps reports for 30 days. However, Network Administrators can change the retention period from 0 to 365 days.
Search (accessible from the Modify Connectivity Services Director Settings page in the Administration workspace of the Junos Space Platform GUI)	
Index auto update interval in seconds	Specify a time interval after which Connectivity Services Director initiates the next indexing on the Search tab. By default this option is selected and the search index update interval is set to 900 seconds. Connectivity Services Director indexes the device inventory data periodically to enable users to perform efficient searches.
Pause indexing during device import	Select this check box to stop indexing while devices are imported into Connectivity Services Director. If you are running short of system memory, selecting this option can help save some memory and speed up the discovery and import of new devices.
Topology (accessible from the Modify Connectivity Services Director Settings page in the Administration workspace of the Junos Space Platform GUI)	
Retention period for Deleted Link days	Move the slider right or left to specify a retention period for the deleted links in Topology. You can also disable the retention of deleted links by moving the slider to the extreme left to denote Never. You can define a maximum of 365 days for deleted links to be maintained in Topology View.

Troubleshooting the Endpoints of Services

Junos OS operation (op) scripts automate network and device management and troubleshooting. Op scripts can perform any function available through the remote procedure calls (RPCs) supported by either the Junos XML management protocol or the Junos Extensible Markup Language (XML) API. Op scripts can be executed manually in the CLI or upon user login, or they can be called from another script. They are executed by the Junos OS management (mgd) process.

Op scripts enable you to do the following things:

- Create custom operational mode commands
- Execute a series of operational mode commands
- Customize the output of operational mode commands
- Shorten troubleshooting time by gathering operational information and iteratively narrowing down the cause of a network problem
- Perform controlled configuration changes
- Monitor the overall status of a device by creating a general operation script that periodically checks network warning parameters, such as high CPU usage.

Op scripts are based on the Junos XML management protocol, and the Junos XML API. Op scripts can be written in either the Extensible Stylesheet Language Transformations (XSLT) or Stylesheet Language Alternative Syntax (SLAX) scripting language. Op scripts use XPath to locate the operational objects to be inspected and XSLT constructs to specify the actions to perform on the located operational objects. The actions can change the output or execute additional commands based on the output.

The troubleshooting feature provides an easy and unique way to troubleshoot the services. You do not have to manually login to a device to check the status of services in the Connectivity Services Director application, but you can do the same using the functionality of operational scripts. You do have the flexibility of writing your own scripts to view the results.

Only Juniper Networks devices are supported by this functionality and this is not applicable to the third-party devices.

The operational scripts can either be created or imported to the platform from the local machine before you start troubleshooting the services or you can run the scripts that are of local type directly from the Functional Audit Result window by clicking the **Troubleshoot** button. For op scripts that are not of local type, the op scripts must be imported and staged on to the device using the Junos Space Network Management Platform application before you can run the scripts from within the Connectivity Services Director application for debugging and diagnosing the service endpoints or devices. Currently, you cannot directly add the scripts to the Connectivity Services Director GUI interface. Scripts with execution type as “Local” (@isLocal=true annotation in the SLAX script) are also listed in troubleshooting window. The listing is sorted and filtered based on the context specified for each service.



BEST PRACTICE: We recommend that you configure a script as a local script for effective and optimal debugging and analysis of the configuration settings contained in the script. The main advantage of a local script is that you need not download the script to a device (because a connection is established with the device by the GUI application and the script is run) and you need not remove the script from a device after you decommission a service.

The following table lists the context in which the OP scripts are written for different types of services:

Table 135: OP Scripts Contexts for Different Service Types

Service Type	Context
P2P LDP	@CONTEXT = "/device/configuration/protocols/l2circuit/neighbor/interface" Example : /device[name="deviceName"]/configuration/protocols/l2circuit/neighbor[name="neighbor IP"]/interface[name="interfaceName.unitID"]
L3VPN	/*@CONTEXT = "/device/configuration/routing-instances/instance/vrf/interface" */ Example : /device[name="device name"]/configuration/routing-instances/instance[name="Service name"]/instance-type[instance-type="vrf"]/interface[name="interfaceName.unitID"]

Table 135: OP Scripts Contexts for Different Service Types (continued)

Service Type	Context
VPLS	<pre>/* @CONTEXT = "/device/configuration/routing-instances/instance/vpls/interface" */</pre> <p>Example : /device[name="device name"]/configuration/ routing-instances/instance[name="Service name"]/instance-type[instance-type="vpls"]/interface[name="interfaceName.unitID"]</p>
P2P (Local switching)	<pre>/* @CONTEXT = "/device/configuration/protocols/l2circuit/local-switching/interface/end-interface" */</pre> <p>Example /device[name="MX801"]/configuration/protocols/l2circuit/local-switching/interface[name="ge-1/0/0/801"]/end-interface[name="ge-1/2/2/881"]</p>
P2P BGP	<pre>/* @CONTEXT = "/device/configuration/routing-instances/instance/bgp/interface" */</pre> <p>Example : /device[name="device name"]/configuration/routing-instances/instance[name="Service name"]/instance-type[instance-type="bgp"]/interface[name="interfaceName.unitID"]</p>
Common context for all services	<pre>/* @CONTEXT = "/device/configuration/interface/" */</pre> <p>Example: /device[name="device name"]/configuration/ interface[name="interfaceName.unitID"]</p> <p>Example commands:</p>

When you select a single service and from the Network Services > Connectivity task pane, select **Audit Results > Functional Audit** to schedule and perform a functional audit operation, the Functional Audit Results window is displayed after the operation of the selected service is validated. If you have previously run a functional audit already run, the result of the previous audit is displayed. To perform a troubleshooting of the selected service, you must click the **Troubleshoot** button. The troubleshooting task runs as a separate event in Connectivity Services Director, whereas troubleshooting was performed together with functional audit in the Services Activation Director GUI.

- [Troubleshooting Services Using Operational Scripts on page 1090](#)

Troubleshooting Services Using Operational Scripts

The operational scripts or the OP scripts are written to view the statistics of a service in the Connectivity Services Director application. All the commands in the OP scripts are user-defined. To view the contexts for writing OP scripts for different service types, refer [Table 135 on page 1089](#).

To execute the OP scripts and view the status of any service:

1. From the **Network Management Platform** task pane, select **Images and Scripts > Scripts**. The **Scripts** page that appears displays a list of the existing scripts.
2. From the list of the scripts available in the SLAX format, right-click a script and click **Stage Scripts on Devices** to push the script onto a device. The **Stage Scripts on Device(s)** page that appears displays a list of the devices associated with the script that you selected.

3. Select the **Select Device Manually** option and select any number of devices to which you want to push the script.



NOTE: The **Enable Scripts on Devices** check box is selected by default.

4. Click **Stage** to stage the script on all the devices that you selected.

The **Stage Scripts Information** dialog box confirms the successful staging of scripts onto the selected devices along with the **Job ID**.

5. Click **Job ID** to view the status of the job on the **Job Management** page.

You are redirected to the **Scripts** page.

6. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
7. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
8. In the Network Services > Connectivity view pane, select **Audit Results > Functional Audit**. Alternatively, you can select a service order, click the **Audit** button at the top of the table of listed service orders from the Manage Network Services page and select **Run Functional Audit**.
9. In the Schedule Functional Audit dialog box, select **Audit Now**, then click **OK**. After the audit is run, the Functional Audit Results window is displayed.
10. From the Functional Audit Results window that displays a list of the devices associated with the service you selected, select the check box next to the device for which you want to diagnose and examine the associated service.
11. Click **Troubleshoot** to perform troubleshooting and analysis of the service for which functional audit is performed.
12. Select the check box next to a service that you want to analyze and monitor for its working and efficiency. The Execute OP Scripts page is displayed.

13. Select an OP script on the **Execute OP Scripts** page.

Script Name	Description	Version	Type	Created Date	Last Updated Date
P2PLDPPredefinedScript.sla	P2P LDP Predefined Script	1	Local	Aug 27, 2015 10:24:22 ...	Aug 27, 2015 10:24:22 ...

Script Name	Name	Description	Value

NOTE: To enter the value for PARAMETERS, click on VALUE column. The value for parameters may be required.

Execute View Last Result Cancel

14. Click the **Value** column to enter any additional parameter for the selected OP script, besides the ones coded in the script.



NOTE: The selection of parameters is entirely dependent on the OP scripts. If the OP scripts support parameters, then all the parameters are listed and you need to enter the values. Parameters can be optional, on the basis of the OP scripts.

15. Click **Execute** to execute the selected OP scripts with the newly added parameters, if any.

A dialog box confirms the execution of the OP scripts along with the **Job ID**.

Job Details

Job 197472 is running

• Scripts results will be available upon job completion.

OK

16. Click **OK**.

You are redirected to the **Execute OP Scripts** page.

17. Click **View Last Result** to view the previous OP scripts execution results.

The **Execute OP Scripts Job Status** dialog box is displayed with the results of the troubleshooting operation.



NOTE: This is an optional step.

Troubleshooting Point-to-Point Services

From the **Execute OP Scripts Job Status** dialog box, you can check status of the interfaces, LDP sessions, neighbor links, and endpoints of a point-to-point service. To select the status you want to check, click on the device from the device list on the left, and select the show command from the **Command** list. This figure shows the routing table for the selected device in the Point-to-Point service.

The following figure shows the status of the LDP session for the selected device and the LDP neighbor status.

Execute OP Scripts Job Status

Device Name	Interface	Script Name	Script Version	Device Name	Status
480R3_EP_Alok_re	ge-0/0/2.212	P2PLDPPredefinedScr...	1	960R2_EP_Alok_re	Success
960R2_EP_Alok_re	ge-0/0/3.212				
480R4_EP_Alok_re	ge-0/0/3.212				

Job Results for P2PLDPPredefinedScript.slax
Script execution output details:

L2Circuit Connection Information			
No Results Found			
Interface Information			
No Results Found			
LDP Session Information			
Address	State	Connection	Hold Time
128.216.194.105	Operational	Open	29
128.216.194.108	Operational	Open	28
128.216.194.118	Operational	Open	23
LDP Neighbor Information			
Neighbor Address	Interface Name	Label	
128.216.194.105	lo0.0	128.216.194.105:0	

Ok

Troubleshooting VPLS Services

From the **Execute OP Scripts Job Status** dialog box, you can check status of the interfaces, LDP sessions, neighbor links, connection instances, and endpoints of a VPLS service. To select the status you want to check, click on the device from the device list on the left, and select the show command from the **Command** list. This figure shows the troubleshooting script results for the selected device in the VPLS service.

Execute OP Scripts Job Status

Device Name	Interface	Script Name	Script Version	Device Name	Status
960R1_EP_Alok_re	ge-0/0/3.1357	VPLSPredefinedScript...	1	960R1_EP_Alok_re	Success
960R1_EP_Alok_re	ge-0/0/4.1357				
960R2_EP_Alok_re	ge-0/0/2.1357				

Job Results for VPLSPredefinedScript.slax

Script execution output details:

VPLS Connection Information		
Connection ID	Connection Type	Connection Status
128.216.194.110(vpls-id 2147467264	rmt	Up

Interface Information	
Admin	Link
up	up

Interface Information Statistics	
Input Packets	Output Packets
0	0

Ok

Troubleshooting L3VPN Services

From the **Execute OP Scripts Job Status** dialog box, you can check status of the interfaces, LDP sessions, neighbor links, and endpoints of a L3VPN service. To select the status you want to check, click on the device from the device list on the left, and select the show command from the **Command** list. This figure shows the troubleshooting script results for the selected device in the L3VPN service.

Execute OP Scripts Job Status

Device Name	Interface	Script Name	Script Version	Device Name	Status
480R3_EP_Alok_re	ge-0/0/2.1	L3VPNPredefinedScript...	1	480R3_EP_Alok_re	Success
480R4_EP_Alok_re	ge-0/0/3.1				

Job Results for L3VPNPredefinedScript.slax

Script execution output details:

Route table Information				
Destination	Protocol	Preference	Age	Via
10.0.88.0/30	Direct	0	01:38:09	ge-0/0/2.1
10.0.88.1/32	Local	0	01:38:09	
10.0.99.0/30	BGP	170	00:58:05	xe-0/2/1.0
224.0.0.5/32	OSPF	10	01:38:10	

BGP Information					
Table Name	Total Paths	Act Paths	Suppressed	History Damp	Pending
Irrelevant-service.inet.0	1	1	0	0	0
Irrelevant-service.mdt.0	0	0	0	0	0

Interface Information	
Admin	Link
up	up

Interface Information Statistics	
Input Packets	Output Packets
0	0

Ok

Related Documentation

- [Performing a Functional Audit on page 1067](#)
- [Performing a Configuration Audit on page 1077](#)
- [Troubleshooting N-PE Devices Before Provisioning a Service on page 1080](#)

- [Modifying the Application Settings of Connectivity Services Director on page 1082](#)
- [Viewing Configuration Audit Results on page 1098](#)
- [Viewing Functional Audit Results on page 1102](#)
- [Viewing Functional Audit Results for an Inverse Multiplexing for ATM Service on page 1106](#)

Basic Requirements of Operational Scripts

For operational (op) scripts, the context is a required argument because a context is transmitted to the script, when the script is run from troubleshooting operation. The format of the argument to be pushed to the script is as follows:

```
var $arguments = {
  <argument> {
    <name> "CONTEXT";
    <description> "The CONTEXT.";
  }
}
var $CONTEXT;
```

The context has parameters based on the service type, which needs to be parsed to use the parameters.

The following is an example of a P2P LDP service context:

Context:

```
/device[name="deviceName"]/configuration/protocols/l2circuit/neighbor[name="neighbor IP"]/interface[name="interfaceName.unitID"]
```

The code in op script to parse the context is as follows:

```
var $tempContext = str:replace(str:replace($CONTEXT, "/device[name=\"", ""),
  "\"]/configuration/protocols/l2circuit/neighbor[name=\"", "|");
var $finalContext = str:replace(str:replace($tempContext,
  "\"]/interface[name=\"", "|"), "\"", "");
var $variables = jcs:split( "\\|", $finalContext );
var $deviceName = $variables[1];
var $neighborIp = $variables[2];
var $interfaceName = $variables[3];
```

The following is an example of a P2P BGP service context:

```
Context: /device[name="device
name"]/configuration/routing-instances/instance[name="Service name" and
instance-type="l2vpn"]/bgp/interface[name="interfaceName.unitID"]
```

The code in op script to parse the context is as follows:

```

var $tempContext1 = str:replace(str:replace($CONTEXT, "/device[name=\"", ""),
"\"]/configuration/routing-instances/instance[name=\"", "|");
var $tempContext2 = str:replace($tempContext1, "\" and
instance-type=\"l2vpn\"", "");
var $finalContext = str:replace(str:replace($tempContext2,
"/bgp/interface[name=\"", "|"), "\"\"", "");
var $variables = jcs:split( "\\|", $finalContext );
var $deviceName = $variables[1];
var $instanceName = $variables[2];
var $interfaceName = $variables[3];

```

The following is an example of a P2P VPLS service context:

Context: /device[name="device
name"]/configuration/routing-instances/instance[name="Service name" and
instance-type="vpls"]/vpls/interface[name="interfaceName.unitID"]

The code in op script to parse the context is as follows:

```

var $tempContext1 = str:replace(str:replace($CONTEXT, "/device[name=\"", ""),
"\"]/configuration/routing-instances/instance[name=\"", "|");
var $tempContext2 = str:replace($tempContext1, "\" and instance-type=\"vpls\"",
""");
var $finalContext = str:replace(str:replace($tempContext2,
"/vpls/interface[name=\"", "|"), "\"\"", "");
var $variables = jcs:split( "\\|", $finalContext );
var $deviceName = $variables[1];
var $instanceName = $variables[2];
var $interfaceName = $variables[3];

```

The following is an example of a P2P L3VPN service context:

Context: /device[name="device
name"]/configuration/routing-instances/instance[name="Service name" and
instance-type="vrf"]/vrf/interface[name="interfaceName.unitID"]

The code in op script to parse the context:

```

var $tempContext1 = str:replace(str:replace($CONTEXT, "/device[name=\"", ""),
"\"]/configuration/routing-instances/instance[name=\"", "|");
var $tempContext2 = str:replace($tempContext1, "\" and instance-type=\"vrf\"",
""");
var $finalContext = str:replace(str:replace($tempContext2,
"/vrf/interface[name=\"", "|"), "\"\"", "");
var $variables = jcs:split( "\\|", $finalContext );
var $deviceName = $variables[1];
var $instanceName = $variables[2];
var $interfaceName = $variables[3];

```


Predefined Scripts for Troubleshooting

Predefined troubleshooting scripts are included by default, during the installation of Connectivity Services Director. The following are the script names for each service and the commands supported for them.

P2P LDP Service

P2PLDPPredefinedScript.slax is the predefined script that is uploaded.

The following are the supported commands:

- get-l2ckt-connection-information
- get-interface-information
- get-ldp-session-information
- get-ldp-neighbor-information

P2P BGP Service

P2PBGPPredefinedScript.slax is the predefined script that is uploaded.

The following are the supported commands:

- get-l2vpn-connection-information
- get-interface-information
- get-bgp-summary-information
- get-interface-statistics

VPLS Service

VPLSPredefinedScript.slax is the predefined script that is uploaded.

The following are the supported commands:

- get-vpls-connection-information
- get-interface-information
- get-interface-statistics

L3VPN Service

L3VPNPredefinedScript.slax is the predefined script that is uploaded.

The following are the supported commands:

- get-vrrp-connection-information
- get-interface-information
- get-interface-statistics

RSVP LSP Service

RSVPLSPPredefinedScript.slax is the predefined script that is uploaded.

The following are the supported commands:

- get-mpls-connection-information
- get-mpls-lsp-information

Related Documentation

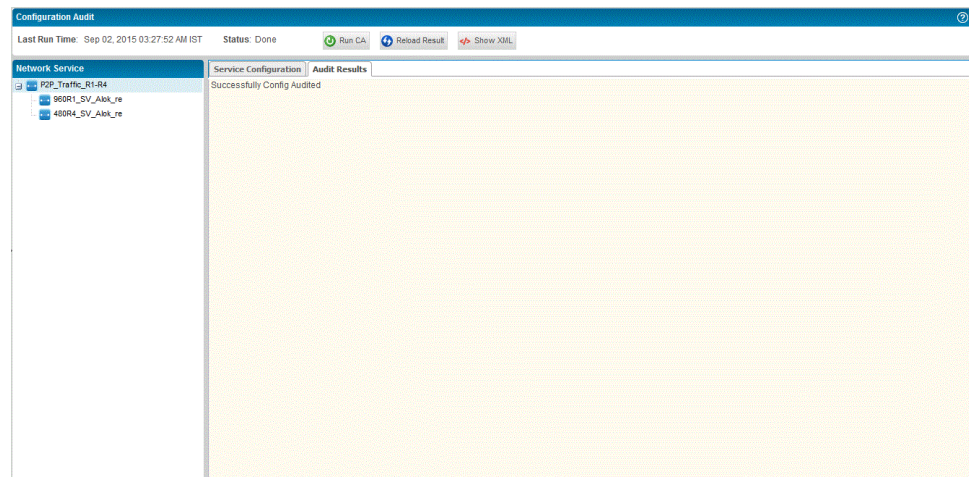
- [Troubleshooting the Endpoints of Services on page 1088](#)

Viewing Configuration Audit Results

After performing a configuration audit, check the detailed results of the audit:

1. a. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
- b. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
- c. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
- d. In the **Network Services > Connectivity** task pane, select **Service Provisioning > Audit/Results > Configuration Audit**.

The configuration audit results are displayed if an audit operation was previously performed on the selected service.



Examine the audit results for missing configuration information, and keep the window open for later comparison with the service configuration in the Junos Space database.

You can validate policies for the hub and spoke (1 interface).



NOTE: In the Service Configuration tab of the Configuration Audit dialog box, you can observe several lines with the delete statement in the service settings. These delete statements indicate the policy attributes that are deleted from the corresponding service on a device. Whenever a service is created or modified, the policy options are always deleted from the device to prevent the previously existing policies from interfering with the service. The presence of the delete statements is an expected behavior and does not indicate any incorrect service configuration.

2. To view the service configuration in the Junos Space database, in Deploy mode, from the **Network Services > Connectivity** task pane, select **Service Provisioning > Deploy Services**. The Manage Service Deployment page is displayed on the bottom part of the right pane. Select a service from the **Manage Service Deployment** page, then in the **Actions** menu, select **View Service Configuration**.

A new window opens and shows the service configuration.

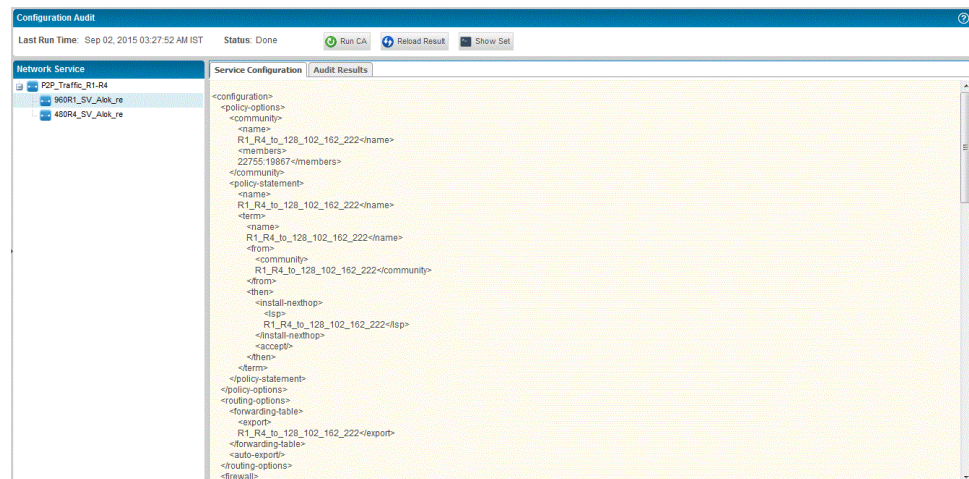
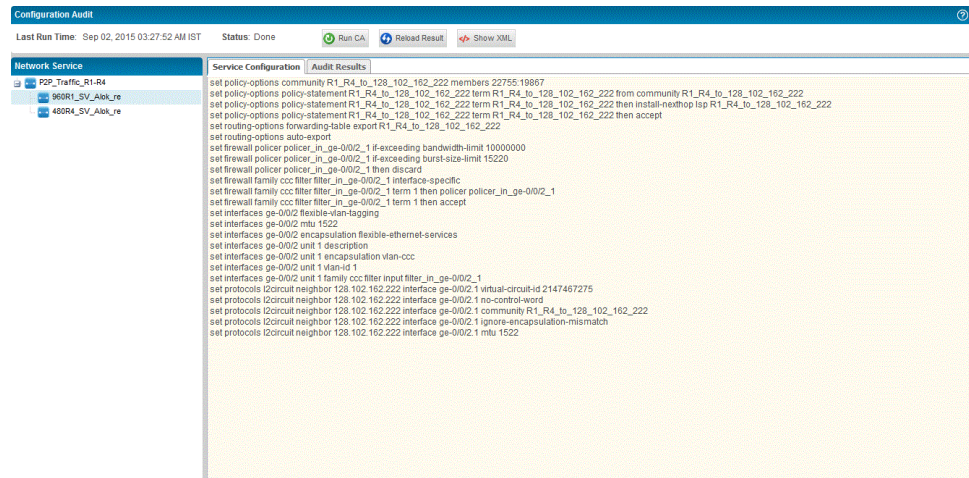
If a CFM is configured in P2P service or VPLS service, the configuration audit result displays the CFM configuration details.

3. Compare the contents of the Service Configuration with those of the **Configuration Audit Results** window for each device in turn. If you see discrepancies, then it is likely that the service configuration was modified out-of-band. If so, you might need to synchronize the device with the Junos Space database.

For step-by-step instructions about synchronizing devices, see *Resynchronizing Managed Devices with the Network* for details.

After the audit job is completed, you can view the output of the operation in the Configuration Audit Results window that is displayed on the right pane. The left pane displays a tree of devices associated with the specified service. You can select a **Service-name > Interface-name Device-name** in the left pane of the window. The attribute definitions and parameters defined in the service are displayed in the right pane. The right pane contains three tabs— Service Configuration, Template Configuration, and Audit Results. The Service Configuration tab displays the settings specified for the service on the device in CLI format. This tab displays the elements or components specified for a service template in the form of configuration stanzas and hierarchy levels. This display is similar to the **show** command that you can use at a certain **[edit]** hierarchy level to view the defined settings. The Template Configuration tab displays the service attributes and options defined in the service template, if any, that is associated with the service. The Audit Results tab displays the status of the audit job that was run, such as whether the job succeeded or failed. You can also view the service definition and associated template details under the Service Config and Template Config tabs in Junos OS XML API format, instead of the CLI format.

Click the **Show XML Config** button at the top-right corner of the window to view the audit results in XML API format. Alternatively, click the **Show Set** button to view the audit results in the manner in which they are displayed in the Junos OS CLI interface. The **Show XML/Set** button is a toggle button.



The Junos OS command-line interface (CLI) and the Junos OS infrastructure communicate using XML. When you issue an operational mode command in the CLI, the CLI converts the command into XML format for processing. After processing, Junos OS returns the output in the form of an XML document, which the CLI converts back into a readable format for display. Remote client applications also use XML-based data encoding for operational and configuration requests on devices running Junos OS. The Junos XML API is an XML representation of Junos configuration statements and operational mode commands. It defines an XML equivalent for all statements in the Junos configuration hierarchy and many of the commands that you issue in CLI operational mode. Each operational mode command with a Junos XML counterpart maps to a request tag element and, if necessary, a response tag element.

Click **Reload Result** at the top-right corner of the window to refresh and display the results of the audit. When you click this button, only the output of the audit operation is displayed

afresh and the audit job is not run again. You can refresh the results only for completed audit instances. When you select **Service-name** in the left pane of the window, service status information is displayed in the right pane. Click **Run Configuration Audit** after selecting the services you need to run the audit job again.

Configuration audit can be run for multiple services from Build mode of Service View of the Connectivity Services Director GUI. From the Manage Network Services page, select the check boxes beside multiple services, click the **Audit** button at the top of the table of configured services, and select **Run Configuration Audit** from the drop-down menu.

We recommend that you configure a script as a local script for effective and optimal debugging and analysis of the configuration settings contained in the script. The main advantage of a local script is that you need not download the script to a device (because a connection is established with the device by the GUI application and the script is run) and you need not remove the script from a device after you decommission a service.

- Related Documentation**
- [Viewing Functional Audit Results on page 1102](#)
 - [Performing a Functional Audit on page 1067](#)
 - [Performing a Configuration Audit on page 1077](#)

Viewing Functional Audit Results

To view the results of a functional audit of a service, follow this procedure:

After performing a functional audit on a service (see [“Performing a Functional Audit” on page 1067](#)), look at the functional audit results:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
4. In the **Network Services > Connectivity** task pane, select **Service Provisioning > Audit/Results > Functional Audit**.

The **Functional Audit Result** window appears, displaying Service Status in the right panel.

If a CFM is configured in a P2P service or VPLS service, the functional audit results includes the result of both P2P and VPLS services.





A green up-arrow in the Service Status header bar indicates that the service has passed the functional audit in both the control plane and the data plane. A red down-arrow indicates that the service failed either or both the control plane validation and the data plane validation.

Depending on the type of service, the left panel lists

- The name of the service
- Each endpoint in the service

Icons representing the endpoint indicate its role in the service and its up or down state. [Table 136 on page 1103](#) describes these icons for a point-to-multipoint service.

Table 136: Point-to-Multipoint Service Endpoint Icons

Icon	Meaning
	Hub in a point-to-multipoint service. Endpoint state is up.
	Hub in a point-to-multipoint service. Endpoint state is down.
	Spoke in a point-to-multipoint service. Endpoint state is up.
	Spoke in a point-to-multipoint service. Endpoint state is down.

- Interface name
 - A numeric value indicating the subinterface name: the VLAN-ID for an 802.1Q interface, the service VLAN-ID for a Q-in-Q interface, or 0 for a dedicated port.
 - Device name
- To show all endpoints in the service, in the left panel header, select **All**. To display only the endpoints indicating failed validation, select **Failed**. Failed is dimmed if the functional audit returned no validation errors.
 - To view details for an individual interface or endpoint, select it in the left panel. The header bar on the right panel changes to End Point or Interface Status, and details for the selected item are displayed below.

- Expand each device to show the link from that device to the other N-PE device in the service.

An icon next to each link indicates whether the functional audit commands reported correct functioning of the control plane and data plane. [Table 137 on page 1103](#) describes these icons.

Table 137: Functional Audit Success Status Icons



Icon	Meaning
	Control plane and data plane function correctly.

Table 137: Functional Audit Success Status Icons (continued)

Icon	Meaning
	Errors were reported in the functioning of either the control plane or the data plane.

8. In the left panel, select a link.

The panel to the right shows the validation results for the control plane validation and data plane validation for the selected link. Icons indicate the success or failure of each set of tests.

The panel to the right shows the validation results for the control plane validation and data plane validation for the selected link. Icons indicate the success or failure of each of these sets of tests. [Table 138 on page 1104](#) describes icons and the textual information provided in the box beside the icon.

Table 138: Multipoint-to-Multipoint Service Control Plane and Data Plane Validation Icons





Icon	Meaning	Explanation
	Control plane up	The text box shows the name of the remote N-PE device and confirms that the data plane is operational.
	Control plane down	The text box shows the name of the configured remote N-PE device and, in the Command status field, explains why the test failed.
	Control plane status unknown	The text box indicates the name of the configured remote N-PE device and, in the Result field, an explanation as to why the functional audit operation was unable to test the control plane—for example, configuration was missing on the device.
	Data plane up	The text box indicates the number of packets transmitted and received, and confirms that no data packets were lost during the audit.
	Data plane down	The text box indicates that data packets were lost during the audit.

Table 138: Multipoint-to-Multipoint Service Control Plane and Data Plane Validation Icons (continued)



Icon	Meaning	Explanation
	Data plane status unknown	The functional audit was unable to complete the data plane test. The Result field in the text box indicates the reason—for example, the platform does not support data plane testing, or the connection to the remote N-PE device is down.

The control plane and data plane validation checks must both show operational status for the link to be considered operational.

- To troubleshoot a service, click the **Troubleshoot** button. To select the status you want to check, click the device from the device list on the left, and select the show command from the **Command** list.

An icon next to each command indicates whether the command execution is successful or failed. [Table 139 on page 1105](#) describes these icons.

Table 139: Command Status Icons

Icon	Meaning
	Command execution is successful and the command status is up.
	<ul style="list-style-type: none"> Command execution is failed, or, In case of multiple rows, one of the status value is down



NOTE:

- Data plane information between two endpoints in a VPLS service is provided only for MX Series devices. This information is not provided for M Series devices.
- Junos OS Release 9.3 and Junos OS Release 9.4 do not support data plane validation. The Functional Audit Results screens do not display data plane validation information if any device in the service is running one of these Junos OS releases.

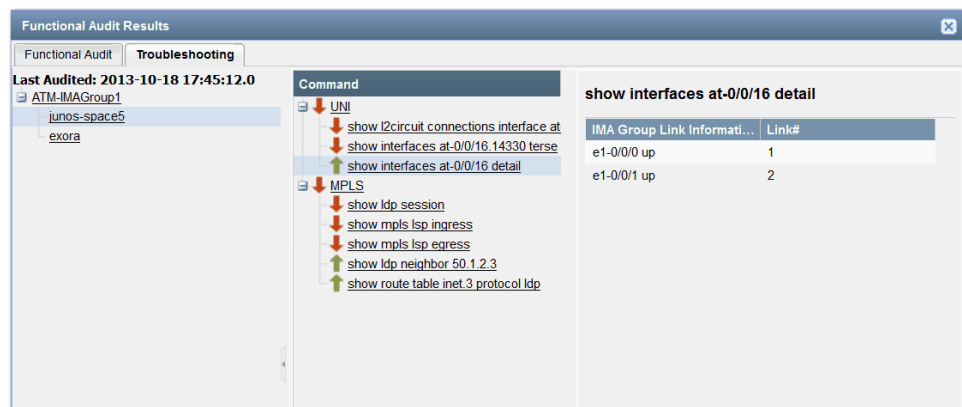
Related Documentation

- [Viewing Configuration Audit Results on page 1098](#)
- [Performing a Functional Audit on page 1067](#)
- [Performing a Configuration Audit on page 1077](#)

Viewing Functional Audit Results for an Inverse Multiplexing for ATM Service

To view functional audit results for an Inverse Multiplexing for ATM Service:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. In the **Network Services > Connectivity** task pane, select **Service Provisioning > Manage Services**.
4. In the **Manage Services** screen, select the service for which you want to view the functional audit results.
5. Right-click the service, or click the **Audit/Results** menu, and select **View Functional Audit Results**.
6. In the **Functional Audit Results** window, click the **Troubleshoot** button.



In the **Troubleshooting** tab, when you select a **show interfaces** command for a UNI interface that is configured as an IMA Group Link, the command displays details for the IMA group interface.

Related Documentation

- [Viewing Configuration Audit Results on page 1098](#)
- [Viewing Functional Audit Results on page 1102](#)
- [Performing a Functional Audit on page 1067](#)
- [Performing a Configuration Audit on page 1077](#)

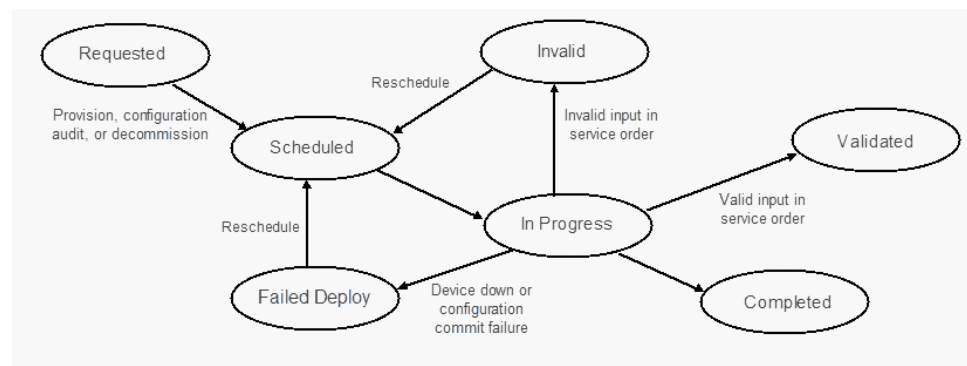
Modifying a Saved Service Order

Before a service order can affect a service, it must transition through the following states:

- **Requested**—When the service provisioner has created the service order, but has not yet attempted to deploy it or schedule it for deployment, the service order is in the Requested state.
- **Scheduled**—After the service provisioner has scheduled the service order for deployment, the service order transitions to the Scheduled state.
- **In Progress**—When a scheduled service order reaches its time for deployment, it transitions to the transitory In Progress state. From this state, the Junos Space software attempts to deploy the service.
- **Validated**—When all the information in the service order is successfully validated, the service order transitions to the Validated state.
- **Completed**—Successful deployment transitions the service order to the Completed state.
- **Invalid**—If the Junos Space software cannot deploy the service because of invalid information in the service order itself, the service order enters the Invalid state. The service provisioner must resolve the issues that cause the failure before re-creating the service order and rescheduling it for deployment.
- **Failed Deploy**—If the device is down or the Junos Space software is unable to push the service configuration to the device, the service order transitions to the Failed Deploy state.
- **Deactivated**—When you disable a service order, the configuration attributes associated with such a service order are deactivated and commented out in the device settings. By disabling a service, the traffic processing for the traversed packets is impacted. In certain network topologies, you might require a service-related settings to be disabled for a certain period to perform troubleshooting or modification to the traffic-handling method, and you might want to reactivate a disabled service later when you have completed network maintenance and analysis work. In such a case, it might be beneficial to use the deactivation functionality for a service order. The deactivated service is propagated to the devices associated with the service order. To disable a service, the service must not contain any pending or uncommitted changes. Also, the service must be in the Deployed or Re-Activated state.
- **Reactivated**—After you disable a service order to deactivate the configuration settings on devices mapped to the service, you might require the service settings to be reenabled after you have modified the service parameters, either directly on the device or using the Connectivity Services Director application. In such a case, you can use the reactivation functionality to revive and activate the service properties on devices. To disable a service, the service must not contain any pending or uncommitted changes. Also, the service must be in the Deactivated state.

Figure 51 on page 1108 illustrates the service order states.

Figure 51: Service Order States



To view the state of a service order, in Deploy mode, select **Network Services > Connectivity** from the View pane and drill down to the type of service for which you want to modify a service order, and select **Service Provisioning > Deploy Services** from the task pane. The Manage Service Deployment inventory page lists the service orders and their state.

The Junos Space Connectivity Services Director application provides the flexibility to modify an existing service order. You can modify a service order when the order state is Requested, Validated, or Invalid. You cannot modify a service order when the order state is Scheduled, Completed, or Failed Deploy.

To modify a service order:

1. In Deploy mode, select **Network Services > Connectivity** from the View pane and drill down to the type of service for which you want to modify a service order, and select **Service Provisioning > Deploy Services** from the task pane.
2. From the Manage Service Deployment page, select an existing service order, and then click **Modify**.

The Modify Service Order window appears.



NOTE: The modify option is unavailable if the service order is in Scheduled, or Completed, or Failed Deployed state.

3. Modify the fields as needed.



NOTE: When you modify a service or a service order, the read-only fields in the different pages of the wizard for service or service order modification are grayed out to indicate that you cannot modify those attributes.

The following table lists the fields that you can modify in a point-to-point service order, VPLS service order, and Layer 3 VPN service order.

Point-to-Point Service Order	VPLS Service Order	Layer 3 VPN Service Order
Name	Name	Name
Customer	Customer	Customer
Comments	Comments	Comments
VLAN ID	VLAN ID	VLAN ID
VCID	Inner VLAN ID	Route Target
CFM	VLAN Tag to stack	Hub Route Target
PE device	PE device	Spoke Route Target
UNI interface	UNI interface	UNI Interface
UNI description	UNI description	Route Distinguisher
MTU (Bytes)	MTU	Hub Route Distinguisher
Bandwidth	Bandwidth	Spoke Route Distinguisher
RSVP LSP name	Enable P2P-Spoke	Autopick Interface IP Address
PW backup settings	Ethernet Option in case of Asymmetric	VRF Table label
VPI	Neighbor Hub	Export Direct Routes
VCI	Backup NeighborHub	AS override
Outgoing label	Hub	Hub
-	Customer VLAN Range Start	Maximum prefixes
-	Customer VLAN Range End	IP address pool NOTE: While modifying a Layer 3 VPN service order, you must select the IP address pool.
-	MAC learning	Peer AS
-	Interface MAC limit	-
-	MAC statistics	-

Point-to-Point Service Order	VPLS Service Order	Layer 3 VPN Service Order
-	MAC table size	-
-	Disable tunnel services	-
-	Disable local switching	-
-	Fast reroute priority	-
-	Label block size	-
-	Connectivity type	-



NOTE: You can also change a local switching service order to a normal point-to-point service order.

4. Click **Save**.

The service order is modified. You can now deploy the service order with modified parameters to the device.

Related Documentation

- [Creating a Point-to-Point ATM or TDM Pseudowire Service Order on page 816](#)
- [Creating a Point-to-Point Service Order on page 829](#)
- [Creating a Multipoint-to-Multipoint VPLS Service Order on page 881](#)
- [Creating a Point-to-Multipoint VPLS Service Order on page 905](#)
- [Creating a Full Mesh Layer 3 VPN Ethernet Service Order on page 941](#)
- [Creating a Hub-and-Spoke Layer 3 VPN Service Order on page 964](#)

Viewing Service-Level Alarms

The Junos Space Network Application Platform has integrated a third party tool, OpenNMS, to provide network monitoring capabilities. The OpenNMS network management application platform provides solutions for enterprises and carriers. OpenNMS is installed as part of Platform, which exposes some of OpenNMS' functionality through the Network Monitoring workspace. The default performance management configuration of OpenNMS for Space supports generic counters, CPU, memory, temperature, and Mobility counters. For information on this default configuration, see the subset of the OpenNMS documentation included in this Junos Space Network Application Platform User Guide.



CAUTION: Although additional OpenNMS functionality can be accessed by customizing its XML files, editing these files can affect the functionality of the Network Monitoring workspace. Juniper Networks does not support changes to OpenNMS.

When certain types of events are persistent, or when the condition causing the event crosses a threshold, SNMP sends a notification, also called a trap to Connectivity Services Director. Connectivity Services Director correlates traps, describing a condition, into an alarm. SNMP also plays another role in Connectivity Services Director. Enabling devices for SNMP with the appropriate read-only V1/V2/V3 credentials, can speed up device discovery.

To access the alarms page for a particular service:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
3. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
4. From the task pane, select **Service Provisioning > Deploy Services**. The top part of the right pane displays the Manage Network Services page, with the table of services, and the bottom part of the right pane displays the Manage Service Deployment page, with the table of service orders.
5. From the Manage Network Services page, select the check box next to the service for which you want to view alarms.



TIP: In Build mode of Service View, from the View pane, if you select the Network Services node and do not expand the Network Services > Connectivity tree, the top pane displays a pie chart that enables you to view and examine the different services configured for devices, and the types of service protocols configured. The Services by Type graph displays the count of services for each type of service definition. Mouse over each segment of the pie to view the number corresponding to the percentage of service orders for each of the charts. This chart provides a visual overview of customers and service orders on your network, and enables you to quickly access related and commonly needed information. For

example, you can check for failed service orders and then access a list of failed requests so you can begin to take restoration measure.

.....

The top pane displays information about the services that have been previously created, such as the name of the service, the functional audit status, the performance management status, and the status of the service. You can modify the properties of the service, conduct a functional or configuration audit, force-deploy or deactivate the service, and view alarms associated with a particular service order for debugging and corrective action. Services can be in one of the following service states:

- **Completed**—The service order has been successfully deployed.
 - **Scheduled for deployment**—The service provisioner has scheduled the service order for deployment.
 - **Deployment Failed**—An attempted service deployment was not successfully completed or failed an audit.
 - **In Progress**—The Connectivity Services Director application is in the process of deploying the service.
 - **Requested**—The service provisioner has created the service order, but has not yet attempted to deploy it or schedule it for deployment.
 - **Invalid**—The service order is not valid.
6. Click the **View Alarms** button. You are navigated to the Alarms page in Fault mode. See [“Alarm Detail Monitor \(Service View\)” on page 1280](#) for more information.

**Related
Documentation**

- [Managing Jobs on page 118](#)
- [Deleting a Partial Configuration of an LSP Service Order on page 1014](#)
- [Deleting a Service Order on page 1015](#)
- [Deploying a Service on page 1016](#)
- [Validating the Pending Configuration of a Service Order on page 1018](#)
- [Viewing the Configuration of a Pending Service Order on page 1020](#)
- [SNMP MIBs and Traps Reference](#)
- [Junos Space Network Monitoring Reference](#)

Troubleshooting Devices and Services

- [Performance Management Overview on page 1113](#)
- [Monitoring Performance Management Statistics on page 1115](#)
- [Viewing Performance Management Statistics on page 1121](#)
- [Service Troubleshooting Overview on page 1129](#)

Performance Management Overview

In performance management (PM), the Connectivity Services Director application provides an option to measure the frame delay, frame loss, frame delay variation, and service availability. These measurements are achieved in either of the following ways:

- Triggering a one-way delay
- Triggering a two-way delay
- Loss

The performance measurement is useful for generating periodic service level agreement conformance reports from the deployed network and for studying traffic patterns in the network over a period of time. The iterator profiles are configured on remote MEP for measurement of frame delay (ETH-DM), frame loss (ETH-LM) and statistical frame loss (SFL).

Monitoring Performance Statistics

The PM statistics can be collected in the following two ways:

1. On-Demand Mode
2. Proactive Mode



NOTE: The Connectivity Services Director application supports only the on-demand mode.

On-Demand Mode

In on-demand mode, you can trigger the measurements. You can also collect loss measurement (ETH-LM) and delay measurements (ETH-DM).

Loss Measurement

The frame loss is calculated by collecting the counter values applicable for ingress and egress service frames. The counters maintain a count of transmitted and received data frames between a pair of MEPs. The loss measurement statistics are retrieved as the output of the **monitor ethernet loss-measurement** command and are also stored at the initiator. The frame counts are stored at both the initiator and the receiver MEPs for later retrieval.

The on-demand loss measurement statistics is collected for point-to-point service only. There are two linear charts: Near-End-CIR and Far-End-CIR. For each interval, the graph plots three values: Average case, best case, and worst case frame loss.

Delay Measurement

To start an ethernet frame delay measurement session, the router initiates an exchange of frames carrying one-way or two-way frame delay measurement protocol data units (PDUs) between the local and remote MEPs. Ethernet frame delay measurement statistics are measured and stored at only one of the MEPs.

For one-way ethernet frame delay measurement, only the receiver MEP (on the remote system) collects statistics. For two-way Ethernet frame delay measurement, only the initiator MEP (on the local system) collects statistics.

The on-demand delay measurement statistics are collected for point-to-point and VPLS services. Either the one-way or two-way delay measurements statistics are collected for the services at a given point of time. For each interval, the graph plots three value: Average delay, best case delay and worst case delay.

Proactive Mode

In this mode SLA measurements are triggered by an iterator application. The proactive performance monitoring is supported only on VPWS and VPLS.

Performance Management of Test Traffic

The Connectivity Services Director application enables you to create Threshold Crossing Alert (TCA) Profiles to apply service level agreement (SLA) parameters to test traffic as defined by the following standards:

- L2 Ethernet OAM/ ITU-T Y.1731
- RFC2544

Specifically, the parameters are:

- Bandwidth Utilization
- Delay

- Delay Variation—Jitter
- Frame Loss
- Throughput

See [Creating a TCA Profile](#).

**Related
Documentation**

- [Monitoring Performance Management Statistics on page 1115](#)
- [Viewing Performance Management Statistics on page 1121](#)
- [Service Troubleshooting Overview on page 1129](#)
- [Performing a Configuration Audit on page 1077](#)

Monitoring Performance Management Statistics

The following topics show how to monitor the performance statistics for point-to-point and VPLS services:

You can employ the ITU-T Y.1731 standard-compliant Ethernet loss measurement (ETH-LM), Ethernet synthetic loss measurement (ETH-SLM), and Ethernet delay measurement (ETH-DM) capabilities to analyze and examine the operating efficiency and performance status. These performance monitoring functionalities can be run for P2P and VPLS services. You can start and stop the collection of performance monitoring (PM) statistics on the services that you want to monitor. The retrieval and computation of statistical details is performed using SNMP MIBs.

A predefined event script, Y1731_PM.slax, is available on the Scripts page of the Junos Space Platform GUI, which displays all the scripts imported into the Junos Space Platform database (accessible by selecting **Network management platform > Images and scripts > Scripts**). This script needs to be downloaded on devices. Whenever you trigger the PM mechanism from the Connectivity Services Director GUI, an event is initiated, which in turn causes the SLAX script to be run. The event continues to run the script until the event is stopped. The event runs the script at intervals of 5 minutes. The monitoring framework is used to consolidate and display the retrieved counters and values. You can start the PM collection utility only on one pair of devices at a time. You cannot start the PM collection functionality on multiple pairs of devices simultaneously.



NOTE: Although you can start or stop the collection of PM statistics without a predefined event script made available on the corresponding devices by selecting PM Statistics > Start or Stop from the Tasks pane in Monitor mode of Service view (no error is displayed and the start or stop of PM statistics collection is successful), you must ensure that the event script is present on the devices before you trigger the mechanism for collection of PM statistics. Otherwise, although the operation does not display an error in the GUI, no backend processing occurs.

- [Monitoring Statistics for a Point-to-Point Service on page 1116](#)
- [Monitoring Statistics for a VPLS Service on page 1118](#)

Monitoring Statistics for a Point-to-Point Service

You can start a performance monitoring operation on a service to diagnose the working efficiency and operating quality from the Monitor mode in Service View of Connectivity Services Director.

To monitor the statistics for the point-to-point service:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Monitor** icon on the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside P2P Services to view the P2P service orders. Select the P2P service order for which you want to monitor performance statistics.

Alternatively, click the plus sign (+) beside VPLS Services to view the VPLS service orders. Select the VPLS service order for which you want to monitor performance statistics.

5. From the tasks pane, select **PM Statistics > Start**. The **Monitor Performance Statistics** window is displayed.



NOTE: If a CFM profile is not associated with the service, an informational message is displayed stating that an OAM or CFM profile must be mapped with the service.

Y1731 Start PM

Endpoint Device

Source Device: PE8_re

Destination Device: PE9_re

Parameters

Request Count: 10

delay(seconds): 1

Frame Priority(802.1p): 0

Statistics To Monitor

☒ One-Way Delay

☐ Two-Way Delay

☐ Loss

Start

Cancel



NOTE: The Start PM Statistics action is enabled only if the CFM is enabled in the selected point-to-point service. Always perform a functional audit before monitoring the statistics. The Start PM Statistics action is disabled if the functional audit status of a service is Down.

6. Fill in the fields as indicated in the table.

Field	Action
Source Device	Select a local device from the list.
Destination Device	Select a remote device from the list.
Request Count	Specify the number of frames to be sent to a specific peer MEP. Range: 1 through 65,535 frames Default: 10 frames

Field	Action
Delay (seconds)	Specify the wait interval for the frame transfer. Range: 1 through 255 seconds Default: 1 second
Frame Priority (802.1p)	Select the dot1p (IEEE 802.1p or packet classification layer 2 headers) priority of continuity-check and link-trace packet. Range: 0 through 7 Default: 0
Monitor Statistics	Select one of the following check boxes: <ul style="list-style-type: none"> • Two-Way delay • One-Way delay • Loss

7. Click **OK**.



NOTE: When you stop PM statistical collection, a popup dialog box is displayed, prompting you to confirm whether you want to stop PM statistical collection. Click **OK** to confirm the action. Click **Cancel** to discard the changes.

This action initiates a statistics collection on the endpoint device. The **View PM Statistics** action is enabled on successful initiation of the statistics.

To terminate the performance monitoring task, select **PM Statistics > Stop** from the tasks pane for the selected service.

If you are upgrading from the older version of Services Activation Director to Connectivity Services Director 1.0, you must stop any performance monitoring and restart the collection of PM statistics on the endpoints. A seamless migration of PM statistics from Services Activation Director is not supported because the mechanism used to retrieve and store the PM statistical details is different between Services Activation Director and Connectivity Services Director. While utility MIBs (OpenNMS for SNMP trap collection and correlation) and remote procedure calls (RPC) are used in Services Activation Director, only utility MIBs are used in Connectivity Services Director to collect the data. Also, event scripts are different between the two applications, which causes the object ID to be changed.

Monitoring Statistics for a VPLS Service

You can start a performance monitoring operation on a service to diagnose the working efficiency and operating quality from the Monitor mode in Service View of Connectivity Services Director.

To monitor the statistics for the VPLS Service:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Monitor** icon on the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside P2P Services to view the P2P service orders. Select the P2P service order for which you want to monitor performance statistics.

Alternatively, click the plus sign (+) beside VPLS Services to view the VPLS service orders. Select the VPLS service order for which you want to monitor performance statistics.

5. From the tasks pane, select **PM Statistics > Start**. The **Monitor Performance Statistics** window is displayed.

Y1731 Start PM

Endpoint Device

Source Device: 480R3_EP_Alok_re

Destination Device: 480R4_EP_Alok_re

Parameters

Request Count: 10

delay(seconds): 1

Frame Priority(802.1p): 0

Statistics To Monitor

☒ One-Way Delay

☒ Two-Way Delay

☒ Loss

Start Cancel



NOTE: The **Start PM Statistics** action is enabled only if the CFM is enabled in the selected VPLS service. Always perform a functional audit before monitoring the statistics. The **Start PM Statistics** action is disabled if the functional audit status of a service is Down.

6. Fill in the fields as indicated in the table.

Field	Action
Source Device	Select a local device from the list.
Destination Device	Select a remote device from the list.
Request Count	Specify the number of frames to be sent to a specific peer MEP. Range: 1 through 65,535 frames Default: 10 frames
Delay (seconds)	Specify the wait interval for the frame transfer. Range: 1 through 255 seconds Default: 1 second
Frame Priority (802.1p)	Select the 802.1p priority of continuity-check and link-trace packet. Range: 0 through 7 Default: 0
Monitor Statistics	Select Two-Way delay.

7. Click **OK**.

This action initiates a statistics collection on the endpoint device. The **View PM Statistics** action is enabled on successful initiation of the statistics.

To terminate the performance monitoring task, select **PM Statistics > Stop** from the tasks pane for the selected service.

If you are upgrading from the older version of Services Activation Director to Connectivity Services Director 1.0, you must stop any performance monitoring and restart the collection of PM statistics on the endpoints. A seamless migration of PM statistics from Services Activation Director is not supported because the mechanism used to retrieve and store the PM statistical details is different between Services Activation Director and Connectivity Services Director. While utility MIBs (OpenNMS for SNMP trap collection and correlation) and remote procedure calls (RPC) are used in Services Activation Director, only utility MIBs are used in Connectivity Services Director to collect the data. Also, event scripts are different between the two applications, which causes the object ID to be changed.

Related Documentation

- [Performance Management Overview on page 1113](#)
- [Viewing Performance Management Statistics on page 1121](#)
- [Service Troubleshooting Overview on page 1129](#)
- [Performing a Configuration Audit on page 1077](#)

Viewing Performance Management Statistics

You can employ the ITU-T Y.1731 standard-compliant Ethernet loss measurement (ETH-LM), Ethernet synthetic loss measurement (ETH-SLM), and Ethernet delay measurement (ETH-DM) capabilities to analyze and examine the operating efficiency and performance status. These performance monitoring functionalities can be run for P2P and VPLS services. You can start and stop the collection of performance monitoring (PM) statistics on the services that you want to monitor. The retrieval and computation of statistical details is performed using SNMP MIBs.

A predefined event script, PM.slax, is available, which needs to be downloaded on devices. Whenever you trigger the PM mechanism from the Connectivity Services Director GUI, an event is initiated, which in turn causes the SLAX script to be run. The event continues to run the script until the event is stopped. The event runs the script at intervals of 5 minutes. The monitoring framework is used to consolidate and display the retrieved counters and values. You can start the PM collection utility only on one pair of devices at a time. You cannot start the PM collection functionality on multiple pairs of devices simultaneously.

The following topics show how to view the performance statistics for point-to-point and VPLS services:

- [Viewing Y.1731 Performance Monitoring Statistics for Point-to-Point Services on page 1121](#)
- [Viewing Y.1731 Performance Monitoring Statistics for VPLS Services on page 1125](#)

Viewing Y.1731 Performance Monitoring Statistics for Point-to-Point Services

The Y.1731 monitoring functionality is not enabled by default. You must explicitly start the PM collection mechanism by selecting **PM Statistics > Start** from the task pane after selecting the specified service in the View pane. The graphical representation of the retrieved statistical details for the service is displayed, based on data availability. The data collected is retained after you stop the PM collection utility for future reference and correlation.

If you are upgrading from the older version of Services Activation Director to Connectivity Services Director 1.0, you must stop any performance monitoring and restart the collection of PM statistics on the endpoints.



NOTE: The refresh of values and statuses of the parameters displayed in the graphs and tables of different monitors depends on the polling interval configured under the Monitoring tab of the Preferences page (accessible by clicking the down arrow beside the System button in the Connectivity Services Director banner and selecting Preferences).

To view the statistics for the point-to-point service:

1. Select Service View from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Monitor** icon on the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside P2P Services to view the P2P service orders. Select the P2P service order for which you want to monitor performance statistics.

Alternatively, click the plus sign (+) beside VPLS Services to view the VPLS service orders. Select the VPLS service order for which you want to monitor performance statistics.

5. Select the **Service Performance** tab.



NOTE: The View PM Statistics action is enabled only after performing the Start PM Statistics.

6. View and analyze the respective graph.

The following monitors are displayed:

Connections

This monitor shows the status of connections between peer devices. In the tabular view, the row represents the source device and the columns denote the neighboring and destination devices. This monitor is applicable for P2P and VPLS services. A green up-arrow in the indicates that the adjoining device in the network path to the destination device is operationally up. A red down-arrow indicates that the device is down. For the device for which the connection status is displayed, a value of NA is displayed under its own corresponding column to denote that it is not applicable. Click Refresh at the top of the monitor to update and display the contents of the table.

From the Time Interval drop-down box, select 1 Hour, 8 Hours, 1 Day, 1 Week, 1 Month, 3 Months, 6 Months, 1 Year, or Custom to specify the duration for which the data polled from devices needs to be displayed. If you select the Custom option, the Time range popup dialog box is displayed. Specify the date from the calendar, and select the Time From (Start time in the 24-hour time format of collection of data), and Time To (End

time in the 24-hour time format of collection of data). Click OK to save the settings. Else, click Cancel to discard the configuration.

Loss Measurement

The Loss Measurement graph displays a real-time linear plot of delay value with respect to the time. The x-axis represents the time and the y-axis represents the frame loss ratio. Near-end frame loss refers to the count of frame loss associated with ingress data frames. Far-end frame loss refers to the count of frame loss associated with egress data frames. The lines represent the best case frame loss or the lowest frame loss, the worst case frame loss or the highest frame loss, and the average frame loss or the median of the highest and lowest frame losses. The frame loss is calculated by collecting the counter values applicable for ingress and egress service frames. The counters maintain a count of transmitted and received data frames between a pair of MEPs. The loss measurement statistics are retrieved as the output of the monitor ethernet loss-measurement command and are also stored at the initiator. The frame counts are stored at both the initiator and the receiver MEPs for later retrieval. The on-demand loss measurement statistics is collected for point-to-point service only. There are two linear charts: Near-End-CIR and Far-End-CIR. For each interval, the graph plots three values: Average case, best case, and worst case frame loss. From the Loss End drop-down list, select **Near-end (CIR)** to display frame loss statistics associated with ingress data frames or **Far-end (CIR)** to display frame loss statistics associated with egress data frames. Mouse over the legends to view the lines corresponding to best-case, average, and worst-case frame loss statistics.

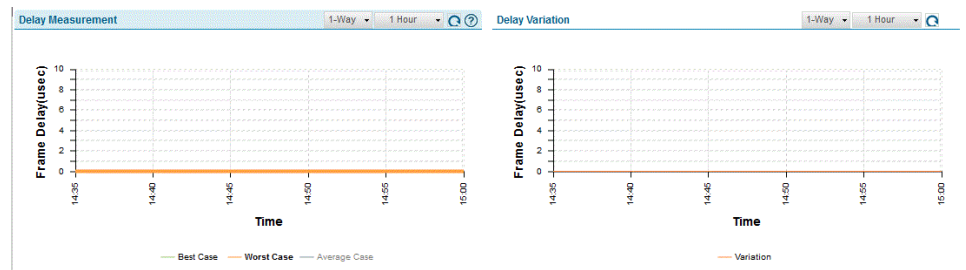
Delay Measurement

The Delay Measurement graph displays a real-time linear plot of delay value with respect to the time. The x-axis represents the time and the y-axis represents frame delay in microseconds. The legends reference average one-way delay, best-case one-way delay, and worst-case one way delay for one-way delay measurement. The green line denotes the lowest one-way frame delay for the statistics displayed, the orange line denotes the highest one-way frame delay for the statistics displayed, and the blue line denotes the average one-way frame delay for the statistics displayed. The legends reference average two-way delay, best-case two-way delay, and worst-case two-way delay for two-way delay measurement. The green line denotes the lowest two-way frame delay for the statistics displayed, the orange line denotes the highest two-way frame delay for the statistics displayed, and the blue line denotes the average two-way frame delay for the statistics displayed. From the Delay End drop-down box, select **1-Way** or **2-Way** to display the one-way or two-way frame delay measurement protocols respectively.

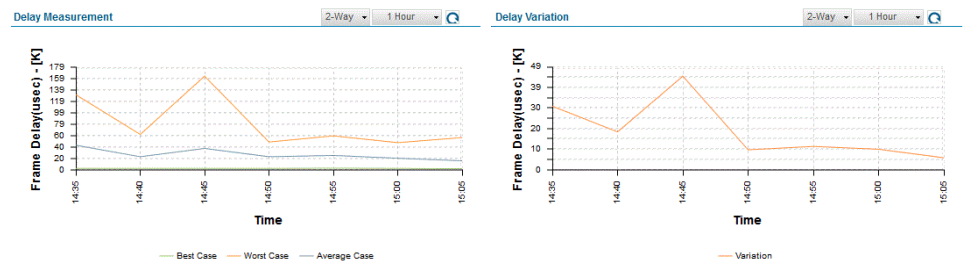
Delay Variation

The Delay Variation graph displays the difference between the consecutive frame delay values. The x-axis represents the time and the y-axis represents delay variation in microseconds. The line denotes the average one-way delay variation or the average one-way “frame jitter” for the statistics displayed for one-way frame delay measurement. The line denotes the average two-way delay variation or the average two-way “frame jitter” for the statistics displayed for two-way delay measurement.

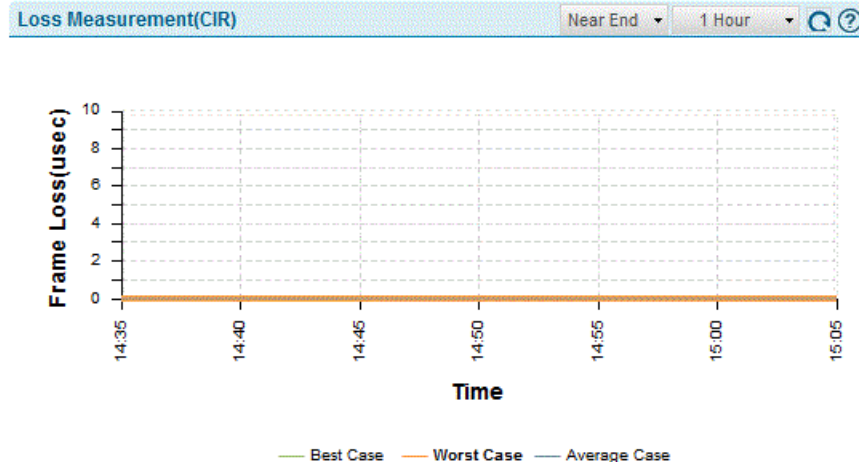
If the delay measurement is one-way, the following graph is displayed.

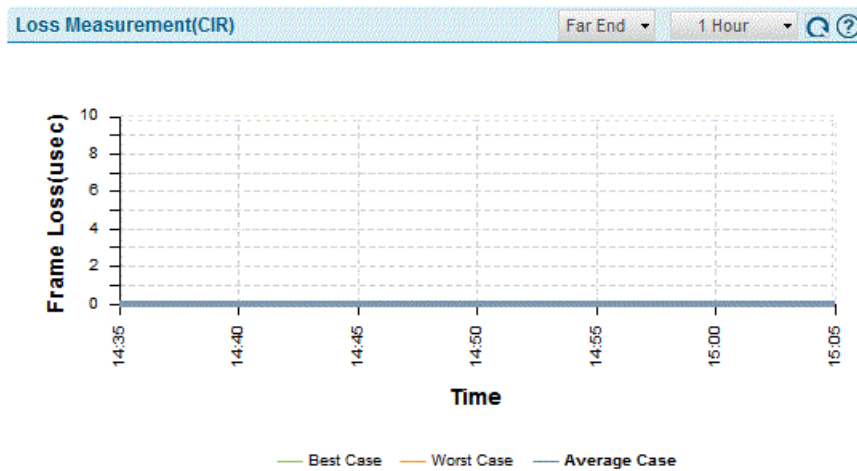


If the delay measurement is two-way, the following graph is displayed.



The Loss Measurement monitor displays two real-time linear plots: Near End (CIR) and Far End (CIR). The three parameters in each graph plot are average case, best case, and worst case of frame-loss.





The graph is plotted in real-time. By default, the total time duration is ten minutes. If the duration of statistics collection exceeds ten minutes, the graph scrolls and shows the data of latest ten minutes.

- See Also**
- [Performance Management Overview on page 1113](#)
 - [Monitoring Performance Management Statistics on page 1115](#)
 - [Viewing Performance Management Statistics on page 1121](#)
 - [Service Troubleshooting Overview on page 1129](#)
 - [Performing a Configuration Audit on page 1077](#)

Viewing Y.1731 Performance Monitoring Statistics for VPLS Services

If you are upgrading from the older version of Services Activation Director to Connectivity Services Director 1.0, you must stop any performance monitoring and restart the collection of PM statistics on the endpoints.

The Y.1731 monitoring functionality is not enabled by default. You must explicitly start the PM collection mechanism by selecting **PM Statistics > Start** from the task pane after selecting the specified service in the View pane. The graphical representation of the retrieved statistical details for the service is displayed, based on data availability. The data collected is retained after you stop the PM collection utility for future reference and correlation.



NOTE: The refresh of values and statuses of the parameters displayed in the graphs and tables of different monitors depends on the polling interval configured under the Monitoring tab of the Preferences page (accessible by clicking the down arrow beside the System button in the Connectivity Services Director banner and selecting Preferences).

To view the statistics for the VPLS service:

1. Select Service View from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Monitor** icon on the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside P2P Services to view the P2P service orders. Select the P2P service order for which you want to monitor performance statistics.

Alternatively, click the plus sign (+) beside VPLS Services to view the VPLS service orders. Select the VPLS service order for which you want to monitor performance statistics.

5. Select the **Service Performance** tab.



NOTE: The View PM Statistics action is enabled only after performing the Start PM Statistics.

View and analyze the graphs.

The following monitors are displayed:

Connections

This monitor shows the status of connections between peer devices. In the tabular view, the row represents the source device and the columns denote the neighboring and destination devices. This monitor is applicable for P2P and VPLS services. A green up-arrow in the indicates that the adjoining device in the network path to the destination device is operationally up. A red down-arrow indicates that the device is down. For the device for which the connection status is displayed, a value of NA is displayed under its own corresponding column to denote that it is not applicable. Click Refresh at the top of the monitor to update and display the contents of the table.

From the Time Interval drop-down box, select 1 Hour, 8 Hours, 1 Day, 1 Week, 1 Month, 3 Months, 6 Months, 1 Year, or Custom to specify the duration for which the data polled from devices needs to be displayed. If you select the Custom option, the Time range popup dialog box is displayed. Specify the date from the calendar, and select the Time From (Start time in the 24-hour time format of collection of data), and Time To (End time in the 24-hour time format of collection of data). Click OK to save the settings. Else, click Cancel to discard the configuration.

Loss Measurement

The Loss Measurement graph displays a real-time linear plot of delay value with respect to the time. The x-axis represents the time and the y-axis represents the frame loss ratio. Near-end frame loss refers to the count of frame loss associated with ingress data frames. Far-end frame loss refers to the count of frame loss associated with

egress data frames. The lines represent the best case frame loss or the lowest frame loss, the worst case frame loss or the highest frame loss, and the average frame loss or the median of the highest and lowest frame losses. The frame loss is calculated by collecting the counter values applicable for ingress and egress service frames. The counters maintain a count of transmitted and received data frames between a pair of MEPs. The loss measurement statistics are retrieved as the output of the monitor ethernet loss-measurement command and are also stored at the initiator. The frame counts are stored at both the initiator and the receiver MEPs for later retrieval. The on-demand loss measurement statistics is collected for point-to-point service only. There are two linear charts: Near-End-CIR and Far-End-CIR. For each interval, the graph plots three values: Average case, best case, and worst case frame loss. From the Loss End drop-down list, select **Near-end (CIR)** to display frame loss statistics associated with ingress data frames or **Far-end (CIR)** to display frame loss statistics associated with egress data frames. Mouse over the legends to view the lines corresponding to best-case, average, and worst-case frame loss statistics.

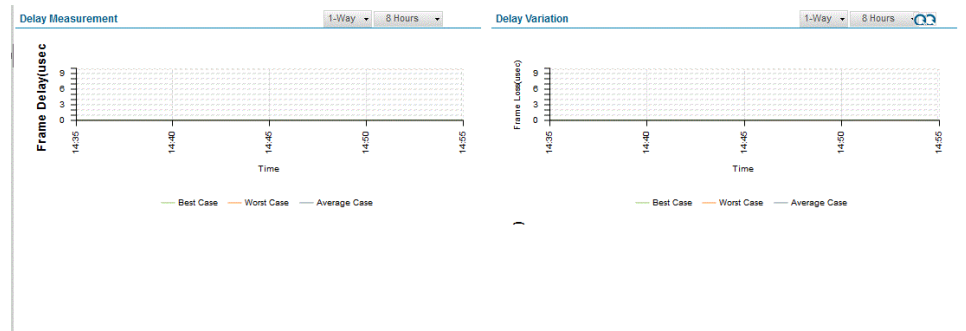
Delay Measurement

The Delay Measurement graph displays a real-time linear plot of delay value with respect to the time. The x-axis represents the time and the y-axis represents frame delay in microseconds. The legends reference average one-way delay, best-case one-way delay, and worst-case one way delay for one-way delay measurement. The green line denotes the lowest one-way frame delay for the statistics displayed, the orange line denotes the highest one-way frame delay for the statistics displayed, and the blue line denotes the average one-way frame delay for the statistics displayed. The legends reference average two-way delay, best-case two-way delay, and worst-case two-way delay for two-way delay measurement. The green line denotes the lowest two-way frame delay for the statistics displayed, the orange line denotes the highest two-way frame delay for the statistics displayed, and the blue line denotes the average two-way frame delay for the statistics displayed. From the Delay End drop-down box, select **1-Way** or **2-Way** to display the one-way or two-way frame delay measurement protocols respectively.

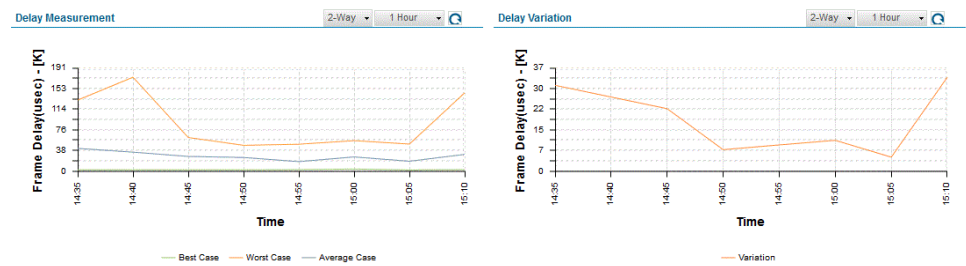
Delay Variation

The Delay Variation graph displays the difference between the consecutive frame delay values. The x-axis represents the time and the y-axis represents delay variation in microseconds. The line denotes the average one-way delay variation or the average one-way “frame jitter” for the statistics displayed for one-way frame delay measurement. The line denotes the average two-way delay variation or the average two-way “frame jitter” for the statistics displayed for two-way delay measurement.

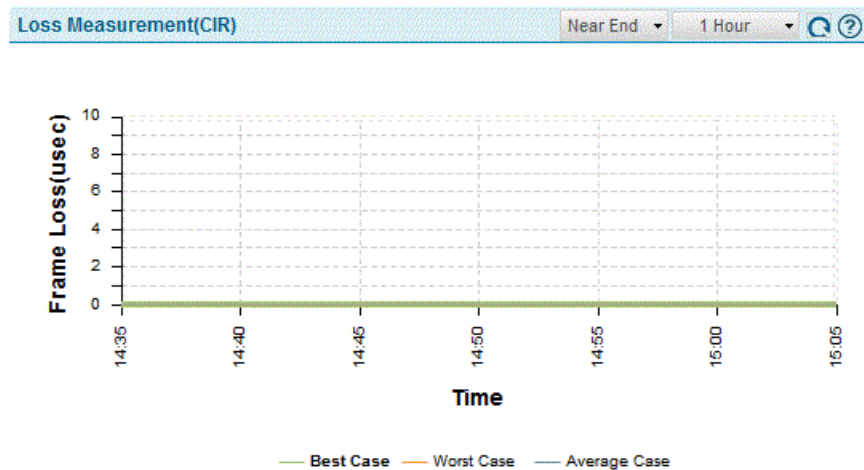
If the delay measurement is one-way, the following graph is displayed.

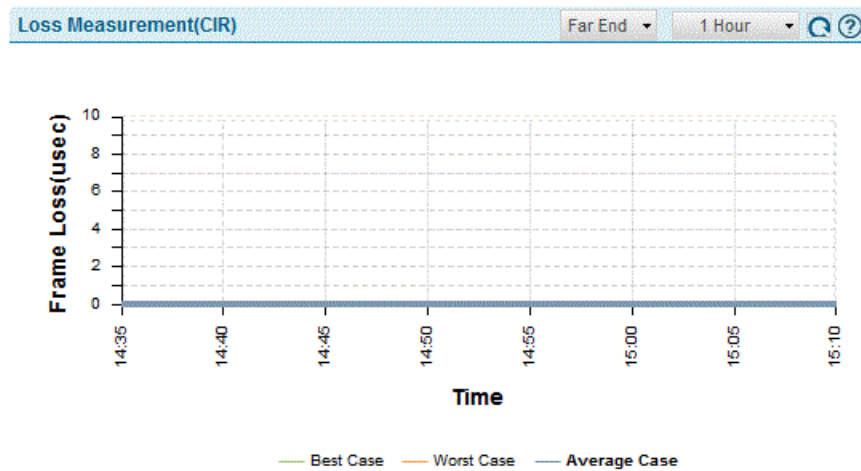


If the delay measurement is two-way, the following graph is displayed.



The Loss Measurement monitor displays two real-time linear plots: Near End (CIR) and Far End (CIR). The three parameters in each graph plot are average case, best case, and worst case of frame-loss.





The graph is plotted in real-time. By default, the total time duration is ten minutes. If the duration of statistics collection exceeds ten minutes, the graph scrolls and shows the data of latest ten minutes.

- See Also**
- [Performance Management Overview on page 1113](#)
 - [Monitoring Performance Management Statistics on page 1115](#)
 - [Viewing Performance Management Statistics on page 1121](#)
 - [Service Troubleshooting Overview on page 1129](#)
 - [Performing a Configuration Audit on page 1077](#)

- Related Documentation**
- [Performance Management Overview on page 1113](#)
 - [Viewing Performance Management Statistics on page 1121](#)
 - [Service Troubleshooting Overview on page 1129](#)
 - [Performing a Configuration Audit on page 1077](#)

Service Troubleshooting Overview

Common reasons for the failure of a service are that a PE device configured for that service is down, or that device has had its service configuration changed so that it no longer matches the service configuration in the Junos Space database.

The primary tools in Junos Space for troubleshooting service problems are:

- Functional audit
- Configuration audit
- Job Management

If the functional audit shows the service to be running, the next step is to perform a configuration audit to see whether the service configuration has been changed out of band, and is no longer consistent with the service configuration in the Junos Space database.

You can view the results of both configuration and functional audits from the **Manage Services** page. You can also view the service configuration from the **Manage Services** page.

In the **Job Management** page, use the **Summary** column to obtain information about failed deployments and failed audits. For deployments in general, the **Summary** column contains useful service information such as the VC ID and endpoint information. For some failed deployments, this column also contains information about why the deployment failed. The following is an example of a failed deployment in the **Job Management** page.

Jobs - Job Management										
0 Item Selected										
ID	Name	Percent Complete	State	Job Type	Parameters	Summary	Scheduled Start ...	Owner	Recurrence	Retr...
458759	Cloud Infrastructure Event Purge-458759	0.0	Scheduled	Cloud Infrastructure Event Purge			Sep 4, 2015 5:30:00 AM IST		Every 86400000 milliseconds First occurrence: Sep 2, 2015 5:30:00 AM IST	0
622654	Vpls-Test-scale Deployment	0.0	Cancelled	Deploy Service		Job was cancelled by user super	Sep 3, 2015 9:45:00 PM IST	super		0
622685	Auto Resynchronize devices-622685	0.0	Scheduled	Auto Resynchroniz e devices	Devices: junos-ms80-2-space		Sep 3, 2015 3:37:27 PM IST			0
622683	Auto Resynchronize devices-622683	100.0	Failure	Auto Resynchroniz e devices	Devices: junos-ms240-space	Number of Reconciled Devices: 1 Number of Reconciled succeeded: 0 Number of Reconciled failed: 1	Sep 3, 2015 3:25:17 PM IST			0
622679	Auto Resynchronize devices-622679	100.0	Failure	Auto Resynchroniz e devices	Devices: RouterZ1-re	Number of Reconciled Devices: 1 Number of Reconciled succeeded: 0 Number of Reconciled failed: 1	Sep 3, 2015 3:21:46 PM IST			0
622675	vpls-bgp-res-tst Deployment	100.0	Success	Deploy Service		Deployed On Device [RouterZ1-re] On Device [RouterY1-re] On Device [RouterX1-re] Failed to addNetworkServiceFailure in Fm deployment Service monitoring is not working properly	Sep 3, 2015 3:19:08 PM IST	super		0
622674	007_P2P_RESValidate Service Order	100.0	Success	Validate Service		Validated On Device [PE9-re] On Device [480R4_EP_Alok-re] On Device [PE10-re] On Device [480R3_EP_Alok-re]	Sep 3, 2015 3:14:43 PM IST	super		0
622673	006_P2P_RESValidate Service Order	100.0	Success	Validate Service		Validated On Device [PE9-re] On Device [480R4_EP_Alok-re] On Device [480R3_EP_Alok-re] On Device [PE10-re]	Sep 3, 2015 3:11:59 PM IST	super		0
622672	005_P2P_RESValidate Service Order	100.0	Failure	Validate Service		Validating On Device [480R4_EP_Alok-re]Error Downloading Configuration	Sep 3, 2015 3:08:25 PM IST	super		0

Related Documentation

- [Performing a Functional Audit on page 1067](#)
- [Performing a Configuration Audit on page 1077](#)
- [Troubleshooting N-PE Devices Before Provisioning a Service on page 1080](#)
- [Modifying the Application Settings of Connectivity Services Director on page 1082](#)
- [Troubleshooting the Endpoints of Services on page 1088](#)
- [Viewing Configuration Audit Results on page 1098](#)
- [Viewing Functional Audit Results on page 1102](#)
- [Viewing Functional Audit Results for an Inverse Multiplexing for ATM Service on page 1106](#)

PART 13

Working in Monitor Mode

- [About Monitor Mode on page 1133](#)
- [Monitoring Traffic on page 1139](#)
- [Monitoring Devices on page 1159](#)
- [General Monitoring on page 1163](#)
- [Monitor Reference on page 1167](#)
- [Detecting and Examining the Health and Performance of Services on page 1191](#)

CHAPTER 39

About Monitor Mode

- [Understanding Monitor Mode in Views Other than Service View of Connectivity Services Director on page 1133](#)
- [Understanding the Monitor Mode Tasks Pane in Views Other than Service View on page 1136](#)

Understanding Monitor Mode in Views Other than Service View of Connectivity Services Director

Monitor mode in Connectivity Services Director provides you visibility into your network status and performance. Connectivity Services Director monitors its managed devices and maintains the information it collects from the devices in a database. Monitor mode displays this information in easy-to-understand graphs and in tables that you can sort and filter, allowing you to quickly visualize the state of your network, spot trends developing over time, and find important details.

Monitor mode divides monitoring activity using the Traffic tab, which provides information about traffic on routers and interfaces.

You can access the Traffic tab on the Monitor mode landing page. An additional tab, the Summary tab, is available that provides a high-level dashboard for the scope selected in the View pane. The monitoring information displayed in the Summary tab also appears on other tabs.

This topic describes:

- [Scope and Monitor Tab Availability on page 1133](#)
- [Monitors and Tasks on page 1134](#)
- [Scope and Data Aggregation on page 1134](#)
- [How Connectivity Services Director Collects and Displays Monitoring Data on page 1134](#)
- [How Connectivity Services Director Displays and Stores Trend Data on page 1135](#)
- [More About the Monitor Tabs on page 1136](#)

Scope and Monitor Tab Availability

Your current scope—that is, your view and node selection in the View pane—affects which Monitor tabs are available. For example, if you select a router, the RF tab is not available.

The shading of the tabs indicate whether a tab is selected, available, or not available:

- The currently selected tab has dark text on a light background.
- Tabs that are available but not selected have dark text on a dark background.
- Tabs that are not available for your current scope have light text on a light background.

When you enter Monitor mode from another mode, the Summary tab is selected for all scopes. If you have selected a tab and then change scope, the tab remains selected if it is supported in the new scope. If it is not supported in the new scope, Connectivity Services Director selects a default tab for that scope.

Monitors and Tasks

When you click a Monitor tab, the landing page for that tab is displayed, which contains a set of monitors. These monitors enable you to see at a glance important information about the aspect of your network being monitored. For example, the monitors in the Traffic tab present high-level information about the traffic or packets flow in the selected scope.

Detailed information is also available from many monitors when you click the Details icon on the monitor. If the Details icon is not visible in the title bar of a monitor, mouse over the monitor to make it visible. For example, if you click the Details icon from the Current Sessions By Type monitor, you can view detailed information about the current sessions.

In addition to monitors, each tab provides a set of tasks available from the Tasks pane. These tasks enable you to perform additional monitoring functions. Some tasks enable you to view more specialized monitoring data; others enable you to perform an operation, such as pinging a host. For a complete list of tasks available in Monitor mode, see [“Understanding the Monitor Mode Tasks Pane in Views Other than Service View” on page 1136](#).

The scope you select affects which monitors are displayed and which tasks are available.

Scope and Data Aggregation

Connectivity Services Director enables you to more than monitor individual devices. It provides a broader network view by aggregating data from devices and making that data available for viewing at higher scopes within the network.

Not all data is aggregated at higher scopes. For example, it does not make sense to provide power supply status at any higher scope than the device itself. Whenever monitors are available at a scope higher than the device scope, however, the data presented is aggregated data from all devices contained in that scope.

How Connectivity Services Director Collects and Displays Monitoring Data

Connectivity Services Director collects monitoring data from all its managed devices at regular intervals known as polling intervals. These polling intervals can vary according to the type of data being collected. Connectivity Services Director sets default polling

intervals for each type of data—you can, however, change these polling intervals in Preferences.

The polling intervals are aligned to clock time. For example, if the polling interval is set to 5 minutes, then within every hour, Connectivity Services Director collects data at :00, :05, :10, :15, and so on. If the polling interval is set to 15 minutes, Connectivity Services Director collects data within every hour at :00, :15, :30, and :45.

Connectivity Services Director uses the Juniper Networks Device Management Interface (DMI) to the managed devices to collect the data. If you have a Junos Space fabric, Connectivity Services Director balances the load of polling the managed devices across the nodes in the fabric.

When you display a monitor, the current data is from the last polling interval. Displaying or refreshing a monitor does not trigger Connectivity Services Director to collect data. However, Connectivity Services Director automatically refreshes monitors with new data after a polling interval completes. Each monitor displays the time that the data was last refreshed.

The detail windows for monitors are not automatically refreshed after a polling period completes. You must manually refresh them to obtain new polling data.

How Connectivity Services Director Displays and Stores Trend Data

In addition to displaying current data, Connectivity Services Director also displays historical data in trend graphs so that you can view trends in network performance over time.

When you display a trend graph, you can select the time period over which the data is displayed—usually 1 hour, 8 hours, 1 day, 1 week, 1 month, 3 months, 6 months, or 1 year. These predefined periods are always relative to the current time and date—that is, if you select a week, the data is from the last 7 days. You can also define a custom time period, which enables you to display data for a period between specific dates and times.

For a trend graph displaying a predefined period of 1 hour, the number of data points depends on the configured polling interval. For periods greater than an hour, the number of data points displayed depends on the time period selected and how Connectivity Services Director consolidates data over time.

To allow storing of monitoring data for a long period of time, Connectivity Services Director consolidates older data. Consolidation involves deriving a single value from a set of shorter term values, generally by averaging the shorter term values, and then using that value as a data point in a longer term data set. After the shorter term data is consolidated into longer term data, it is discarded to save storage space. For example, if a value is polled every 5 minutes, the set of 12 values is consolidated into a single value after an hour has passed. That value then becomes one of the 24 data points that makes up the data set for a day. Similarly, after a day has passed, data is consolidated into one data point that represents that day; after a month has passed, data is consolidated into a one data point that represents that month. Data is not kept for more than a year.

For all trend graphs, Connectivity Services Director will not display data until it has more than two data points to display. This means that after you discover a device, trend data will not appear until three polling periods have passed.

More About the Monitor Tabs

The following sections provide more information about each tab in Monitor mode.

- [The Summary Tab on page 1136](#)
- [The Traffic Tab on page 1136](#)

The Summary Tab

The Summary tab is displayed whenever you enter Monitor mode. It serves as a high-level dashboard for the current selected scope in the View pane.

The monitors displayed in the Summary tab can belong to any of the Monitor categories. Each scope has a predefined set of monitors that are displayed.

When you select an individual device in the View pane, the Summary tab itself displays an arrow that indicates whether the device is up (green up arrow) or down (red down arrow).

For the My Network scope, you can customize what monitors appear on Summary tab, giving you the ability to view at a glance those aspects of network health and performance that are most important to you.

The Traffic Tab

The Traffic tab provides information for analyzing traffic on routers. The four monitors provide an aggregated view of all network traffic on a device, such as proportion of current proportion of multicast, unicast, broadcast traffic or the trend in packet errors. Tasks provide more detailed looks at traffic, such as traffic statistics for individual ports or the degree in which a port's bandwidth is being used.

Understanding the Monitor Mode Tasks Pane in Views Other than Service View

The Tasks pane in Monitor mode displays a list of tasks that are available for the currently selected Monitor tab. These tasks provide monitoring functions in addition to the monitors available under each tab.

The tasks listed in the Tasks pane vary according to the selected tab—that is, Summary or Traffic—and the scope you have selected in the View pane. For example, the L3 VLAN Statistics task is available only when you select the Traffic tab and a router or a device in the View pane.

For each Monitor mode tab, the following tables list each task and provide a short description of the task:

- [Table 140 on page 1137](#): Summary Tab Tasks
- [Table 141 on page 1137](#): Traffic Tab Tasks
- Key Tasks—Connectivity Services Director enables you to group the tasks that you perform frequently and create a list of key tasks. You can add any task from the Tasks pane to the Key Tasks list by selecting a task and clicking the plus (+) sign that appears adjacent to the task. For some modes, you can see that Connectivity Services Director

has predefined some key tasks for you. You can modify this set of tasks to suit your requirements. This feature is available in Task pane irrespective of your current mode, scope, or view.

Table 140: Summary Tab Tasks

Task	Description
Compare Device Statistics	Compares statistics from multiple devices in real time.
Ping To a Host	From the selected device, pings the host you specify and returns the results.
Port Utilization	Displays port utilization trend information for the devices in the selected scope. You can view overall port utilization for the selected device or can view individual port utilization.
Select Monitors to display	Selects the monitors that are displayed in the Summary tab
Show ARP Table	Shows Address Resolution Protocol (ARP) table information for a device.
Show Routing Instances	Show the routing instances configured on an MX Series router.
Traceroute To a Host	From the selected device, traces the route to the host you specify and returns the results.

Table 141: Traffic Tab Tasks

Task	Description
Compare Device Statistics	Compares statistics from multiple devices in real time.
L3 VLAN Statistics	Displays packet in and out statistics for Layer 3 VLANs on the selected device.
Ping To a Host	From the selected device, pings the host you specify and returns the results.
Port Statistics	Displays packet and error statistics for all ports on the selected device.
Port Utilization	Displays port utilization trend information for the devices in the selected scope. You can view overall port utilization for the selected device or can view individual port utilization.
Show ARP Table	Shows Address Resolution Protocol (ARP) table information for a device.
Show Routing Instances	Show the routing instances configured on an MX Series router.
Traceroute To a Host	From the selected device, traces the route to the host you specify and returns the results.

Related Documentation • [Understanding Monitor Mode in Views Other than Service View of Connectivity Services Director on page 1133](#)

Monitoring Traffic

- [Monitoring Traffic on Devices on page 1139](#)
- [Monitoring Port Traffic Statistics on page 1140](#)
- [Monitoring Traffic on Layer 3 VLANs on page 1142](#)
- [Monitoring Port Utilization on page 1143](#)
- [Monitoring Routing Instances on page 1147](#)
- [Viewing Congestion Events on page 1157](#)

Monitoring Traffic on Devices

The monitors on the Traffic tab provide information about the traffic traversing routers and virtual MX Series (vMX) routers.

To monitor traffic on a device:

1. Click **Monitor** in the Connectivity Services Director banner.
2. Select the device in the View pane that contains the traffic you want to monitor.
3. Select the **Traffic** tab to open the traffic monitors.
4. To get help for a monitor, click the Help button in its title bar.

The available monitors include:

- [“Unicast vs Broadcast/Multicast Monitor” on page 1173](#): shows the distribution of unicast, broadcast, and multicast traffic entering and leaving the device.
- [“Unicast vs Broadcast/Multicast Trend Monitor” on page 1174](#): shows trend data about the distribution of unicast, broadcast, and multicast traffic entering and leaving the device.
- [“Traffic Trend Monitor” on page 1173](#): shows trend data about the amount of traffic entering and leaving the device.
- [“Error Trend Monitor” on page 1167](#): shows trend data about the amount of errors on the device.

Monitoring Port Traffic Statistics

This topic describes how to monitor port traffic statistics on a device. You can monitor port traffic statistics for a router, virtual router, or a security device.

This topic describes:

- [Procedure for Monitoring Port Traffic Statistics on page 1140](#)
- [Port on Device Window on page 1140](#)
- [Port Traffic Stats Window on page 1141](#)

Procedure for Monitoring Port Traffic Statistics

1. Click **Monitor** in the Connectivity Services Director banner.
2. Select a node in the View pane that contains the port traffic you want to monitor.
3. Select the **Traffic** tab.
4. In the Tasks pane, select **View > Port Statistics**.

The Port Traffic Stats window opens. For information about this window, click the Help button in the title bar of the window or see [“Port Traffic Stats Window” on page 1141](#).

Port on Device Window

Port on Device window displays the details of all the ports on devices that are configured for network traffic analysis. [Table 142 on page 1140](#) describes the fields that are displayed in the Port on Device window.

Table 142: Port on Device table field descriptions

Field Name	Description
Port Name	Identification of the port.
Admin State	The administrative state of the port: enabled (UP) or disabled (DOWN).
Operational State	The operational status—link up (UP) or link down (DOWN).
Max Bandwidth	The actual bandwidth available on the port, in megabits (Mb).
Negotiated Bandwidth	The negotiated bandwidth based on the speed that is configured or auto-negotiated for the interface.

To view more details about the traffic on any port, select the port and click View Traffic. The Traffic on Port window opens.

Port Traffic Stats Window

The Port Traffic Stats window displays information about the port traffic on the node you selected in the View pane. It contains the following elements:

- Port Traffic Trend graph—This line graph shows trends in the data and error rates on the port selected in the ports table below it. The horizontal axis shows the times when samples were taken. The vertical axis shows the data rate on the left side (in packets per second) and the error rate on the right side (in errors per second).

To display traffic for a different port, select the port from the table below the graph. To change the time period over which to display the traffic trends, select a time period from the list in the upper right corner.



NOTE: After a device is discovered, trend data does not appear immediately—it appears only after three polling periods have elapsed.

To highlight a line on the graph, mouse over the line legend. To remove or restore a line, click the line legend. To see numeric values, mouse over where a data line intersects with a dotted vertical grid line.

- Ports table (on the lower left side of the window)—This table provides information about the ports as described in [Table 143 on page 1141](#). Selecting a port from this table updates the Port Traffic Trend graph to display traffic information about the selected port.
- Counter selection table (on the lower right side of the window)—This table enables you to select which counters to display on the Port Traffic Trend graph. It includes separate tabs for packet counters and error counters. Select the check box in the Show column of each counter that you want to display on the graph. The Per/Sec column shows the rate per second of that row's counter.

Table 143: Port Traffic Window

Table Column	Description
Serial Num	Serial number of the device to which the port belongs.
Port Name	Port name.
Port Usage Type	Port mode—either ACCESS or UPLINK.
MAC Addresses	Port MAC address.
Link Type	Full duplex, half duplex, or unspecified.
In Packets/Sec.(Current)	Current rate of inbound packets.

Table 143: Port Traffic Window (continued)

Table Column	Description
Out Packets/Sec.(Current)	Current rate of outbound packets.

Monitoring Traffic on Layer 3 VLANs

This topic describes how to monitor Layer 3 VLAN traffic statistics on a device. You can monitor Layer 3 VLAN statistics for a router, virtual router, or a security device.

This topic describes:

- [Procedure for Monitoring Layer 3 VLAN Traffic Statistics on page 1142](#)
- [L3 VLAN Traffic Stats Window on page 1142](#)

Procedure for Monitoring Layer 3 VLAN Traffic Statistics

1. Click **Monitor** in the Connectivity Services Director banner.
2. Select a node in the View pane that contains the Layer 3 VLAN traffic you want to monitor.
3. Select the **Traffic** tab.
4. In the Tasks pane, select **View > L3 VLAN Statistics**.

The L3 VLAN Traffic Stats window opens. For information about this window, click the Help button in the title bar of the window or see [“L3 VLAN Traffic Stats Window” on page 1142](#).

L3 VLAN Traffic Stats Window

The L3 VLAN Traffic Stats window displays information about the Layer 3 VLAN traffic on the node you selected in the View pane. It contains two panes:

- **VLAN Traffic line graph**—This graph shows the data transmission rate on the Layer 3 VLAN selected in the table beneath the graph. The horizontal axis shows the times when samples were taken. The vertical axis shows the data rate, in bytes per second.
To show a Layer 3 VLAN on the VLAN Traffic line graph, select the Layer 3 VLAN from the table beneath the graph. To highlight a line on the graph, mouse over the line legend. To remove or restore a line, click the line legend. To see numeric values, mouse over a data point.
- **Layer 3 VLAN traffic statistics table**—This table provides information about the Layer 3 VLANs as described in [Table 144 on page 1143](#). Selecting a Layer 3 VLAN from this table updates the VLAN Traffic graph to display the traffic information for the selected Layer 3 VLAN.

Table 144: Layer 3 VLAN Traffic Statistics Table

Table Column	Description
L3 Interface	Layer 3 interface assigned to the VLAN.
SerialNo	The serial number of the device containing the Layer 3 VLAN.
VLAN Name	VLAN name.
VLAN ID	VLAN ID.
Description	VLAN description.
In Packet	Number of packets entering the VLAN.
Out Packet	Number of packets leaving the VLAN.

Monitoring Port Utilization

Connectivity Services Director provides information about port utilization in either one of two places, depending on the node you select in the View pane:

- Port Utilization monitor—This monitor, available in the Summary tab, provides a bar chart that shows the aggregate utilization of the ports on a device or devices over a period of time that you select. For more information about using the Port Utilization monitor, see *Port Utilization Monitor*.
- Port Utilization task—This task, available from **View > Port Utilization** in the Tasks pane of the Summary or Traffic tabs, provides a bar chart similar to the Port Utilization monitor bar chart. Unlike the Port Utilization monitor, it also enables you to obtain information on individual port utilization over time when you have selected an individual device or Layer 3 Fabric in the View pane.

This topic describes the Port Utilization task. It describes:

- [How to Access the Port Utilization Task on page 1143](#)
- [Port Utilization Details Window on page 1144](#)
- [Utilization for Device Window on page 1144](#)
- [Utilization for IP Fabric Window on page 1146](#)

How to Access the Port Utilization Task

1. Click **Monitor** in the Connectivity Services Director banner.
2. Select a node in the View pane that contains the ports whose utilization you want to monitor.

3. Select the **Summary** or **Traffic** tab.

4. In the Tasks pane, select **View > Port Utilization**.

If you have selected a node that contains more than one device, the Port Utilization Details window opens. For information about this window, see [“Port Utilization Details Window” on page 1144](#).

If you have selected an individual device, the Utilization for Device window opens. For information about this window, see [“Utilization for Device Window” on page 1144](#).

If you have selected a Layer 3 Fabric, the Utilization for IP Fabric window opens. For information about this window, see [“Utilization for IP Fabric Window” on page 1146](#).

Port Utilization Details Window

This window provides a bar chart showing the aggregate port utilization trend for the devices within the selected scope.

Each bar in the bar chart represents the overall port utilization for all the devices at a polling interval. The vertical axis shows the number of ports polled. The horizontal axis shows the time when each poll was taken.

Each bar is divided into the following colored sections to indicate the distribution of port utilization at the polling interval:

- Green indicates ports that operated at less than 50% of negotiated speed.
- Orange indicates ports that operated at between 50% and 80% of negotiated speed.
- Red indicates ports that operated at more than 80% of negotiated speed.

You can perform the following actions on the bar chart:

- Change the time period over which to display the trend data by selecting a time period from the list in the upper right corner.
- Remove or restore a utilization category (bar color) by clicking its legend.
- Display a numeric value by mousing over a bar.

Utilization for Device Window

The Utilization for Device window shows the port utilization trend for individual devices and ports. It is available when you select a individual device in the View pane.

The Utilization for Device window provides two views of port utilization:

- **Device**—This view provides a trend chart of overall port use on the device over time.
- **Port**—This view provides a heat map of all the ports on the device, enabling you to view the utilization of individual ports. You can choose a port from the heat map to view a utilization trend chart for that particular port.

The Device view is the default view. Click **Port** to change to the Port view.

Device View

The Device view provides a bar chart that shows the trend of overall port use on the device. Each bar represents the overall port utilization at a polling interval. The vertical axis shows the number of ports polled. The horizontal axis shows the time when each poll was taken.

Each bar is divided into the following colored sections to indicate the distribution of port utilization at the polling interval:

- Green indicates ports that operated at less than 50% of negotiated speed.
- Orange indicates ports that operated at between 50% and 80% of negotiated speed.
- Red indicates ports that operated at more than 80% of negotiated speed.

You can perform the following actions in Device view:

- Change the time period over which to display the trend data by selecting a time period from the list in the upper right corner.
- Remove or restore a utilization category (bar color) by clicking its legend.
- Display a numeric value by mousing over a bar.

Port View

The Port view provides utilization heat maps of the ports on the device—one heat map for access ports and another for uplink ports. In the heat maps, each port on the device is represented by a box that is color-coded to indicate the level of port utilization. Cooler colors (for example, green) indicate lower port utilization, while hotter colors (for example, red) indicate higher port utilization.

Click a port box to display a utilization trend chart for that individual port.

You can perform the following actions in the Port view:

- On a heat map:
 - Mouse over a port box to see more information about the port such as the port utilization percent, port type, MAC address of the port, duplex mode, device serial number, admin status and operational status of the port, negotiated speed, and the last flap time.
 - Change the time period over which the port utilization percentage is derived.
 - Click a port box to display the utilization trend chart for that port.
 - Use the percentage slider under the port heat map to display only those ports for which utilization falls within a certain percentage range.
- On the port utilization trend chart:
 - Change the time period over which to display the trend data.
 - Display the percentage utilization and polling time by mousing over a data point.

Utilization for IP Fabric Window

The Utilization for IP Fabric window provides information about port utilization for the devices and ports within a Layer 3 Fabric. It is available when you select a Layer 3 Fabric in the View pane.

The top part of the Utilization for IP Fabric window displays a heat map of the devices in the Layer 3 Fabric. Each device in the Layer 3 Fabric shown as either a spine or leaf device and is color-coded to show the overall port utilization on the device.

You can interact with this fabric-level heat map as follows:

- Mouse over a box representing a device. Information about that device is displayed, such as IP address, model, overall port utilization, and a list of the five ports with the highest utilization.
- Click a box representing a device. The information in the remainder of the window is changed to reflect the port utilization of the device.

You can select two different views of the port utilization on the device:

- Device—This view provides a trend chart of overall port use on the device over time.
- Port—This view provides a heat map of all the ports on the device, enabling you to view the utilization of individual ports. You can choose a port from the heat map to view a utilization trend chart for that particular port.

The Device view is the default view. Click **Port** to change to the Port view.

Device View

The Device view provides a bar chart that shows the trend of overall port use on the selected device. Each bar represents the overall port utilization at a polling interval. The vertical axis shows the number of ports polled. The horizontal axis shows the time when each poll was taken.

Each bar is divided into the following colored sections to indicate the distribution of port utilization at the polling interval:

- Green indicates ports that operated at less than 50% of negotiated speed.
- Orange indicates ports that operated at between 50% and 80% of negotiated speed.
- Red indicates ports that operated at more than 80% of negotiated speed.

You can perform the following actions on the bar chart:

- Change the time period over which to display the trend data by selecting a time period from the list in the upper right corner.
- Remove or restore a utilization category (bar color) by clicking its legend.
- Display a numeric value by mousing over a bar.

Port View

The Port view provides utilization heat maps of the ports on the device—one heat map for access ports and another for uplink ports. In the heat maps, each port on the device is represented by a box that is color-coded to indicate the level of port utilization. Cooler colors (for example, green) indicate lower port utilization, while hotter colors (for example, red) indicate higher port utilization.

You can perform the following actions on the device heat map:

- Mouse over a port box to see more information about the port, such as the port utilization percent, port type, MAC address of the port, duplex mode, device serial number, admin status and operational status of the port, negotiated speed, and the last flap time.
- Change the time period over which the port utilization percentage is derived.
- Use the percentage slider under the port heat map to display only those ports whose percent utilization falls within a certain range.
- Click a port box to display the utilization trend chart for that port.

The port utilization trend chart shows the utilization trend for the selected port. You can:

- Change the time period over which to display the trend data.
- Display the percentage utilization and polling time by mousing over a data point.

Monitoring Routing Instances

This topic describes how to monitor VPN routing instances on MX Series routers by using Connectivity Services Director. Using Connectivity Services Director, you can determine which interfaces and bridge domains belong to the routing instances and view traffic statistics for those interfaces and bridge domains. You can also display connection information for Layer 2 VPN and virtual private LAN service (VPLS) routing instances.

Connectivity Services Director can be used to monitor the following types of Layer 2 routing instances:

- Default routing instance
- Ethernet VPN (EVPN)
- Layer 2 VPN
- VPLS
- Virtual switch

Connectivity Services Director can be used to monitor the following types of Layer 3 routing instances:

- Layer 3 VPN

This topic describes:

- [Procedure for Monitoring Routing Instances on page 1148](#)
- [Show Routing Instances Window on page 1148](#)
- [Show Interfaces Window on page 1149](#)
- [Show Bridge Domains Window on page 1150](#)
- [Show Connections on page 1151](#)
- [Show Routing Tables on page 1154](#)
- [Show MAC Table on page 1156](#)

Procedure for Monitoring Routing Instances

Use the options in the Show Routing Instances window to monitor routing instances.

1. Click **Monitor** in the Connectivity Services Director banner.
2. Select an MX Series router in the View pane that contains the port traffic you want to monitor.
3. In the Tasks pane, select **Tasks > Show Routing Instances**.

The Show Routing Instances window opens. For information about this window, click the Help button in the title bar of the window or see [“Show Routing Instances Window” on page 1148](#).

Show Routing Instances Window

The Show Routing Instances window lists the routing instances configured on a selected device. Use this window to display the interfaces or bridge domains belonging to a routing instance and obtain traffic statistics for the interfaces. You can also display information about the VPLS and Layer 2 VPN connections. [Table 145 on page 1148](#) describes the fields in this window.

Table 145: Fields in the Show Routing Instances Window

Field	Description
Routing Instance Name	Name of the routing instance. The default routing instance is named default-switch.

Table 145: Fields in the Show Routing Instances Window (continued)

Field	Description
Type	Identifies the routing instance type: <ul style="list-style-type: none"> • EVPN • L2VPN • L3VPN • Virtual Switch The default routing instance is of this type. <ul style="list-style-type: none"> • VPLS • VRF (L3VPN)
Details	Provides the following information (if configured for the routing instance): <ul style="list-style-type: none"> • Route Distinguisher—Used to identify all routes that are part of the VPN. The route distinguisher makes IP addresses globally unique, so that the same IP address prefixes can be used for different VPNs. • Target—Extended BGP community used to match routes for import and export.
Interfaces	Displays the number of interfaces belonging to the routing instance. Click the number to open the Show Interfaces window, described in “Show Interfaces Window” on page 1149 .
Bridge Domains	Displays the number of bridge domains belonging to the routing instance. Click the number to open the Show Bridged Domains window, described in “Show Bridge Domains Window” on page 1150 .
Actions	<ul style="list-style-type: none"> • Click Show Connections to display information about Layer 2 VPN and VPLS connections. The information described in “Show Connections” on page 1151 is displayed. This link is available only for Layer 2 VPN and VPLS routing instances. • Click Show MAC Table to display the MAC table for the selected routing instance. For details, see “Show MAC Table” on page 1156. • Click Show Routing Table to view the routing table information for the selected routing instance. For details, see “Show Routing Tables” on page 1154.



Show Interfaces Window

The Show Interfaces window lists the logical interfaces configured on the routing instance and provides the information about the interfaces as described in [Table 146 on page 1149](#).

Table 146: Show Interfaces Information

Field	Description
Interface Name	The interface name.
Port Mode	Indicates one of two modes—access or trunk: <ul style="list-style-type: none"> • Access—The interface can be in a single VLAN only. • Trunk—The interface can be in multiple VLANs and accept tagged packets from multiple devices.

Table 146: Show Interfaces Information (continued)

Field	Description
Interface State	Indicates whether the interface is  UP or  DOWN.
STP State	Indicates whether the interface is in a discarding (blocked) or in forwarding (unblocked) state. (Not shown for interfaces belonging to Layer 2 VPN and Layer 3 VPN routing instances.)
Local IP Address	Local IP address. (Shown only for interfaces belonging to Layer 2 VPN and Layer 3 VPN routing instances.)
Remote IP Address	Remote IP address. (Shown only for interfaces belonging to Layer 2 VPN and Layer 3 VPN routing instances.)
Actions	<ul style="list-style-type: none"> Click View Statistics to display traffic statistics for the interface. The Show Interface Statistics window opens, which charts the number of input and output packets and the number of input and output bytes. Click Show MAC Table to display the MAC table for the interface. For more details, see “Show MAC Table” on page 1156.

Show Bridge Domains Window

The Show Bridge Domains window lists the bridge domains configured on the routing instance. To display information about the VLAN IDs and interfaces configured on a bridge domain, select the bridge domain. [Table 147 on page 1150](#) describes the information provided in the Show Bridge Domains window.

Table 147: Show Bridge Domains Information



Field	Description
Bridge Domains	The bridge domain name.
Actions	Click Show MAC Table to display the MAC table for the selected bridge domain. For details, see “Show MAC Table” on page 1156 .
VLAN ID	The VLAN ID or IDs assigned to the bridge domain.
Interface Name	The name of a logical interface assigned to the VLAN ID.
Port Mode	Indicates one of two modes—access or trunk: <ul style="list-style-type: none"> Access—The interface can be in a single VLAN only. Trunk—The interface can be in multiple VLANs and accept tagged packets from multiple devices.
Interface State	Indicates whether the interface is  UP or  DOWN.

Table 147: Show Bridge Domains Information (continued)

Field	Description
STP State	Indicates whether the interface is in a discarding (blocked) or in forwarding (unblocked) state.
Actions	<ul style="list-style-type: none"> Click View Statistics to display traffic statistics for the interface. The Show Interface Statistics window opens, which charts the number of input and output packets and the number of input and output bytes. Click Show MAC Table to display the MAC table for the interface. For details, see “Show MAC Table” on page 1156.

Show Connections

The Show Connections window provides information about the VPN connections for Layer 2 VPN and VPLS routing instances as described in [Table 148 on page 1151](#).

Table 148: Show Connections Information



Field	Description
Local Site Name	Name of the local site.
Local Site ID	Identifier for the local site.
Local Interface Name	Name of the local interface.
Interface Status	Indicates whether the local interface is  UP or  DOWN.
Remote Site ID	Identifier for the remote site.
Remote IP	IP address of the remote provider edge device (PE device).

Table 148: Show Connections Information (continued)

Field	Description
Connection Status	

Table 148: Show Connections Information (continued)

Field	Description
	<p>Status of the connection:</p> <ul style="list-style-type: none"> • EI—The local VPN interface is configured with an encapsulation that is not supported. • EM—The encapsulation type received on this connection from the neighbor does not match the local connection interface encapsulation type. • VC-Dn—The virtual circuit is currently down. • CM—The two routers do not agree on a control word, which causes a control word mismatch. • CN—The virtual circuit is not provisioned properly. • OR—The label associated with the virtual circuit is out of range. • OL—No advertisement has been received for this virtual circuit from the neighbor. There is no outgoing label available for use by this virtual circuit. • LD—All of the CE-facing interfaces to the local site are down. Therefore, the connection to the local site is signaled as down to the other PE routers. No pseudowires can be established. • RD—All the interfaces to the remote neighbor are down. Therefore, the remote site has been signaled as down to the other PE routers. No pseudowires can be established. • LN—The local site has lost path selection to the remote site and therefore no pseudowires can be established from this local site. • RN—The remote site has lost path selection to a local site or to a remote site and therefore no pseudowires are established to this remote site. • XX—The connection is down for an unknown reason. This is a programming error. • MM—The MTUs for the local site and the remote site do not match. • BK—The router is using a backup connection. • PF—Profile parse failure. • RS—The remote site is in a standby state. • NC—The interface encapsulation is not configured as an appropriate CCC (circuit cross-connect), TCC (translational cross-connect), Layer 2 VPN, or VPLS encapsulation. • WE—The encapsulation configured for the interface does not match with the encapsulation configured for the associated connection within the routing instance. • NP—The router detects that interface hardware is not present. The hardware might be offline, a PIC might not be of the compatible type, or the interface might be configured in a different routing instance. • ->—Only the outbound connection is up. • <-—Only the inbound connection is up. • Up—The connection is operational. • Dn—The connection is down. • CF—The router cannot find enough bandwidth to the remote router to satisfy the connection bandwidth requirement. • SC—The local site identifier is the same as the remote site identifier. No pseudowire can be established between these two sites. You must configure different values for the local and remote site identifiers. • LM—The local site identifier is not the minimum designated, which means it is not of the lowest value. There is another local site with a lower value for site

Table 148: Show Connections Information (continued)

Field	Description
	<p>identifier. Pseudowires are not being established to this local site and the associated local site identifier is not being used to distribute Layer 2 VPN or VPLS label blocks. However, this is not an error state. Traffic continues to be forwarded to the PE router interfaces connected to the local sites when the local sites are in this state.</p> <ul style="list-style-type: none"> • RM—The remote site identifier is not the minimum designated, which means it is not the lowest. There is another remote site connected to the same PE router which has lower site identifier. The PE router cannot establish a pseudowire to this remote site and the associated remote site identifier cannot be used to distribute VPLS label blocks. However, this is not an error state. Traffic continues to be forwarded to the PE router interface connected to this remote site when the remote site is in this state. • IL—The incoming packets for the connection have no MPLS label. • MI—The configured mesh group identifier is in use by another system in the network. • ST—The router has switched to a standby connection. • PB—Profile is busy. • SN—The neighbor is static.
Time Last Up	The time when the connection was last in the Up condition.

Show Routing Tables

The Routing Tables window enables you view the routing table information for the selected virtual routing instance. For L3VPN and EVP services, you can determine which LSPs or tunnels are being used by looking at the routing tables.

- **Routing Tables**—The Routing Tables table shows the routing tables associated with the virtual instance and the number of active routes in each table. Click on a routing table to display the actual contents of the routing table.
- **Details**—The Details table shows the contents of the selected routing table. [Table 149 on page 1154](#) displays the fields that are displayed in the Details table.

Table 149: Show Routing Table Field Descriptions

Name	Description
Routing Instance	Name of the routing instance.
Number of Destinations	Number of destinations for which there are routes in the routing table.
Active Routes	Number of routes that are active.
Hidden Routes	Number of routes that are not used because of routing policy.
Hold-down Routes	Number of routes that are in the hold-down state before being declared inactive.
Total Routes	Total number of routes.

Table 149: Show Routing Table Field Descriptions (continued)

Name	Description
Destination Prefix	<p>Route destination (for example:10.0.0.1/24). Sometimes the route information is presented in another format, such as:</p> <ul style="list-style-type: none"> • MPLS-label (for example, 80001). • interface-name (for example, ge-1/0/2). • neighbor-address:control-word-status:encapsulation type:vc-id:source (Layer 2 circuit only. For example, 10.1.1.195:NoCtrlWord:1:1:Local/96): <ul style="list-style-type: none"> • neighbor-address—Address of the neighbor. • control-word-status—Whether the use of the control word has been negotiated for this virtual circuit: NoCtrlWord or CtrlWord. • encapsulation type—Type of encapsulation, represented by a number: (1) Frame Relay DLCI, (2) ATM AAL5 VCC transport, (3) ATM transparent cell transport, (4) Ethernet, (5) VLAN Ethernet, (6) HDLC, (7) PPP, (8) ATM VCC cell transport, (10) ATM VPC cell transport. • vc-id—Virtual circuit identifier. • source—Source of the advertisement: Local or Remote.
State	State of the route.
Protocol	Name of the protocol from which the route was learned. For example, OSPF , RSVP , and Static .
Protocol Preference	Preferred protocol for this routing instance. Junos OS uses this preference to choose which routes become active in the routing table.
Age	Displays how long since the route was learned.
Metric	Cost value of the indicated route. For routes within an AS, the cost is determined by the IGP and the individual protocol metrics. For external routes, destinations, or routing domains, the cost is determined by a preference value.
BGP Local Preference	A metric used by BGP sessions to indicate the degree of preference for an external route. The route with the highest local preference value is preferred.
Route Learned From	Interface from which the route was received.
AS Path	<p>AS path through which the route was learned. The letters at the end of the AS path indicate the path origin, providing an indication of the state of the route at the point at which the AS path originated:</p> <ul style="list-style-type: none"> • I—IGP • E—EGP • ?—Incomplete; typically, the AS path was aggregated.
Validation State	<p>(BGP-learned routes) Validation status of the route:</p> <ul style="list-style-type: none"> • Invalid—Indicates that the prefix is found, but either the corresponding AS received from the EBGP peer is not the AS that appears in the database, or the prefix length in the BGP update message is longer than the maximum length permitted in the database. • Unknown—Indicates that the prefix is not among the prefixes or prefix ranges in the database. • Valid—Indicates that the prefix and autonomous system pair are found in the database.

Table 149: Show Routing Table Field Descriptions (continued)

Name	Description
Next Hop Type	Next hop to the destination. An angle bracket (>) indicates that the route is the selected route. If the destination is Discard, traffic is dropped.
Local Interface	The local interface used to reach the next hop.
Address	IP address of the interface.
Via Interface	Interface used to reach the next hop. If there is more than one interface available to the next hop, the interface that is actually used is followed by the word Selected.
MPLS Label	MPLS label and operation occurring at the next hop. The operation can be pop (where a label is removed from the top of the stack), push (where another label is added to the label stack), or swap (where a label is replaced by another label).

Show MAC Table

The Show MAC table window displays the MAC table for the selected routing instance. [Table 150 on page 1156](#) describes the fields that are displayed in the Show MAC Table window.

Table 150: Show MAC Table fields

Field Name	Description
Routing Instance	Name of the routing instance.
Type	Identifies the routing instance type: <ul style="list-style-type: none"> • EVPN • L2VPN • L3VPN • Virtual Switch The default routing instance is of this type. <ul style="list-style-type: none"> • VPLS • VRF (L3VPN)
Bridge Domain	Name of the bridging domain.
VLAN ID	VLAN ID of the routing instance or bridge domain in which the MAC address was learned.
MAC Address	MAC address or addresses learned on a logical interface.

Table 150: Show MAC Table fields (continued)

Field Name	Description
MAC Flags	<p>Status of MAC address learning properties for each interface:</p> <ul style="list-style-type: none"> • S—Static MAC address is configured. • D—Dynamic MAC address is configured. • L—Locally learned MAC address is configured. • C—Control MAC address is configured. • SE—MAC accounting is enabled. • NM—Non-configured MAC. • R—Remote PE MAC address is configured.
Logical Interface	Name of the logical interface.

Viewing Congestion Events

This topic describes how to view congestion events on a device. A congestion event occurs when congestion on a device port exceeds the configured threshold.

You can view congestion events only for devices that support Cloud Analytics Engine and that have the high-frequency traffic statistics feature enabled in Connectivity Services Director.

To view congestion events on a device, you must first do the following:

- Configure the Data Learning Engine (DLE) settings under **Preferences > Monitoring > Data Learning Engine Settings**. The DLE is a component of Cloud Analytics Engine.
- Enable high-frequency traffic statistics on the device and optionally configure thresholds.

To view congestion events on a device:

1. In the View pane, select a device on which the high-frequency traffic statistics feature is enabled.
2. Click **Monitor** in the Connectivity Services Director banner to open Monitor mode.
3. In the Tasks pane, select **Tasks > View Congestion Events**. The View Congestion Events window opens.

The View Congestion Events window lists congestion events that occurred on the device during the time span of 1 minute. The table column headings are the seconds within the selected minute. Each row represents a device interface. Each cell represents the activity on that interface during that second. When congestion events occurred during that second, a bubble appears in the cell. The size of the bubble indicates how many congestion events occurred during that second. The color of the bubble indicates the severity of the

congestion during that second: cooler colors indicate lower severity, and hotter colors indicate higher severity.

You can perform these actions in the View Congestion Events window :

- Use the Select Hour and Select Minute lists to select the minute in which to display congestion events and then click **Submit**.
- Mouse over a port name to change the bubbles in its row into the number of congestion events that occurred during each second.
- Click a bubble to open a bar chart that shows detailed information about the congestion events that occurred during that second.

Monitoring Devices

- [Comparing Device Statistics on page 1159](#)
- [Showing ARP Table Information on page 1160](#)

Comparing Device Statistics

This topic describes how to compare statistics from multiple network devices and interfaces in real time. You select which devices, interfaces, and counters to compare, and how often to poll for new statistics.

This topic describes:

- [Procedure for Comparing Device Statistics on page 1159](#)
- [Compare Interfaces Window on page 1159](#)

Procedure for Comparing Device Statistics

1. Click **Monitor** in the Connectivity Services Director banner.

You can compare device statistics in any tab in Monitor mode.

2. In the Tasks pane, select **Tasks > Compare Device Statistics**.

The Compare Interfaces window opens. For information about this window, click the Help button in the title bar of the window or see [“Compare Interfaces Window” on page 1159](#).

Compare Interfaces Window

The Compare Interfaces window enables you to compare statistics from multiple device interfaces in real time. The search scope is the entire managed network, regardless of which node is selected in the View pane.

To compare device statistics:

1. Select the devices to compare from the device tree in the Select Devices section.
2. Select a device in the Selected Devices section to select which of its interfaces to compare.

The Select Interfaces section lists the device's interfaces. You can select up to two interfaces per device.

3. Select an Interface in the Select Interfaces section to select which of its counters to compare.

The Select Counters section lists the interface's counters.

4. Select the counters to compare in the Select Counters section.
5. Repeat the process of selecting devices, interfaces, and counters to compare until you are finished selecting what to compare.

6. Select how often the data will be refreshed from the **Data Collection Frequency** list.

7. Click the **Compare** button to start comparing information.

A page opens containing a line graph for each counter you selected. Each graph displays all the interfaces for which its counter is selected.

8. To pause data collection, click the **Pause** button. To resume data collection, click the **Resume** button.

9. To change data collection settings, click the **Back** button.

Showing ARP Table Information

This topic describes how to show Address Resolution Protocol (ARP) table information for a device. ARP table information is collected from the selected device when this task runs. You can search for ARP table records.

- [Procedure for Showing ARP Table Information on page 1160](#)
- [Show ARP Table Information Window on page 1161](#)

Procedure for Showing ARP Table Information

To show ARP table information for a device:

1. Click **Monitor** in the Connectivity Services Director banner.
2. Select the device in the View pane that you want to monitor.
3. Select **Tasks > Show ARP Table** in the Task pane.

The Show ARP Table Information window opens. For information about this window, click the Help button in the title bar of the window or see [Table 151 on page 1161](#). You can click the Refresh button below the table to refresh the data from the device.

Show ARP Table Information Window

The Show ARP Table Information Window shows information from the selected device's ARP table.

Table 151: Show ARP Table Information Window

Control or Column	Description
Search controls	Search for ARP table records. Enter search text in the text box. The table of ARP records displays only matching records. Click the X button to clear the search and display all records.
MAC Address	MAC address.
IP Address	IP address.
Interface Name	Interface name.
Expiring in (sec)	Number of seconds until the record expires from the ARP table.

General Monitoring

- [Selecting Monitors To Display on the Summary Tab on page 1163](#)
- [Changing Monitor Polling Interval and Data Collection on page 1164](#)
- [Pinging Host Devices on page 1164](#)
- [Troubleshooting Network Connections Using Traceroute on page 1165](#)

Selecting Monitors To Display on the Summary Tab

When you select the My Network node in the View pane, the Summary tab in Monitor mode enables you to select which monitors to display. If you select more than four monitors, a scroll bar appears to allow you to scroll to the additional monitors.

To select monitors to display on the Summary tab:

1. Click **Monitor** in the Connectivity Services Director banner.
2. Select the **My Network** node in the View pane (the top node in the tree).
3. To select which monitors to display on the Summary tab:
 - a. Click **Select Monitors to Display** in the Tasks pane.

The Select Monitors window opens. The monitors that are already selected to display are listed in the Selected list. The other available monitors are listed in the Available list.
 - b. To move a monitor from one list to the other list, click the monitor name, and then click the right or left arrow button, as appropriate.
 - c. To change the order in which the selected monitors appear in the tab, select a monitor name and move it in the list using the up and down arrow buttons. The

arrow buttons at the top and bottom of the stack of buttons move the selected monitor to the top or bottom of the list, respectively.

- d. Click **Save** to save your changes, or click **Cancel** to cancel your changes.
4. To get information about a monitor, click the Help button in its title bar.

Related Documentation

- [Understanding Monitor Mode in Views Other than Service View of Connectivity Services Director on page 1133](#)

Changing Monitor Polling Interval and Data Collection

Network Administrators can change the default polling interval for monitors. The default polling period varies by monitor category. You can change these values in Preferences, found in the Connectivity Services Director banner. You can also enable or disable the data collection processes used by monitors in Preferences.

Pinging Host Devices

Use the Ping Host task in Monitor mode to determine whether an MX Series host can be reached over the network from the device selected in the network tree. Entering a hostname or an address creates a periodic ping task that sends a series of Internet Control Message Protocol (ICMP) echo (ping) requests to the specified host. The output of the task displays in the Response Console.

The Ping from Device to a Host task is available only for ACX Series routers, M Series routers, MX Series routers, and PTX Series routers in your network.

1. Select either IP or HostName in the Remote Host Details box.
2. Type the IP address or hostname for the device that you want to reach.
3. Click **Ping** to use the default settings and start the requests or select the plus (+) symbol to use the Advanced Search Criteria. The fields in Advanced Search Criteria are described in [Table 152 on page 1164](#).

Table 152: Ping Host Advanced Search Criteria Field Descriptions

Field	Description	Default
Count	Indicates the number of ping requests to send. Valid values are 1 through 24.	3
Type of Service	Sets the type-of-service (ToS) field in the IP header of the ping packets. The range of values is 0 through 255. If the routing platform does not support ToS, the field is ignored.	0

Table 152: Ping Host Advanced Search Criteria Field Descriptions (continued)

Field	Description	Default
Time To Live	Indicates the time-to-live hop count for the ping request packet. Valid values are 0 through 255.	32
Wait Interval	Indicates the amount of time in seconds between ping requests. Valid values are 0 through 24; a 0 value sends the request immediately.	0
Packet Size	Indicates the size of the ping request packet in bytes. The routing platform adds 8 bytes of ICMP header to this size before sending the request packet.	56
Interface	Sends the ping requests on the interface you specify. If you do not specify this option, ping requests are sent on all interfaces.	All
Source	Uses the source address that you specify in the ping request packet.	None

Related Documentation

- [Understanding Monitor Mode in Views Other than Service View of Connectivity Services Director on page 1133](#)

Troubleshooting Network Connections Using Traceroute

Traceroute is a diagnostic tool that enables you to display the route that a packet takes to reach the destination and measure transit delays of packets across an Internet Protocol (IP) network. You can use traceroute to troubleshoot and identify points of failure in your switching network. In traceroute, the source device sends three Internet Control Message Protocol (ICMP) echo request packets to the destination device. This is done sequentially till the source receives an ICMP echo reply message from the destination device. The time-to-live (TTL) value is used in determining the number of intermediate devices that the packets traverse before reaching the destination device.

You can use traceroute for ACX, M, MX, and PTX Series routers.

To start a traceroute from the selected device to another device in your network:

1. Select either IP or HostName in the Remote Host Details box.
2. Type the IP address or hostname for the device to which you want to start a traceroute.
3. Click **Trace** to use the default settings and start the traceroute or select the plus (+) symbol to use the Advanced Options. The fields in Advanced Options are described in [Table 153 on page 1166](#).

Table 153: Traceroute Advanced Options Field Descriptions

Field	Description	Default
Interface	Sends the Internet Control Message Protocol (ICMP) echo request packets on the interface you specify. If you do not specify this option, ICMP packets are sent on all interfaces.	Select a value from the list.
Time To Live	Indicates the time-to-live hop count for the ICMP echo request packets. Default value is 30. Valid values are 1 through 255.	30
Wait Interval	Indicates the amount of time in seconds between echo requests. Default value is 5. Valid values are 1 through 24.	5
Type of Service	Sets the type-of-service (ToS) field in the IP header of the echo packets. The range of values is 0 through 255. If the routing platform does not support ToS, the field is ignored.	0

Related Documentation

- [Understanding Monitor Mode in Views Other than Service View of Connectivity Services Director on page 1133](#)

CHAPTER 43

Monitor Reference

- [Error Trend Monitor on page 1167](#)
- [Equipment Status Summary Monitor on page 1169](#)
- [Equipment Summary By Type Monitor on page 1170](#)
- [Port Status Monitor on page 1170](#)
- [Port Utilization Monitor on page 1172](#)
- [Status Monitor for Routers on page 1172](#)
- [Traffic Trend Monitor on page 1173](#)
- [Unicast vs Broadcast/Multicast Monitor on page 1173](#)
- [Unicast vs Broadcast/Multicast Trend Monitor on page 1174](#)
- [Session Trends Monitor on page 1175](#)
- [Current Sessions by Type Monitor on page 1177](#)
- [User Session Details Window on page 1177](#)
- [Current Active Alarms Monitor \(All Views Except Service View\) on page 1179](#)
- [Top Sessions by MAC Address Monitor on page 1180](#)
- [Top APs by Session Monitor on page 1181](#)
- [Radio Technology Type Statistics Monitor on page 1182](#)
- [Top Talker - Wired Devices Monitor on page 1183](#)
- [Top Users Monitor on page 1184](#)
- [Top APs by Traffic Monitor on page 1185](#)
- [Top Talker - Wireless Devices Monitor on page 1186](#)
- [RF Interference Sources Monitor for Devices on page 1187](#)

Error Trend Monitor

The Error Trend monitor displays inbound and outbound error trends on the node you selected in the View pane. This monitor is available in the Traffic tab.

This topic describes:

- [Error Trend on page 1168](#)
- [Error Trend Details on page 1168](#)

Error Trend

A line graph shows the rate inbound and outbound errors over time. The horizontal axis shows the times when samples were taken. The vertical axis shows errors per second.



NOTE: After a device is discovered, trend data does not appear immediately—it appears only after three polling periods have elapsed.

You can perform the following actions on the line graph:

- Change the time period over which to display the traffic trends by selecting a time period from the list in the upper right corner.
- Highlight a line in the graph by mousing over the line's legend.
- Remove or restore a line by clicking its legend.
- Display a numeric value by mousing over a data point.

Error Trend Details

The Error Trend details window displays detailed information about errors on the node you selected in the View pane. It contains the following elements:

- A line graph shows the rate of errors over time. The horizontal axis shows the times when samples were taken. The vertical axis shows errors.



NOTE: After a device is discovered, trend data does not appear immediately—it appears only after three polling periods have elapsed.

You can perform the following actions on the line graph:

- Change the time period over which to display the traffic trends by selecting a time period from the list in the upper right corner.
- Highlight a line in the graph by mousing over the line's legend.
- Remove or restore a line by clicking its legend.
- Display a numeric value by mousing over a data point.
- Error Trend Details table—Shows detailed information about the data gathered at each sample. For information about this table, see [Table 154 on page 1169](#)
- Error Trend Additional Details table—Shows additional error trend details and enables you to display them on the graph. For information about this table, see [Table 155 on page 1169](#).

Table 154: Error Trend Details Table

Column	Description
Time	Time when a data sample was taken from devices.
Errors In	Number of inbound errors reported in the sample.
Errors Out	Number of outbound errors reported in the sample.
CRC Errors In	Number of inbound cyclic redundancy check (CRC) errors reported in the sample.
CRC Errors Out	Number of outbound CRC errors reported in the sample.

Table 155: Error Trend Additional Details Table

Column	Description
Series Name	Name of the data series.
Series Value	Value of the data series.
Show	Select the check box to display the series on the graph. Clear the check box to remove the series from the graph.

Equipment Status Summary Monitor

The Equipment Status Summary monitor provides status highlights for the routers in the current scope. Both the summary and details show up to five available fields.

[Table 156 on page 1169](#) describes the fields in this monitor.

Table 156: Equipment Status Summary Fields

Field	Function	Default View
Device	Indicates the type of device.	Summary Details
Up	Indicates how many of the devices are up.	Summary Details
Down	Indicates how many of the devices are down.	Summary Details
Unknown	Indicates if the controller cannot identify the device.	Summary Details
Disabled	Indicates if the device is disabled.	Summary Details

Equipment Summary By Type Monitor

The Equipment Summary By Type monitor provides summary and detailed information about the type and number of devices in the scope selected in the View pane. This monitor is available on the Summary tab in Monitor mode.

Equipment Summary By Type

The summary view of the Equipment Summary By Type monitor shows the distribution of device types in the selected scope. Routers in a Virtual Chassis are counted separately from standalone routers.

Mouse over a segment of the pie chart to see the actual number of devices of that type. Click the details icon to open the Equipment Summary By Type Detail View window.

Equipment Summary By Type Details

The Equipment Summary By Type Detail View window provides details about the distribution of device types in the selected scope. Each table row represents a device type. Device types are defined by the combination of a device family, platform, and operating system version (for some device types). See [Table 157 on page 1170](#) for a description of the table columns.

Table 157: Equipment Summary By Type Detail View

Table Column	Description
Device Family	Device family.
Platform	Device platform.
OS Version	Operating system version running on the device.
Device Type	Device type.
Count	Number of devices of this platform in the selected scope.

Port Status Monitor

The Port Status monitor provides summary and detailed information about the status of the physical network interfaces for the selected node in the View pane.

If the selected node represents an individual device, the monitor displays data specific to the ports on the device. If the selected node contains multiple devices, the monitor displays data aggregated from all the ports on all the devices.

This topic describes:

- [Port Status Summary on page 1171](#)
- [Port Status Details on page 1171](#)

Port Status Summary

The summary view of the Port Status monitor displays two pie charts:

- Admin Status—Of the interfaces on the selected node, shows the proportion of interfaces that are administratively enabled and that are administratively disabled.
- Free vs Used—Of the network interfaces that are administratively enabled, shows the proportion of interfaces that are in use (operationally up) and that are not in use (operationally down).

Mouse over a pie segment to view the actual number of ports. Click the details icon to open the Port Status Details window.

Port Status Details

The Port Status Details table provides details about the physical network interfaces for the selected node, as shown in [Table 158 on page 1171](#).







NOTE: You must have a transceiver installed in an SFP, SFP+, or XFP port for information about the port to appear.

Table 158: Port Status Details Table

Field	Description
Port Name	The name of the physical interface.
MAC Address	<p>For standalone devices, the first five groups of hexadecimal digits are determined when the device is manufactured. The device then assigns a unique MAC address to each interface by assigning a unique identifier as the last group of hexadecimal digits.</p> <p>For Virtual Chassis members, the first four groups of hexadecimal digits are determined when the switch is manufactured. The fifth group of hexadecimal digits reflects the role of the member in the chassis, such as master or linecard.</p>
Serial Number	The hardware serial number of the device.
Host Name	The hostname of the device.
Description	A text description of the physical interface.
Current Negotiated Speed (Mbps)	The actual operating speed of the port, in megabits per second (Mbps). Depending on the results of autonegotiation, this speed might be less than the maximum speed supported by the port as indicated by port type.
Configured Speed	The speed configured for the port. If the speed is configured to be determined by autonegotiation, the configured speed is shown as Auto.
Duplex Mode	The duplex mode: full (full-duplex), half (half-duplex), or auto (autonegotiation).
Port Type	The port type (for example, 1 Gigabit Ethernet or 10 Gigabit Ethernet interface).

Table 158: Port Status Details Table (continued)

Field	Description
Admin Status	Indicates the administrative state of the port as  UP or  DOWN.
Operational Status	Indicates the operational status of the port as  UP or  DOWN.
Last Flap Time	Date and time at which the advertised link became unavailable, and then, available again.

Port Utilization Monitor

The Port Utilization Monitor displays a bar chart with information about the port traffic utilization on the node selected in the View pane. Each bar in the chart represents the port traffic utilization data gathered at a polling interval. The vertical axis shows the number of ports polled. The horizontal axis shows the time when each poll was taken. The data shown in the graph is aggregated from all the ports contained in the node selected in the View pane.

Each bar is divided into the following colored sections to indicate the distribution of port traffic utilization at the polling interval:

- Green indicates ports that operated at less than 50% of negotiated speed.
- Orange indicates ports that operated at between 50% and 80% of negotiated speed.
- Red indicates ports that operated at more than 80% of negotiated speed.

You can perform the following actions on the bar chart:

- Change the time period over which to display the data by selecting a time period from the list in the upper right corner.
- Remove or restore a utilization category (bar color) by clicking its legend.
- Display a numeric value by mousing over a bar.

Status Monitor for Routers

This monitor provides key information about the status for a standalone switch or a router when the device is selected in any of the views. This monitor is on the Equipment tab in Monitor mode.

[Table 159 on page 1172](#) describes the fields in this monitor.

Table 159: Status Monitor Fields

Field	Function
Serial Number	Indicates the hardware serial number of the device.

Table 159: Status Monitor Fields (continued)

Field	Function
IP Address	Indicates the IP address of the device.
Uptime	Indicates the amount of time since the last boot of the unit in days, hours, minutes, and seconds.
Status	Indicates whether the device is up or down.
Used MAC Addresses	Indicates the number of MAC addresses in use on the device.
Used VLANs	Indicates the number of VLAN memberships for this device.
Last Configured Time	Indicates the date and time when the device was last configured.
Temperature (°C)	Indicates the ambient temperature (in degrees Celsius).
Junos Version	Indicates the version and release level of Junos OS running on the device.

Traffic Trend Monitor

The Traffic Trend monitor displays inbound and outbound traffic trends on the node you selected in the View pane. This monitor is available in the Traffic tab. A line graph shows the rate of each type of traffic over time. The horizontal axis shows the times when samples were taken. The vertical axis shows the data rate, in packets per second.



NOTE: After a device is discovered, trend data does not appear immediately—it appears only after three polling periods have elapsed.

You can perform the following actions on the line graph:

- Change the time period over which to display the traffic trends by selecting a time period from the list in the upper right corner.
- Highlight a line in the graph by mousing over the line's legend.
- Remove or restore a line by clicking its legend.
- Display a numeric value by mousing over a data point.

Unicast vs Broadcast/Multicast Monitor

The Unicast vs Broadcast/Multicast monitor displays a pie chart of the current distribution of unicast, broadcast, and multicast traffic types on the node you selected in the View pane. This monitor is available in the Traffic tab.

The traffic is divided into these categories:

- Unicast inbound
- Unicast outbound
- Broadcast inbound
- Broadcast outbound
- Multicast inbound
- Multicast outbound

Mouse over a pie segment to view the actual number of packets.

Unicast vs Broadcast/Multicast Trend Monitor

The Unicast vs Broadcast/Multicast Trend monitor displays trends in the data rates of unicast, broadcast, and multicast traffic on the node you selected in the View pane. This monitor is available on the Traffic tab. A line graph shows the rate of each type of traffic over time. The horizontal axis shows the times when samples were taken. The vertical axis shows the data rate, in packets per second.



NOTE: After a device is discovered, trend data does not appear immediately—it appears only after three polling periods have elapsed.

The traffic is divided into these categories:

- Unicast inbound
- Unicast outbound
- Broadcast inbound
- Broadcast outbound
- Multicast inbound
- Multicast outbound

You can perform the following actions on the line graph:

- Change the time period over which to display the traffic trends by selecting a time period from the list in the upper right corner.
- Highlight a line in the graph by mousing over the line's legend.
- Remove or restore a line by clicking its legend.
- Display a numeric value by mousing over a data point.

Session Trends Monitor

The Session Trends monitor provides summary and detailed trend information about the number of active sessions and users within the node selected in the View pane.



NOTE: After a device is discovered, trend data does not appear immediately—it appears only after three polling periods have occurred.

- [Session Trends on page 1175](#)
- [Session Details on page 1175](#)

Session Trends

The summary view of the Session Trends monitor displays a line graph of the number of active sessions and users over time within the node selected in the View pane. The vertical axis is the number of active sessions or users. The horizontal axis shows the polling interval times.

You can perform the following actions on the line graph:

- Change the time period over which to display the trend data by selecting a time period from the list in the upper right corner.
- Select which SSID to monitor from the **Choose SSID** list.
- Select which VLAN to monitor from the **Choose VLAN** list. This option appears only when you have selected a switch in the View pane.
- Display the number of sessions or users at a polling interval by mousing over the plotted data point.
- Highlight a line in the graph by mousing over the line's legend.
- Remove or restore a line by clicking its legend.

Because data points plotted against the x-axis can represent data consolidated from multiple polling periods, three lines are plotted for session count and for user count: the maximum, minimum, and average counts that occurred during the consolidated polling periods.

Session Details

The Session Details window provides detailed trend information about the number of active sessions and users within the current node selected in the View pane. It contains these panes:

- The top pane contains a line graph of the number of active sessions and users over time within the node selected in the View pane.

You can perform the following actions on the line graph:

- Change the time period over which to display the trend data by selecting a time period from the list in the upper right corner.
- Display the number of sessions or users at a polling interval by mousing over the plotted data point.
- Highlight a line in the graph by mousing over the line's legend.
- Remove or restore a line by clicking its legend.

Because data points plotted against the x-axis can represent data consolidated from multiple polling periods, three lines are plotted for both session count and user count: the maximum, minimum, and average session and user counts that occurred during the consolidated polling periods.

- The bottom pane contains a table with detailed information about the active sessions.

The following table describes the columns that appear in current session details tables.

Table 160: User Session Details Table

Table Column	Description
User Name	Client's user name
MAC Address	Client's MAC address.
Device Type	Client's device type.
Device Group	Client's device group.
Device Profile	Client's device profile.
Controller IP	IP address of the controller to which the client is connected.
AP ID	ID of the wireless access point to which the client is connected.
AP NAME	Name of the wireless access point to which the client is connected.
SSID	SSID to which the wireless client is connected.
VLAN	VLAN to which the client is connected.
Client IP	Client's IP address.
Auth Type	Authorization type used for the client.
B/w[KBps]	Bandwidth used by the client.
Data Usage (KBytes)	Data transmitted and received by the client, in kilobytes.
Elapsed Time	Length of time the session has been active.

Table 160: User Session Details Table (continued)

Table Column	Description
Sample Time	Time when the most recent sample was taken.
RSSI	Received signal strength indication (RSSI). Specified in decibels referred to 1 milliwatt (dBm). A higher value indicates a stronger signal.
Roam In Time	The time when the session roamed in to the wireless access point.



TIP: Some table columns are hidden by default. To select which columns to display, mouse over any column heading, click the arrow that appears, mouse over **Columns** in the drop-down menu, and then select the columns to display from the list.

Current Sessions by Type Monitor

The Current Sessions by Type monitor provides summary and detailed information about the active sessions within the node selected in the View pane. This monitor is available in the Client tab.



NOTE: If the selected scope is a single switch, this monitor is named Current Sessions by VLAN, and shows the distribution of current sessions by VLAN.

- [Current Sessions by Type on page 1177](#)
- [Current Session Details on page 1177](#)

Current Sessions by Type

The summary view of the Current Sessions by Type monitor shows a pie chart of the active sessions within the node selected in the View pane. The chart shows the distribution of sessions by the session type. To change the session type shown in the monitor, select from the **Choose Sessions By Type** list.

Current Session Details

To see detailed information about the sessions in the Current Sessions monitor, click the **Details** button in the monitor title bar. The User Session Details window opens.

User Session Details Window

The User Session Details window provides information about the active sessions within the node selected in the View pane. To open this window, click the **Details** button in the Current Sessions or Current Sessions by Type monitors.

The following table describes the columns that appear in the user session details table:

Table 161: User Session Details Table

Table Column	Description
User Name	Client's user name
MAC Address	Client's MAC address.
Device Type	Client's device type.
Device Group	Client's device group.
Device Profile	Client's device profile.
Controller IP	IP address of the controller to which the client is connected.
AP ID	ID of the wireless access point to which the client is connected.
AP NAME	Name of the wireless access point to which the client is connected.
SSID	SSID to which the wireless client is connected.
VLAN	VLAN to which the client is connected.
Client IP	Client's IP address.
Auth Type	Authorization type used for the client.
B/w[KBps]	Bandwidth used by the client.
Data Usage (KBytes)	Data transmitted and received by the client, in kilobytes.
Elapsed Time	Length of time the session has been active.
Sample Time	Time when the most recent sample was taken.
RSSI	Received signal strength indication (RSSI). Specified in decibels referred to 1 milliwatt (dBm). A higher value indicates a stronger signal.
Roam In Time	The time when the session roamed in to the wireless access point.



TIP: Some table columns are hidden by default. To select which columns to display, mouse over any column heading, click the arrow that appears, mouse over **Columns** in the drop-down menu, and then select the columns to display from the list.

Current Active Alarms Monitor (All Views Except Service View)

The Current Active Alarms monitor shows any active alarm that has not yet been cleared. It is one of the four standard monitors available in Alarm mode. Current Active Alarms is a table that has four fields and appear by default. However, nine fields are available for selection. View [Table 162 on page 1179](#) for a description of the table.

Table 162: Current Active Alarms Monitor

Table Column	Description	Shown in Summary by Default	Shown in Detailed View by Default
Name	The alarm name.	Yes	Yes
ID	A system and sequentially-generated identification number.	No	No
Assigned To	If assigned to an individual, it shows the name of the person assigned; otherwise, it shows System to mark that the alarm is still unassigned.	No	Yes
Severity	The severity of the alarm. Severity levels are: <ul style="list-style-type: none"> • Critical—A critical condition exists; immediate action is necessary. • Major—A major error has occurred; escalate or notify as necessary. • Minor—A minor error has occurred; notify or monitor the condition. • Info—An informational message; no action is necessary. 	Yes	Yes
Entity ID	The identification of the entity responsible for causing this alarm. The Entity ID is the key for correlation of events into an alarm. The Entity ID could be a MAC address of a radio or an IP address of the device.	Yes	Yes
Source	The IP address of the device or network element that generated the alarm. The SNMP agent is located at the source IP. In most cases, the source IP is the IP address of the switch or controller.	No	No
Reporting Device	The hostname or IP address of the reporting device.	Yes	Yes
Creation Date	The date and time the alarm was first reported.	No	No
Last Updated	The date and time that the information for the alarm was last modified.	Yes	Yes
Updated By	Either the system or the last user who modified the alarm.	No	No

Clicking the Details icon opens Alarm Details where you can sort and disposition alarms by state (Acknowledged, Clear, Active).

Top Sessions by MAC Address Monitor

The Top Sessions by MAC Address monitor provides summary and detailed information about the sessions within the node you selected in the View pane that use the most bandwidth. This monitor is available in the Client tab.

This monitor includes only wireless network sessions, not sessions on wired connections. If the node you selected in the View pane contains only wired sessions, this monitor does not appear. If the node contains both wired and wireless sessions, only the wireless sessions appear in the monitor.

This topic describes:

- [Top Sessions on page 1180](#)
- [Top Session by MAC Details on page 1180](#)

Top Sessions

The summary view of the Top Sessions by MAC Address monitor displays a bar chart of the sessions within the node you selected in the View pane that consume the most bandwidth. The vertical axis shows the session MAC addresses. The horizontal axis shows different information depending on the time period you select in the list in the title bar:

- If you select the **Current** time period, the horizontal axis shows the session's incremental data usage.
- If you select any time period other than **Current**, the horizontal axis shows the session's total data usage.

You can mouse over a bar to see more information about that session. You can select which SSID to monitor from the **Choose SSID** list.

Top Session by MAC Details

The Top Session by MAC Details window displays detailed information about the top sessions within the node you selected in the View pane.

To change the number of top sessions displayed, select a number from the Top *N* list in the upper right corner.

To change the time period for which data is shown, select a time period from the time period list. By default, the Current time period is selected. When Current is selected, the data from the most recent polling period is shown. When any time period other than Current is selected, the data for the entire selected time period is shown.

The following table describes the columns that appear in Top Sessions by MAC Details table.

Table 163: Top Session Details Table

Table Column	Description
User Name	Client's user name To copy the text in this table cell: Click the cell, highlight the text, right-click the cell, and select Copy from the context menu.
MAC Address	Client's MAC address. To copy the text in this table cell: Click the cell, highlight the text, right-click the cell, and select Copy from the context menu.
Number of Sessions	Number of sessions.
AP Name	Name of the wireless access point to which the client is connected.
AP ID	ID of the wireless access point client is connected to.
Incremental Data Usage (KBytes)	The session's current incremental data usage. Appears only when the Current time period is selected.
Total Data Usage (KBytes)	The session's total data usage. Appears when any time period other than Current is selected.

Top APs by Session Monitor

The Top APs by Session monitor provides summary and detailed information about the wireless access points with the most active sessions within the node selected in the View pane. This monitor is available in the Client tab.

- [Top APs by Session Summary on page 1181](#)
- [Top APs by Session Details on page 1181](#)

Top APs by Session Summary

The summary view of the Top APs by Session monitor displays a bar chart of the wireless access points with the most active sessions within the node selected in the View pane. The wireless access points are shown on the vertical axis. The number of sessions is shown on the horizontal axis.

Top APs by Session Details

To see detailed information about the top wireless access points by sessions, click the **Details** button in the monitor title bar. [Table 164 on page 1181](#) describes the information in the Top APs by Sessions window.

Table 164: Top APs by Sessions Window

Column	Description
AP Name	Wireless access point name.

Table 164: Top APs by Sessions Window (continued)

Column	Description
Serial Number	Wireless access point serial number.
WLC Controller	Wireless controller that controls the wireless access point.
Location	Location of the wireless access point.
Number of Sessions	Number of active sessions on the wireless access point.
Bandwidth (KBytes)	Wireless access point bandwidth.

Radio Technology Type Statistics Monitor

The Radio Technology Type Statistics monitor provides summary and detailed information about the usage of radio technology types within the node selected in the View pane. This monitor is available on the Summary tab in Monitor mode.

- [Radio Technology Type Statistics Summary on page 1182](#)
- [Radio Technology Type Statistics Details on page 1183](#)

Radio Technology Type Statistics Summary

The summary view of the Radio Technology Type Statistics monitor shows summary information about the usage of radio technology types within the node selected in the View pane. Select the category of information to show from the Tech Type Params By list box at the bottom of the monitor. [Table 165 on page 1182](#) describes the information shown for each category.

Table 165: Radio Technology Type Statistics Summary Categories

Category	Description
Sessions by Technology Type	Shows a pie chart of the distribution of radio technologies among the active sessions. You can mouse over the slices of the pie chart to see additional information.
Users by Technology Type	Shows a pie chart of the distribution of radio technologies among the active users. A user is an account that authenticates to get network access. A user can have multiple active sessions by using multiple network devices with the same account. You can mouse over the slices of the pie chart to see additional information.
Average SNR by Technology Type	Shows a bar chart of the signal-to-noise ratio (SNR) of the current sessions. Select the radio technology type to show from the list to the left of the chart. The chart shows the number of sessions on the vertical axis and the SNR on the horizontal axis. The average SNR of all sessions on the chart is shown below the chart.
Bandwidth Usage by Technology Type	Shows a pie chart of the percentage of wireless bandwidth used by each radio technology. Mouse over the slices of the pie chart to see additional information.

Table 165: Radio Technology Type Statistics Summary Categories (continued)

Category	Description
Amount of Time (last 10 min)	Shows a bar chart of the amount of time each radio technology type has been continuously active on the network.

Radio Technology Type Statistics Details

To see detailed information about the radio technology type statistics, click the **Details** button in the monitor title bar. [Table 166 on page 1183](#) describes the information in the The Radio Type Statistics window.

Table 166: Radio Type Statistics Window

Column	Description
Tech Type	Radio technology type.
No. of Sessions	Number of sessions using the radio technology type.
No. of Users	Number of users using the radio technology type.
Users Percentage	Percentage of users using the radio technology type.
Bandwidth Usage	Bandwidth used by the radio technology type.
Bandwidth Percentage	Percentage of bandwidth used by the radio technology type.
Time Amount	Amount of time during the polling period when at least one session using that radio type was active. The maximum amount is the length of the polling period.
Time Percentage	Percentage of time during the polling period when at least one session using that radio type was active.
Average SNR	Average SNR for the radio technology type.

Top Talker - Wired Devices Monitor

The Top Talker - Wired Devices monitor provides summary and detailed information about the wired devices that are using the most bandwidth.

- [Top Talker - Wired Devices Summary on page 1183](#)
- [Top Talker - Wired Devices Details on page 1184](#)

Top Talker - Wired Devices Summary

The summary view of the Top Talker - Wired Devices monitor has a bar chart that shows summary information about the wired devices that are using the most bandwidth. Device names or addresses are listed on the vertical axis. Data usage in kilobytes is shown on the horizontal axis. You can mouse over a bar to see more information about that device.

Top Talker - Wired Devices Details

To see detailed information about the top talkers, click the **Details** button in the monitor title bar. The Top Talker - Wired Devices monitor details window has a table containing detailed information about the devices that are using the most bandwidth.

[Table 167 on page 1184](#) describes the columns in the table. To close the details page, click the **Minimize** button in the title bar.

Table 167: Top Hosts Monitor Details

Column	Description
Host Name	Host's host name.
MAC Address	Host's MAC address
Data Usage (KBytes)	Data used by the host, in kilobytes.
Device Serial Number	Device's serial number.

Top Users Monitor

The Top Users monitor provides summary and detailed information about the users within the node you selected in the View pane that use the most bandwidth. This monitor is available on the Client tab.

This monitor includes only wireless network users, not users on wired connections. If the node you select in the View pane contains only wired users, this monitor does not appear. If the node contains both wired and wireless users, only the wireless users appear in the monitor.

This topic describes:

- [Top Users on page 1184](#)
- [Top Session By User Details on page 1185](#)

Top Users

The summary view of the Top Users monitor displays a bar chart of the top bandwidth users within the node you selected in the View pane. The vertical axis shows the user names. The horizontal axis shows different information depending on the time period you select in the list in the title bar:

- If you select the **Current** time period, the horizontal axis shows the user's incremental data usage.
- If you select any time period other than **Current**, the horizontal axis shows the user's total data usage.

You can mouse over a bar to see more information about that user. You can select which SSID to monitor from the **Choose SSID** list.

Top Session By User Details

The Top Session By User Details window displays detailed information about the top users within the node you selected in the View pane.

To change the number of top users displayed, select a number from the Top *N* list in the upper right corner.

To change the time period for which data is shown, select a time period from the time period list. By default, the Current time period is selected. When Current is selected, the data from the most recent polling period is shown. When any time period other than Current is selected, the data for the entire selected time period is shown.

The following table describes the columns that appear in Top Session By Users Details table.

Table 168: Top Session Details Table

Table Column	Description
User Name	Client's user name To copy the text in this table cell: Click the cell, highlight the text, right-click the cell, and select Copy from the context menu.
MAC Address	Client's MAC address. To copy the text in this table cell: Click the cell, highlight the text, right-click the cell, and select Copy from the context menu.
Number of Sessions	Number of sessions.
AP Name	Name of the wireless access point to which the client is connected.
AP ID	ID of the wireless access point client is connected to.
Incremental Data Usage (KBytes)	The session's current incremental data usage. Appears only when the Current time period is selected.
Total Data Usage (KBytes)	The session's total data usage. Appears when any time period other than Current is selected.

Top APs by Traffic Monitor

The Top APs by Traffic monitor provides summary and detailed information about the wireless access points with the most traffic within the node selected in the View pane. This monitor is available on the Summary tab.

- [Top APs by Traffic Summary on page 1186](#)
- [Top APs by Traffic Details on page 1186](#)

Top APs by Traffic Summary

The summary view of the Top APs by Traffic monitor displays a bar chart of the wireless access points with the most traffic within the node selected in the View pane. The wireless access points are shown on the vertical axis. The traffic is shown on the horizontal axis.

Top APs by Traffic Details

To see detailed information about the top wireless access points by traffic, click the **Details** button in the monitor title bar. [Table 169 on page 1186](#) describes the information in the Top APs by Traffic Details window.

Table 169: Top APs by Traffic Details Window

Column	Description
AP Name	Wireless access point name.
Serial Number	Wireless access point serial number.
WLC Controller	Wireless controller that controls the wireless access point.
Location	Location of the wireless access point.
Number of Sessions	Number of active sessions on the wireless access point.
Bandwidth (KBytes)	Wireless access point bandwidth.

Top Talker - Wireless Devices Monitor

The Top Talker-Wireless Devices widget provides summary and detailed information about the top client device types that are generating wireless network traffic. Device types correspond to the platform or operating system of the device, for example, Windows or Android.

This topic describes:

- [Top Talker-Wireless Devices Summary on page 1186](#)
- [Top Talker-Wireless Devices Details on page 1187](#)

Top Talker-Wireless Devices Summary

The summary view of the Top Talker-Wireless Devices monitor has a bar chart showing summary information about the top client device types that are generating wireless network traffic. Device types are listed on the vertical axis. Data usage in kilobytes is shown on the horizontal axis. You can mouse over a bar to see more information about it, including the number of devices of that type.

Top Talker-Wireless Devices Details

To see detailed information about the Top Talker-Wireless Devices, click the **Details** button in the monitor title bar. The Top Talker-Wireless Devices monitor details window has a table containing detailed information about the top client device types that are generating wireless network traffic. [Table 170 on page 1187](#) describes the columns in the table.

Table 170: Top Talker-Wireless Devices Details Window

Column	Description
Number of Device(s)	Number of devices of the device type.
Device Type	Device type.
Data Usage (KBytes)	Data used by devices of the device type, in kilobytes.

RF Interference Sources Monitor for Devices

The RF Interference Sources monitor for wireless devices consists of a summary pie chart that reflects all wireless traffic experienced by the object selected in the View pane. You can select any one of the objects listed in [Table 171 on page 1187](#) in the view pane:

Table 171: Wireless Objects With Interference Tracking









Icon	Object
	Entire Wireless Network in any view.
	Wireless Mobility Domain in any view.
	Controller Cluster in any view. NOTE: You cannot see interference for a single controller.
	Individual access point in any view.
	Individual radio in any view.
	Selecting a floor in logical view displays all access points on that floor.
	Selecting a building in logical view displays all access points in that building.
	Selecting a site from the logical view displays all access points in that building.

Table 171: Wireless Objects With Interference Tracking (continued)

Icon	Object
	Wiring closet—to create a wiring closet.

Connectivity Services Director tracks and monitors interference from these sources:

- Microwave ovens—Most domestic microwave ovens use 2.45 GHz, and can interfere with Wi-Fi channels from 8 to 10 (or even 7 to 11). Interference varies depending on the model of the oven—for example, commercial restaurant microwave ovens sweep over a wider spectrum and have a higher duty cycle.
- Continuous wave devices continuously transmit at a particular frequency without attempting to share the radio frequency medium with other devices. Devices that use continuous wave technology in the same frequency bands as wireless LAN networks will interfere with wireless communications, reducing performance or totally preventing communication. Several examples of devices that may use continuous wave transmission that interferes with Wi-Fi are video surveillance cameras and baby monitors.
- Bluetooth devices
- Phone FHSS from cordless phones
- Unknown devices

To track these devices, Connectivity Services Director polls the controllers at the standard interval. The categories with the largest sections of the pie chart cause the most interference.

You can perform the following actions on the pie chart:

- Change the time period over which to display interference by selecting a time period from the list in the upper right corner.
- Display a numeric value for interference occurrences by mousing over a section of the chart.
- Click the monitor's title to see a list of interfering objects along with the information listed in [Table 172 on page 1188](#).

Table 172: Information on RF Interference Sources for a Radio

Information	Description
Last Seen	Date and time the interference was last detected.
Transmitter ID	If the interference is caused by an object with a MAC address, the MAC address is displayed. If the object has no MAC address, MSS calculates a MAC address, using the characteristics of the object. This way, you can correlate interference events over time.
Listener MAC	MAC address of the access point that detected the interference.

Table 172: Information on RF Interference Sources for a Radio (continued)

Information	Description
AP	Name of the access point that detected the interference.
Controller	Name of the controller that reported the interference.
Channel	Channel the interference affected.
RSSI	Received signal strength indication (RSSI), in decibels referred to 1 milliwatt (dBm). A higher value indicates a stronger signal.
Duty Cycle	Reported fraction of time that the source is emitting RF.
Source Type	Possible sources of interference include Bluetooth, Continuous Wave, Microwave Oven, Unknown, and Phone FHSS.
CIM (%)	Estimated severity of interference on this channel caused by the source.

Interference is frequently not a problem on wireless networks with light traffic, but as traffic becomes heavier, throughput and capacity decrease and other problems become apparent. RF interference can cause packet retransmission. Interference is also a security concern because jamming can bring down the network .

Ideally, interference retransmission does not cause more than 10% of the total number of packets sent. If your retransmission percentage is higher, you can try to lower it by:

- Locating and eliminating offending devices. If the item cannot be removed, you can add electromagnetic interference (EMI) shielding such as grounded mesh, foils, insulating foams, or insulating paint. This will limit the interference to a small area.
- Moving clients to channels with less interference. Keep in mind, however, that Bluetooth devices, cordless phones, 802.11FH devices, and jamming emissions are broadband, so it's not possible to change channels away from them—they are everywhere in the band.

Detecting and Examining the Health and Performance of Services

- [Service Monitoring Capabilities in Connectivity Services Director on page 1192](#)
- [Computation of Statistics Polled from Devices for Display in Widgets on Monitoring Pages on page 1193](#)
- [Configuring the Aggregation Method for Viewing Monitoring Details on page 1194](#)
- [Viewing the Service Monitoring Summary Page for a Consolidated Listing of Services on page 1196](#)
- [Monitoring the Service Summary Details of P2P Services for Optimal Debugging on page 1199](#)
- [Monitoring the Service Summary Details of VPLS Services for Optimal Debugging on page 1202](#)
- [Monitoring the Service Summary Details of Layer 3 VPN Services for Optimal Debugging on page 1206](#)
- [Monitoring the Service Traffic Statistics of P2P Services for Correlating Device Counters on page 1209](#)
- [Monitoring the Service Traffic Statistics of VPLS Services for Correlating Device Counters on page 1213](#)
- [Monitoring the Service Traffic Statistics of Layer 3 VPN Services for Correlating Device Counters on page 1215](#)
- [Monitoring the Service Transport Details of P2P Services for Easy Analysis on page 1218](#)
- [Monitoring the Service Transport Details of VPLS Services for Easy Analysis on page 1221](#)
- [Monitoring the Service Transport Details of Layer 3 VPN Services for Easy Analysis on page 1225](#)
- [Viewing Y.1731 Performance Monitoring Statistics for Point-to-Point Services on page 1229](#)
- [Viewing Y.1731 Performance Monitoring Statistics for VPLS Services on page 1233](#)
- [Clearing Interface Statistics on page 1237](#)
- [Viewing MAC Table Details on page 1239](#)
- [Viewing Interface Statistics on page 1241](#)
- [Viewing Interface Status Details on page 1243](#)
- [MPLS Connectivity Verification and Troubleshooting Methods on page 1245](#)

- [Using MPLS Ping on page 1247](#)
- [Pingging VPNs, VPLS, and Layer 2 Circuits on page 1249](#)
- [Monitoring Network Reachability by Using the MPLS Ping Capability on page 1250](#)
- [Monitoring Network Reachability by Using the Layer 3 VPN Ping Capability on page 1253](#)
- [Routing Table Overview on page 1256](#)
- [Viewing Routing Table Details on page 1256](#)

Service Monitoring Capabilities in Connectivity Services Director

In a network environment, a network administrator, operator, or a supervisor must be able to quickly and easily monitor the health (working condition), operating efficiency, traffic-handling capacity, and performance status of the managed devices and configured services to be able to take corrective action and restoration measures in case of device alarms, overload conditions, or traffic drops. Using the Monitor mode of the Connectivity Services Director application, you can monitor the managed services on devices, and collect and store the information from the devices in the Connectivity Services Director application database. The monitors or widgets are displayed to enable you to track, diagnose, and rectify discrepancies associated with services configured on devices. The information is displayed in easy-to-understand graphs and in tables that you can sort and filter, allowing you to quickly visualize the state of your network, spot trends developing over time, and find important details.. For example, you might observe that an L3VPN service is reported as down from the summarized information presented for that service on the monitoring page. This high-level view enables you to navigate to the settings for that service and fine-tune to function properly.

The following tabs are displayed when you click the Monitor icon in the Service View of the Connectivity Services Director banner.

- **ServiceSummary**—Displays the consolidated and cumulative status of a service. This tab is applicable for P2P, L3VPN, and VPLS services. The Connections monitor show the status of the connection or link (up or down) between peer devices. In the table displayed for this monitor, the row represents the source device and the column denotes the destination device. The status of the link is displayed for P2P and VPLS services. The Traffic Summary monitor represents the total Egress (Packets out) traffic passing through all the UNI or CE interfaces that are part of the cumulative services. It is displayed for point-to-point (P2P), Layer 3 VPN (L3VPN), and virtual private LAN (VPLS) services. The Current Active Alarms monitor shows any active alarm that has not yet been cleared
- **ServiceTransport**—Displays the transport or packet statistics for data against time between the source and destination devices that you select, and based on the LSP that is used by the endpoint. The source device is the row selected in the Connection Matrix widget on the Service Transport tab. The destination device is chosen from the Traffic Statistics widget on the Service Transport tab. By default, no destination devices are selected. Service transport statistical values are displayed for P2P, VPLS, and L3VPN services.
- **ServiceTraffic**—Displays the end-to-end traffic matrix that signifies the traffic between peer devices. You can view statistical counters and metrics for input packets, input

bytes, output packets, and output bytes. The Interface Statistics monitor shows traffic data on all the user-to-network interfaces (UNI) or site interfaces that are part of the service. These values are on-demand statistical values and the data is retrieved from the device directly without being cached (polling at periodic intervals and displaying a snapshot). This tab is supported for P2P, VPLS, and L3VPN services. The data is available only if queues are enabled on the interface.

- **ServicePerformance**—Displays frame delay, frame loss, frame delay variation, and service availability. These measurements are achieved by triggering a one-way delay, two-way delay, or loss. The performance measurement is useful for generating periodic service-level agreement conformance reports from the deployed network and for studying traffic patterns in the network over a period of time. In proactive mode, SLA measurements are triggered by an iterator application. An iterator is designed to periodically transmit SLA measurement packets in form of ITU-Y.1731-compliant frames for two-way delay measurement or loss measurement for each of the connections registered to it. Iterators make sure that measurement cycles do not occur at the same time for the same connection to avoid CPU overload. The iterator profiles are configured on remote MEP for measurement of Ethernet frame delay measurement (ETH-DM), Ethernet frame loss measurement (ETH-LM), and statistical frame loss (SFL).
- **LSP Summary**—Displays a comprehensive and cohesive view about the configured RSVP LSP service. The status of the LSP and the status of connections between the ingress router and egress routers in an LSP are displayed. The LSP status details are shown for the ingress router. You can also view the ingress, egress, and transit LSP information, such as the primary and secondary states.



NOTE: The values and statuses of the parameters displayed in the graphs and tables of different widgets are refreshed, based on the polling interval configured on the Monitoring tab of the Preferences page (accessible by clicking the down arrow beside the System button on the Connectivity Services Director banner and selecting Preferences).

Related Documentation

- [Configuring the Aggregation Method for Viewing Monitoring Details on page 1194](#)

Computation of Statistics Polled from Devices for Display in Widgets on Monitoring Pages

To interpret the statistical details and counters displayed in the charts and tables of the monitoring pages and in the tabular layouts, it is essential to understand the manner in which the metrics and values are retrieved from the devices and displayed in the GUI pages. In the charts, the time intervals are shown along the x-axis and data points or values of a particular attribute are shown along the y-axis. On the y-axis, the counter value displayed is the differential value between two polling intervals or the aggregated interval. For example, for the input packets of an interface, [Table 173 on page 1194](#) describes the mapping between polled and counter values.

Table 173: Mapping Between Polled Values and Counter Values Displayed in the GUI

Polling value from devices	456789	456800	456825	456840	456840
Counter value shown on the charts and tables	–	11	25	15	0

If the number of data points available between two intervals is more than one, the data is aggregated. The aggregation is based on the Connectivity Services Director application settings that you configure as preferences. One of the following types of statistical metrics can be viewed:

- Total—Sum of the number of packets in a specific time period
- Average—Average of the total number of packets in a specific time period

For example, for the input packets for an interface, the values described in [Table 174 on page 1194](#) illustrate the manner in which the differential values of counters are calculated for different time periods, based on the polling intervals that are used to retrieve details from the devices.

Table 174: Computation of Counters Using Polling Intervals

Polling Time	Start	10:30	10:45	11:00	11:15	11:30	11:45
Polling Counter Value	525	550	555	575	590	625	640
Packets Per Interval	–	25	5	20	15	35	15
Time Interval	–	10:45		11:15		11:45	
Counter Value (Average)	–	15		18		25	
Counter Value (Total)	–	50		45		50	

The number of actual data points varies between the minimum and maximum number of values, based on polling period and data availability. For the time values shown on the graph, the end time indicated is the time at which the last polling or retrieval of data occurred on the device. The interval between two data points is computed by using the total duration for which statistics is displayed by subtracting the period from the end time. The start time displayed is based on the number of intervals calculated by clocking backward from the end time.

Related Documentation

- [Configuring the Aggregation Method for Viewing Monitoring Details on page 1194](#)

Configuring the Aggregation Method for Viewing Monitoring Details

On the pages in Monitor mode of the Connectivity Services Director GUI that display statistical information and counters for traffic flow and packets across peer devices for

various services and device configuration settings, you can select the aggregation or cumulative method that must be used for computing and displaying statistics. You can also modify the application settings to display the aggregation of traffic.

The following two aggregation values are supported:

- **Total**—Sum of the number of packets received in the interval
- **Average**—Average of the total number of packets received in the interval

You can set the aggregation method from the Junos Space Platform GUI or the Connectivity Services Director GUI.

To configure the aggregation method from the Junos Space Platform GUI:

1. From the Network Management Platform task pane, select **Administration > Applications**.

The Applications page that appears displays a list of the applications in the Network Management platform.

2. Right-click Connectivity Services Director and select **Modify Applications Settings**.

The Modify Application Settings page that appears displays a list of the parameters that can be modified.

3. Click the **Monitoring** button to specify the settings.



NOTE: You cannot modify the application settings if another user is currently modifying them.

4. Select the **Perform Monitoring on failed Functional Audit** check box if you want the monitoring functionality to be enabled for services for which functional audit failed. Otherwise, monitoring data is displayed in the widgets in Monitor mode of Service View only on services for which functional audit succeeded.
5. In the Pseudowire Redundancy Transition TimeDelay field, specify the number of minutes after which a remote procedure call (RPC) must be sent from Connectivity Services Director to the device on which redundant pseudowires are configured for monitoring data to be collected.

By default, an RPC call is initiated every 2 minutes.

6. From the Statistics Aggregation Reporting list, select **Total** or **Average**.

The value of the aggregation method determines the manner in which the aggregated results are returned for a query that polls and retrieves data from devices.

7. Click **Modify** to save the changes that you made in the Connectivity Services Director application. Alternatively, click **Cancel** to retain the original settings.

The aggregation method setting is modified.

To configure the aggregation method from the Connectivity Services Director GUI:

1. To open the Preferences page, click the down arrow next to the **System** button on the Connectivity Services Director banner and select Preferences.

The Preferences page opens with User Preferences as the default tab.

2. Click the **Service Activation** tab.

The settings that you can configure for services activation are displayed.

3. From the Statistics Aggregation Reporting list, select **Total** or **Average**.

The aggregation method that you specified is used for computation of values on the monitoring pages.

4. Click **OK** to save the changes. Alternatively, click **Cancel** to discard the changes.

The aggregation method setting is saved.



NOTE: For the charts and tables displayed in Monitor mode of Service View, you can specify the polling interval and enable or disable the following collectors:

- ProvisioningMonitorInterfaceStatusCollector—Defines the polling interval for monitoring the interface status
 - ProvisioningMonitorInterfaceStatsCollector—Defines the polling interval for monitoring the interface statistics
 - ProvisioningMonitorServiceStatusCollector—Defines the polling interval for monitoring the service status
 - ProvisioningMonitorLDPStatsCollector—Defines the polling interval for monitoring the LDP statistics
 - ProvisioningMonitorY1731PMCollector—Defines the polling interval for monitoring the performance management or Y.1731 statistics
 - ProvisioningMonitorLSPStatsCollector—Defines the polling interval for monitoring the LSP statistics
-

**Related
Documentation**

- [Service Monitoring Capabilities in Connectivity Services Director on page 1192](#)
- [Configuring the Aggregation Method for Viewing Monitoring Details on page 1194](#)

Viewing the Service Monitoring Summary Page for a Consolidated Listing of Services

The Service Monitoring Summary page displays a consolidated view of all of the service instances for a particular service type. The customer associated with the service, type of service, service definition upon which the service order is based, the traffic rate in bits per second, and the traffic trend are displayed.



NOTE: The values and statuses of the parameters displayed in the graphs and tables of different widgets are refreshed, based on the polling interval configured on the Monitoring tab of the Preferences page (accessible by clicking the down arrow beside the System button on the Connectivity Services Director banner and selecting Preferences).

To view the Service Monitoring Summary page:

1. Select **Service View** from the View Selector.

The workspaces that are applicable to routing and tunneling services are displayed on the View pane.

2. From the Junos Space user interface, click the **Deploy** icon on the Connectivity Services Director banner.

The functionalities that you can configure in this mode are displayed on the task pane.

3. From the Service View pane, on the left, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.

The Network Services tree is expanded and displayed on the View pane.

4. Click the plus sign (+) beside Connectivity to view services based on protocols.

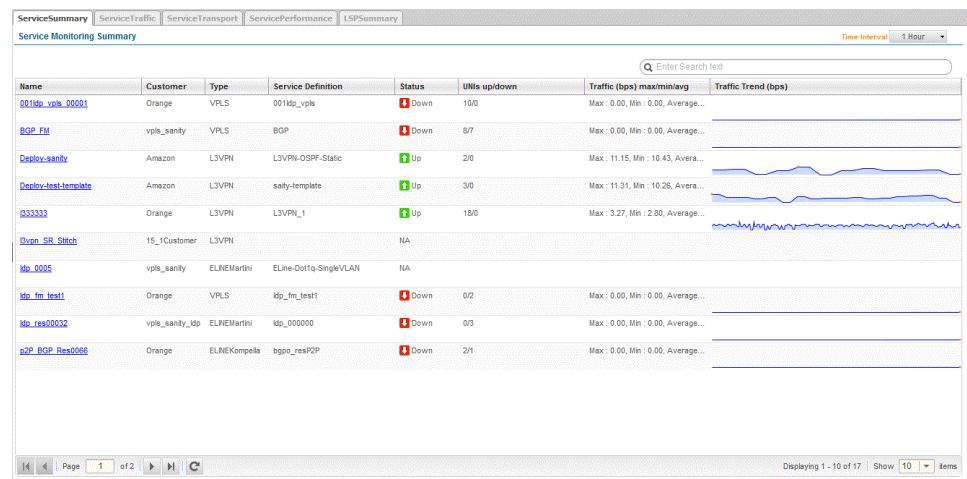
- Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
- Expand the **P2P Services** tree to select a point-to-point service.
- Expand the **VPLS Services** tree to select a VPLS service.

The Service Monitoring Summary page is displayed, if you do not select a particular service from the Service View pane and select the P2P Services, L3VPN Services, or VPLS Services term in the Service View pane.

5. Click the **ServiceSummary** tab.

The Service Monitoring Summary page is displayed.

Figure 52: Service Monitoring Summary Page



The following fields are displayed on this page:

- Name—Name of the configured service. Select the corresponding service from the Network Services > Connectivity tree on the View pane to navigate to the Service Summary page.
 - Customer—Name of the customer associated with the service.
 - Type—Service type, such as P2P, L3VPN, or VPLS.
 - Service Definition—Name of the service definition that is used to create the service.
 - Status—Whether the status is up or down. NA indicates that the status is not available for the corresponding service.
 - UNIs up/down—Number of user-to-network (ingress) interfaces that are in the up and down states.
 - Traffic (bps) max/min/avg—Maximum, minimum, and average rates of traffic handled by the service in bits per second (bps).
 - Traffic Trend (bps)—Line graph that signifies the rate of egress packets (packets that are sent out from an interface) in bps.
6. Select the service name from the Network Services > Connectivity tree on the View pane to view detailed information about the corresponding service.

The Service Summary page for the corresponding service is displayed.

You can view the consolidated and cumulative status or different types of services on the following tabs:

- ServiceSummary tab for P2P services—Displays the consolidated service status for P2P services
- ServiceSummary tab for VPLS services—Displays the consolidated service status for VPLS services

- ServiceSummary tab for L3VPN services—Displays the consolidated service status for L3VPN services

Related Documentation

- [Monitoring the Service Summary Details of P2P Services for Optimal Debugging on page 1199](#)
- [Monitoring the Service Summary Details of VPLS Services for Optimal Debugging on page 1202](#)
- [Monitoring the Service Summary Details of Layer 3 VPN Services for Optimal Debugging on page 1206](#)

Monitoring the Service Summary Details of P2P Services for Optimal Debugging

You can view the Service Summary page of a particular service to display the consolidated and cumulative status of a service. The overall information pertaining to the service that you can obtain from the different widgets displayed on this page enables you to navigate to the appropriate device or service settings page and modify the configuration parameters appropriately. You can view the connection between the different endpoints and also examine the statistics on the packets and bytes traversing through the endpoints. Using the Service Summary page, you can also select the source device for which you want to view the transport metrics and the traffic statistics on the other pages displayed in Monitor mode for the specific service. This page enables you to obtain an effective graphical view in the form of tables of statistics and charts to view the health and performance of devices and services in your network, which enables you to analyze and troubleshoot the parameters that are causing traffic-handling errors.



NOTE: The values and statuses of the parameters displayed in the graphs and tables of different widgets are refreshed, based on the polling interval configured on the Monitoring tab of the Preferences page (accessible by clicking the down arrow beside the System button on the Connectivity Services Director banner and selecting Preferences).

To view the Service Summary page for P2P services:

1. Select **Service View** from the View Selector.

The workspaces that are applicable to routing and tunneling services are displayed on the View pane.

2. From the Junos Space user interface, click the **Monitor** icon in the Connectivity Services Director banner.

The functionalities that you can configure in this mode are displayed on the task pane.

3. From the Service View pane, on the left, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.

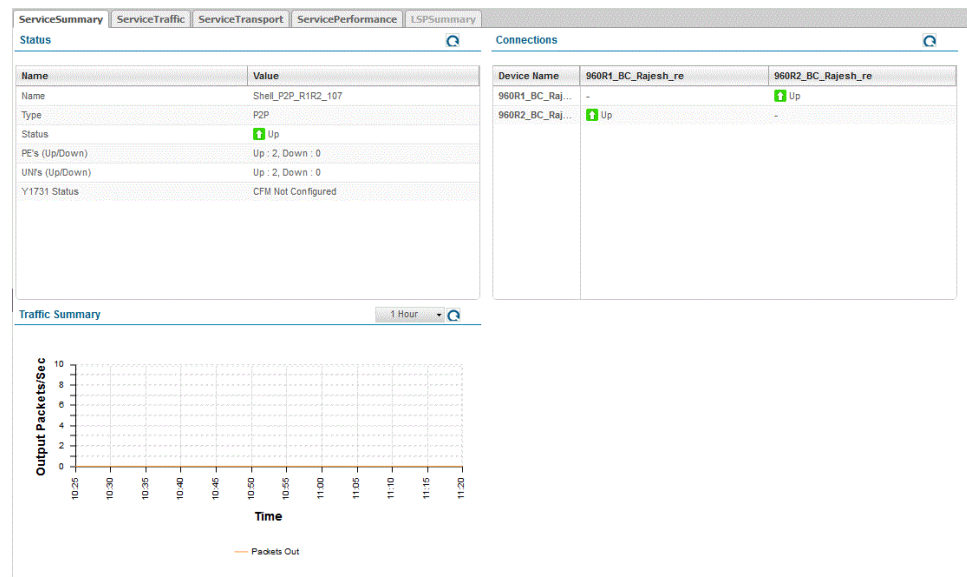
The Network Services tree is expanded and displayed on the View pane.

4. Click the plus sign (+) beside Connectivity to view services based on protocols.
5. Expand the **P2P Services** tree to select a point-to-point service.
6. From the main display area, click the **ServiceSummary** tab. The Service Summary page is displayed.



NOTE: The Service Monitoring Summary page is displayed, if you do not select a particular service from the Service View pane and select the P2P Services term in the Service View pane. The Summary page displays a consolidated view of all of the service instances for a particular service type. The customer associated with the service, type of service, service definition upon which the service order is based, the traffic rate in bits per second, and the traffic trend are displayed. Select the corresponding service from the Network Services > Connectivity tree on the View pane to navigate to the Service Summary page.

The following widgets are displayed on the Service Summary tab.



- [Service Status on page 1201](#)
- [Connections on page 1201](#)
- [Traffic Summary on page 1202](#)
- [Section on page ?](#)

Service Status

This widget displays the cumulative, consolidated status of services, such as P2P. The following fields are displayed in a tabular form in this widget:

- Name—Name of the service.
- Type—Protocol configured for the service, such as ELINE, VPLS, or L3VPN
- Status—Whether the service is up or down.
- PEs (Up/Down)—Number of provider edge devices that are in the up and down states
- UNIs (Up/Down)—Number of user-to-network (ingress) interfaces that are in the up and down states
- OSPF Neighbors—Number of OSPF neighbors
- BGP Neighbors—Number of BGP neighbors
- Local Switch—Whether the local switching mode to terminate multiple Layer 2 circuit pseudowires is configured.
- Y1731 Status—Whether the connectivity fault management (CFM) profile is configured for the service and whether performance monitoring (PM) statistics collection, such as one-way delay measurement and variation, two-way delay measurement and variation, or loss measurement are configured.

Click **Refresh** at the top of the monitor to update and display the contents of the table.

The Service Status monitor is also applicable for a P2P service with any one endpoint as an unmanaged device. For a P2P service, with unmanaged devices, the overall service status, PEs up/down, UNIs up/down, that are based on polling of only managed devices are displayed.

Connections

This monitor shows the status of connections between peer devices. In the tabular view, the row represents the source device and the columns denote the neighboring and destination devices. A green up-arrow in the indicates that the adjoining device in the network path to the destination device is operationally up. A red down-arrow indicates that the device is down. For the device for which the connection status is displayed, a value of NA is displayed under its own corresponding column to denote that it is not applicable. Click **Refresh** at the top of the monitor to update and display the contents of the table.

One of the following values is displayed on the columns that denote the adjacent and destination devices or endpoints:

- PR—Peer Device or Primary-Backup Pair. No Connection such as A/A or Z/Z.
- PBK—Peer Backup. No Connection.

- OL—No advertisement has been received for this virtual circuit from the neighbor. There is no outgoing label available for use by this virtual circuit.
- NA—Not available.

Mouse over the cells in the table to display the description of the connection statuses, such as PR, PBK or NA.

With a P2P service that contains an unmanaged endpoint, the Connections matrix represents the status from managed to unmanaged devices, based on the managed device polling. The connection status from unmanaged to managed is always displayed as NA.

Traffic Summary

This widget displays the total number of egress packets (packets that are sent out) or traffic passing through all the UNI or customer-edge (CE) interfaces associated with the particular service. This monitor is applicable for P2P services. The date and time at which the page was last updated is shown. A line graph is displayed with time on the horizontal axis and the number of output packets on the vertical axis.

From the Time Interval drop-down box, select **1 Hour**, **8 Hours**, **1 Day**, **1 Week**, **1 Month**, **3 Months**, **6 Months**, **1 Year**, or **Custom** to specify the duration for which the data polled from devices needs to be displayed. If you select the **Custom** option, the Time range popup dialog box is displayed. Specify the date from the calendar, and select the **Time From** (Start time in the 24-hour time format of collection of data), and **Time To** (End time in the 24-hour time format of collection of data). Click **OK** to save the settings. Else, click **Cancel** to discard the configuration.

For a P2P service with one endpoint as an unmanaged device, the Traffic Summary monitor represents the total egress traffic trend of only the managed devices. Unmanaged device traffic is not monitored.

Related Documentation

- [Viewing the Service Monitoring Summary Page for a Consolidated Listing of Services on page 1196](#)
- [Monitoring the Service Summary Details of VPLS Services for Optimal Debugging on page 1202](#)
- [Monitoring the Service Summary Details of Layer 3 VPN Services for Optimal Debugging on page 1206](#)

Monitoring the Service Summary Details of VPLS Services for Optimal Debugging

You can view the Service Summary page of a particular service to display the consolidated and cumulative status of a service. The overall information pertaining to the service that you can obtain from the different widgets displayed on this page enables you to navigate to the appropriate device or service settings page and modify the configuration parameters appropriately. You can view the connection between the different endpoints and also examine the statistics on the packets and bytes traversing through the endpoints. Using the Service Summary page, you can also select the source device for which you want to

view the transport metrics and the traffic statistics on the other pages displayed in Monitor mode for the specific service. This page enables you to obtain an effective graphical view in the form of tables of statistics and charts to view the health and performance of devices and services in your network, which enables you to analyze and troubleshoot the parameters that are causing traffic-handling errors.



NOTE: The values and statuses of the parameters displayed in the graphs and tables of different widgets are refreshed, based on the polling interval configured on the Monitoring tab of the Preferences page (accessible by clicking the down arrow beside the System button on the Connectivity Services Director banner and selecting Preferences).

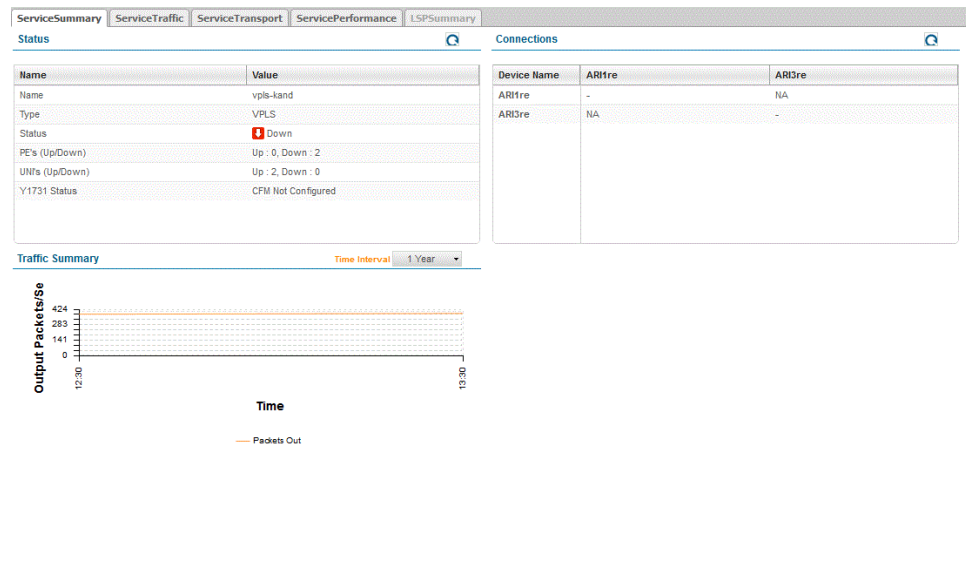
To view the Service Summary page for VPLS services:

1. Select **Service View** from the View Selector.
The workspaces that are applicable to routing and tunneling services are displayed on the View pane.
2. From the Junos Space user interface, click the **Monitor** icon on the Connectivity Services Director banner.
The functionalities that you can configure in this mode are displayed on the task pane.
3. From the Service View pane, on the left, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
The Network Services tree is expanded and displayed on the View pane.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
The Connectivity tree is expanded and displayed on the View pane.
5. Expand the **VPLS Services** tree to select a VPLS service.
6. Click the **ServiceSummary** tab. The Service Summary page is displayed.



NOTE: The Service Monitoring Summary page is displayed, if you do not select a particular service from the Service View pane and select the VPLS Services term in the Service View pane. The Summary page displays a consolidated view of all of the service instances for a particular service type. The customer associated with the service, type of service, service definition upon which the service order is based, the traffic rate in bits per second, and the traffic trend are displayed. Select the corresponding service from the Network Services > Connectivity tree on the View pane to navigate to the Service Summary page.

The following figure shows the Service Summary tab for a VPLS service.



The following widgets or widgets are displayed under this tab for VPLS services. These statistical counters and metrics enable you to view an agglomerative, cohesive snapshot of the service configured on a device.

- [Service Status on page 1204](#)
- [Connections on page 1205](#)
- [Traffic Summary on page 1205](#)

Service Status

This widget displays the cumulative, consolidated status of services, such as VPLS. The following fields are displayed in a tabular form in this widget:

- **Name**—Name of the service.
- **Type**—Protocol configured for the service, such as ELINE, VPLS, or L3VPN.
- **Status**—Whether the service is up or down. A green up-arrow indicates that the adjoining device in the network path to the destination device is operationally up. A red down-arrow indicates that the device is down.
- **PEs (Up/Down)**—Number of provider edge devices that are in the up and down states
- **UNIs (Up/Down)**—Number of user-to-network (ingress) interfaces that are in the up and down states
- **Local Switch**—Whether the local switching mode to terminate multiple Layer 2 circuit pseudowires is configured
- **Y1731 Status**—Whether the connectivity fault management (CFM) profile is configured for the service and whether performance monitoring (PM) statistics collection, such

as one-way delay measurement and variation, two-way delay measurement and variation, or loss measurement are configured.

Click **Refresh** at the top of the monitor to update and display the contents of the table.

Connections

This monitor shows the status of connections between peer devices. In the tabular view, the row represents the source device and the columns denote the neighboring and destination devices. This monitor is applicable for VPLS services.

One of the following values is displayed on the columns that denote the adjacent and destination devices or endpoints:

- PR—Peer Device. Primary-Backup Pair. No Connection such as A/A or Z/Z.
- PBK—Peer Backup. No Connection.
- OL—No advertisement has been received for this virtual circuit from the neighbor. There is no outgoing label available for use by this virtual circuit.
- NA—Not available.

Mouse over the cells in the table to display the description of the connection statuses, such as PR, PBK or NA.

For the device for which the connection status is displayed, a hyphen (-) is displayed under its own corresponding column to denote that it is not applicable. Click **Refresh** at the top of the monitor to update and display the contents of the table.

Traffic Summary

This widget displays the total number of egress packets (packets that are sent out) or traffic passing through all the UNI or customer-edge (CE) interfaces associated with the particular service. This monitor is valid for VPLS services. The date and time at which the page was last updated is shown. A line graph is displayed with time on the horizontal axis and the number of output packets on the vertical axis.

From the Time Interval drop-down box, select **1 Hour**, **8 Hours**, **1 Day**, **1 Week**, **1 Month**, **3 Months**, **6 Months**, **1 Year**, or **Custom** to specify the duration for which the data polled from devices needs to be displayed. If you select the **Custom** option, the Time range popup dialog box is displayed. Specify the date from the calendar, and select the **Time From** (Start time in the 24-hour time format of collection of data), and **Time To** (End time in the 24-hour time format of collection of data). Click **OK** to save the settings. Else, click **Cancel** to discard the configuration.

Related Documentation

- [Viewing the Service Monitoring Summary Page for a Consolidated Listing of Services on page 1196](#)
- [Monitoring the Service Summary Details of P2P Services for Optimal Debugging on page 1199](#)
- [Monitoring the Service Summary Details of Layer 3 VPN Services for Optimal Debugging on page 1206](#)

Monitoring the Service Summary Details of Layer 3 VPN Services for Optimal Debugging

You can view the Service Summary page of a particular service to display the consolidated and cumulative status of a service. The overall information pertaining to the service that you can obtain from the different widgets displayed on this page enables you to navigate to the appropriate device or service settings page and modify the configuration parameters appropriately. You can view the connection between the different endpoints and also examine the statistics on the packets and bytes traversing through the endpoints. Using the Service Summary page, you can also select the source device for which you want to view the transport metrics and the traffic statistics on the other pages displayed in Monitor mode for the specific service. This page enables you to obtain an effective graphical view in the form of tables of statistics and charts to view the health and performance of devices and services in your network, which enables you to analyze and troubleshoot the parameters that are causing traffic-handling errors.



NOTE: The values and statuses of the parameters displayed in the graphs and tables of different widgets are refreshed, based on the polling interval configured on the Monitoring tab of the Preferences page (accessible by clicking the down arrow beside the System button on the Connectivity Services Director banner and selecting Preferences).

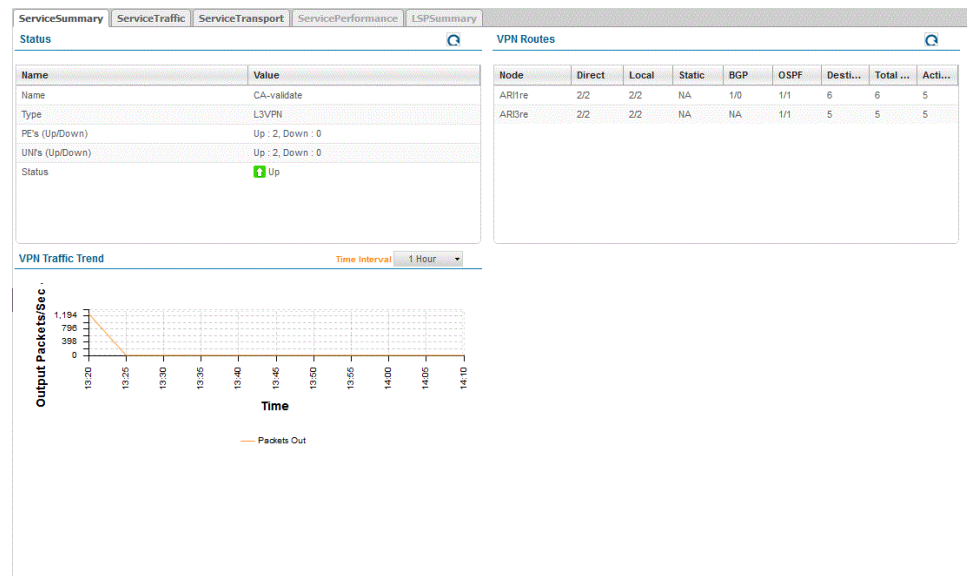
To view the Service Summary page for L3VPN services:

1. Select **Service View** from the View Selector.
The workspaces that are applicable to routing and tunneling services are displayed on the View pane.
2. From the Junos Space user interface, click the **Monitor** icon on the Connectivity Services Director banner.
The functionalities that you can configure in this mode are displayed on the task pane.
3. From the Service View pane, on the left, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
The Network Services tree is expanded and displayed on the View pane.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
The Connectivity tree is expanded and displayed on the View pane.
5. Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
6. Click the **ServiceSummary** tab.
The Service Summary page is displayed.



NOTE: The Service Monitoring Summary page is displayed, if you do not select a particular service from the Service View pane and select the L3VPN Services term in the Service View pane. The Summary page displays a consolidated view of all of the service instances for a particular service type. The customer associated with the service, type of service, service definition upon which the service order is based, the traffic rate in bits per second, and the traffic trend are displayed. Select the corresponding service from the Network Services > Connectivity tree on the View pane to navigate to the Service Summary page.

The following widgets or widgets are displayed under this tab for L3VPN services. These statistical counters and metrics enable you to view an agglomerative snapshot of the service configured on a device.



- [Service Status on page 1207](#)
- [VPN Routes on page 1208](#)
- [VPN Traffic Trend on page 1208](#)

Service Status

This widget displays the operational status of L3VPN services. The following fields are displayed in a tabular form in this widget:

- Name—Name of the service
- Type—Protocol configured for the service
- Status—Whether the service is up or down.

Click **Refresh** at the top of the monitor to update and display the contents of the table.

VPN Routes

This monitor shows the status of routers between peer devices in a VPN connection. The following fields are displayed in a tabular form:

- **Node**—Name of the device configured in a VPN tunnel
- **Direct**—Number of direct routes in the VPN tunnel for the specified node or device that are up and down
- **Local**—Number of local routes in the VPN tunnel for the specified node or device that are up and down
- **Static**—Number of static routes in the VPN tunnel for the specified node or device that are up and down
- **BGP**—Number of BGP routes in the VPN tunnel for the specified node or device that are up and down (BGP routing information includes the complete route to each destination)
- **OSPF**—Number of OSPF routes in the VPN tunnel for the specified node or device that are up and down (OSPF routes IP packets based solely on the destination IP address contained in the IP packet header)
- **Destination Count**—Number of destinations for which there are routes in the routing table.
- **Total Route Count**—Number of routes in the routing table and total number of routes in the following states:
 - active (routes that are active)
 - holddown (routes that are in the pending state before being declared inactive)
 - hidden (routes that are not used because of a routing policy)
- **Active Route Count**—Number of VPN routes that are active

Click **Refresh** at the top of the monitor to update and display the contents of the table.

VPN Traffic Trend

This widget displays the total number of egress packets (packets that are sent out) or traffic passing through all the UNI or customer-edge (CE) interfaces associated with the particular service. The date and time at which the page was last updated is shown. A line graph is displayed with time on the horizontal axis and the number of output bytes on the vertical axis.

From the Time Interval drop-down box, select **1 Hour**, **8 Hours**, **1 Day**, **1 Week**, **1 Month**, **3 Months**, **6 Months**, **1 Year**, or **Custom** to specify the duration for which the data polled from devices needs to be displayed. If you select the **Custom** option, the Time range popup dialog box is displayed. Specify the date from the calendar, and select the **Time From** (Start time in the 24-hour time format of collection of data), and **Time To** (End time in the 24-hour time format of collection of data). Click **OK** to save the settings. Else, click **Cancel** to discard the configuration.

- Related Documentation**
- [Viewing the Service Monitoring Summary Page for a Consolidated Listing of Services on page 1196](#)
 - [Monitoring the Service Summary Details of P2P Services for Optimal Debugging on page 1199](#)
 - [Monitoring the Service Summary Details of VPLS Services for Optimal Debugging on page 1202](#)

Monitoring the Service Traffic Statistics of P2P Services for Correlating Device Counters

You can view the Service Traffic page of a specific service to examine and diagnose the transmission details of packets and the metrics on forwarded or received packets. The interface statistical counters display the number of packets and bytes sent and received from interfaces that are associated with the devices of the service. A pictorial representation of the links in a point-to-point service topology is also shown. You can also view a bar chart of the class-of-service (CoS) queue information for physical interfaces. For rate-limited interfaces hosted on Modular Interface Cards (MICs), Modular Port Concentrators (MPCs), or Enhanced Queuing DPCs, rate-limit packet-drop operations occur before packets are queued for transmission scheduling. For such interfaces, the statistics for queued traffic do not include the packets that have already been dropped due to rate limiting, and consequently the displayed statistics for queued traffic are the same as the displayed statistics for transmitted traffic.

For rate-limited interfaces hosted on other types of hardware, rate-limit packet-drop operations occur after packets are queued for transmission scheduling. For these other interface types, the statistics for queued traffic include the packets that are later dropped due to rate limiting, and consequently the displayed statistics for queued traffic equals the sum of the statistics for transmitted and rate-limited traffic.



NOTE: The values and statuses of the parameters displayed in the graphs and tables of different widgets are refreshed, based on the polling interval configured on the Monitoring tab of the Preferences page (accessible by clicking the down arrow beside the System button on the Connectivity Services Director banner and selecting Preferences).

To view the Service Traffic page for P2P services:

1. Select **Service View** from the View Selector.
The workspaces that are applicable to routing and tunneling services are displayed on the View pane.
2. From the Junos Space user interface, click the **Monitor** icon on the Connectivity Services Director banner.
The functionalities that you can configure in this mode are displayed on the task pane.

- From the Service View pane, on the left, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.

The Network Services tree is expanded and displayed on the View pane.

- Click the plus sign (+) beside Connectivity to view services based on protocols.

The Connectivity tree is expanded and displayed on the View pane.

- Expand the **P2P Services** tree to select a point-to-point service.

- Click the **ServiceTraffic** tab.

The Service Traffic page is displayed.

The following widgets are displayed on the Service Traffic tab.

- [Traffic Graph on page 1210](#)
- [Pseudowire Traffic on page 1211](#)
- [Interface Traffic Statistics/Endpoint Users on page 1212](#)

Figure 53 on page 1210 shows the Service Traffic tab for a point-to-point service.

Figure 53: Service Traffic Page for a P2P Service



Traffic Graph

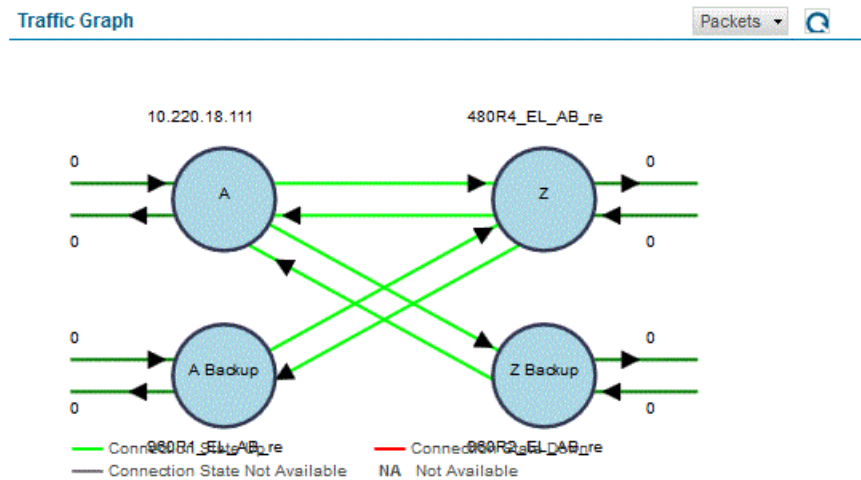
The Traffic Graph monitor displays the number of packets transmitted between the peer devices. A table is shown with the row representing the source device and the columns denoting the devices or network elements in the path up to the destination device. It is applicable for P2P services. From the Statistics Type drop-down list, select Packets or Bytes to display metrics corresponding to the selected parameter.

The Traffic Graph monitor for P2P services is displayed in a pictorial form, with the primary origin or A endpoint, backup origin or A endpoint, primary destination or Z endpoint, and backup destination or Z endpoints shown as circles. Color-coded legends reference the lines that are shown in the graph. The lines correspond to the traffic traversing from the A primary endpoint to the Z primary endpoints, from the A primary endpoint to the Z backup endpoint, and from the Z primary and Z backup endpoints to the A primary endpoint. The arrows indicate the direction of traffic flows. Red lines denote the Layer 2 Ethernet pseudowire traffic between the endpoints to have been dropped or the connection to be down. Green lines denote the pseudowire traffic to be transmitted successfully or the connection to be up. A gray line denotes that connection state is not available, and NA indicates that the statistic is not available. Solid lines denote the connections between primary pseudowires, while dotted lines denote the connections between secondary pseudowires. The numbers that are shown on the connection lines signify the metrics or count corresponding to the type of parameter you selected, such as output packets or output bytes.

On the Service Traffic page, the Traffic Graph monitor is also supported for a P2P service with one endpoint as unmanaged device.

For a P2P service with resiliency, for the redundant pseudowires configured to remote PE routers from the A primary or source endpoint, the traffic statistics for the primary pseudowire over which customer traffic is being transmitted and the backup pseudowire are displayed along the connection lines.

Figure 54: Traffic Graph Monitor for P2P Service with Resiliency



Pseudowire Traffic

This monitor is displayed for P2P services. A line chart is displayed with time on the horizontal axis and the number of output packets or output bytes on the vertical axis. From the Statistics Type drop-down box at the top of the monitor, select Input Packets or Input Bytes to display the number of packets or bytes traversing in the ingress direction (received traffic). Alternatively, select Output Packets/Second or Output Bytes/Second to display metrics corresponding to the transmitted or egress packets or bytes. From the

Select Primary Endpoint list, select the primary endpoint or device for which you want to view the traffic details traversing through the pseudowire in the output direction.

From the Time Interval drop-down box, select 1 Hour, 8 Hours, 1 Day, 1 Week, 1 Month, 3 Months, 6 Months, 1 Year, or Custom to specify the duration for which the data polled from devices needs to be displayed. If you select the Custom option, the Time range popup dialog box is displayed. Specify the date from the calendar, and select the Time From (Start time in the 24-hour time format of collection of data), and Time To (End time in the 24-hour time format of collection of data). Click OK to save the settings. Else, click Cancel to discard the configuration.

Interface Traffic Statistics/Endpoint Users

This monitor is displayed for P2P services. In this monitor, the interface statistics denote the traffic data on all the UNI or site interfaces associated with the service. These values are on-demand statistical values and the data is retrieved from the device directly without being cached (polling at periodic intervals and displaying a snapshot). It is supported for P2P, VPLS, and L3VPN services. The following fields are displayed in a table:

- Device Name—Name of the device
- Interface—Name of the interface
- Packets In—Number of packets received on the interface
- Packets Out—Number of packets sent from the interface
- Bytes In—Number of bytes received on the interface
- Bytes Out—Number of bytes sent from the interface

From the Automatic Refresh list, select **Disabled**, **Every 30 Seconds**, **Every 45 Seconds**, or **Every 1 Minute** to specify the frequency at which the statistics in the table must be updated and displayed. When you disable the auto-refresh capability, the page is not refreshed periodically by itself; instead you can click the **Refresh** icon to update the table contents for viewing.

For a P2P service with one endpoint as unmanaged device, the Interface statistics monitor displays only the managed devices in the list and the corresponding monitored data. Unmanaged devices or its data are not displayed.

Related Documentation

- [Monitoring the Service Traffic Statistics of VPLS Services for Correlating Device Counters on page 1213](#)
- [Monitoring the Service Traffic Statistics of Layer 3 VPN Services for Correlating Device Counters on page 1215](#)
- [Monitoring the Service Transport Details of P2P Services for Easy Analysis on page 1218](#)
- [Monitoring the Service Transport Details of VPLS Services for Easy Analysis on page 1221](#)
- [Monitoring the Service Transport Details of Layer 3 VPN Services for Easy Analysis on page 1225](#)

Monitoring the Service Traffic Statistics of VPLS Services for Correlating Device Counters

You can view the Service Traffic page of a specific service to examine and diagnose the transmission details of packets and the metrics on forwarded or received packets. The interface statistical counters display the number of packets and bytes sent and received from interfaces that are associated with the devices of the service. A pictorial representation of the links in a point-to-point service topology is also shown. You can also view a bar chart of the class-of-service (CoS) queue information for physical interfaces. For rate-limited interfaces hosted on Modular Interface Cards (MICs), Modular Port Concentrators (MPCs), or Enhanced Queuing DPCs, rate-limit packet-drop operations occur before packets are queued for transmission scheduling. For such interfaces, the statistics for queued traffic do not include the packets that have already been dropped due to rate limiting, and consequently the displayed statistics for queued traffic are the same as the displayed statistics for transmitted traffic.

For rate-limited interfaces hosted on other types of hardware, rate-limit packet-drop operations occur after packets are queued for transmission scheduling. For these other interface types, the statistics for queued traffic include the packets that are later dropped due to rate limiting, and consequently the displayed statistics for queued traffic equals the sum of the statistics for transmitted and rate-limited traffic.



NOTE: The values and statuses of the parameters displayed in the graphs and tables of different widgets are refreshed, based on the polling interval configured on the Monitoring tab of the Preferences page (accessible by clicking the down arrow beside the System button on the Connectivity Services Director banner and selecting Preferences).

To view the Service Traffic page for VPLS services:

1. Select **Service View** from the View Selector.
The workspaces that are applicable to routing and tunneling services are displayed on the View pane.
2. From the Junos Space user interface, click the **Monitor** icon on the Connectivity Services Director banner.
The functionalities that you can configure in this mode are displayed on the task pane.
3. From the Service View pane, on the left, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
The Network Services tree is expanded and displayed on the View pane.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
The Connectivity tree is expanded and displayed on the View pane.

5. Expand the **VPLS Services** tree to select a VPLS service.

6. Click the **ServiceTraffic** tab.

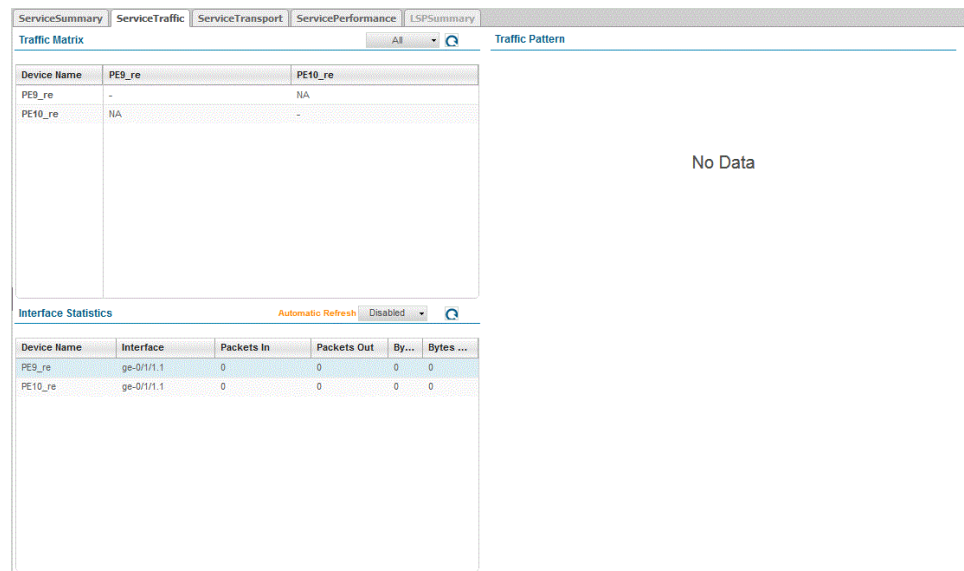
The Service Traffic page is displayed.

The following widgets are displayed on the Service Traffic tab.

- [Traffic Graph on page 1210](#)
- [Interface Traffic Statistics/Endpoint Users on page 1212](#)
- [Traffic Pattern on page 1215](#)

Figure 55 on page 1214 shows the Service Traffic tab for a VPLS service.

Figure 55: Service Traffic Page for a VPLS Service



Traffic Matrix

The Traffic Matrix monitor displays the number of packets transmitted between the peer devices. A table is shown with the row representing the source device and the columns denoting the devices or network elements in the path up to the destination device. It is applicable for VPLS services. From the Statistics Type drop-down list, select Unicast Bytes, Multicast Bytes, Broadcast Bytes, or Flooded Bytes to display metrics corresponding to the selected parameter.

Interface Statistics

This monitor is displayed for VPLS services. In this monitor, the interface statistics denote the traffic data on all the UNI or site interfaces associated with the service. These values are on-demand statistical values and the data is retrieved from the device directly without being cached (polling at periodic intervals and displaying a snapshot). It is supported for P2P, VPLS, and L3VPN services. The following fields are displayed in a table:

- Device Name—Name of the device
- Interface—Name of the interface
- Packets In—Number of packets received on the interface
- Packets Out—Number of packets sent from the interface
- Bytes In—Number of bytes received on the interface
- Bytes Out—Number of bytes sent from the interface

From the Automatic Refresh list, select **Disabled**, **Every 30 Seconds**, **Every 45 Seconds**, or **Every 1 Minute** to specify the frequency at which the statistics in the table must be updated and displayed. When you disable the auto-refresh capability, the page is not refreshed periodically by itself; instead you can click the **Refresh** icon to update the table contents for viewing.

Traffic Pattern

This monitor is displayed for VPLS services. A chord graphic displays the relationship among a set of entities. The association in the form of chords for traffic traversing through devices on which the service is assigned is shown.

Related Documentation

- [Monitoring the Service Traffic Statistics of P2P Services for Correlating Device Counters on page 1209](#)
- [Monitoring the Service Traffic Statistics of Layer 3 VPN Services for Correlating Device Counters on page 1215](#)
- [Monitoring the Service Transport Details of P2P Services for Easy Analysis on page 1218](#)
- [Monitoring the Service Transport Details of VPLS Services for Easy Analysis on page 1221](#)
- [Monitoring the Service Transport Details of Layer 3 VPN Services for Easy Analysis on page 1225](#)

Monitoring the Service Traffic Statistics of Layer 3 VPN Services for Correlating Device Counters

You can view the Service Traffic page of a specific service to examine and diagnose the transmission details of packets and the metrics on forwarded or received packets. The interface statistical counters display the number of packets and bytes sent and received from interfaces that are associated with the devices of the service. A pictorial representation of the links in a point-to-point service topology is also shown. You can also view a bar chart of the class-of-service (CoS) queue information for physical interfaces. For rate-limited interfaces hosted on Modular Interface Cards (MICs), Modular Port Concentrators (MPCs), or Enhanced Queuing DPCs, rate-limit packet-drop operations occur before packets are queued for transmission scheduling. For such interfaces, the statistics for queued traffic do not include the packets that have already been dropped due to rate limiting, and consequently the displayed statistics for queued traffic are the same as the displayed statistics for transmitted traffic.

For rate-limited interfaces hosted on other types of hardware, rate-limit packet-drop operations occur after packets are queued for transmission scheduling. For these other interface types, the statistics for queued traffic include the packets that are later dropped due to rate limiting, and consequently the displayed statistics for queued traffic equals the sum of the statistics for transmitted and rate-limited traffic.



NOTE: The values and statuses of the parameters displayed in the graphs and tables of different widgets are refreshed, based on the polling interval configured on the Monitoring tab of the Preferences page (accessible by clicking the down arrow beside the System button on the Connectivity Services Director banner and selecting Preferences).

To view the Service Traffic page for an L3VPN service:

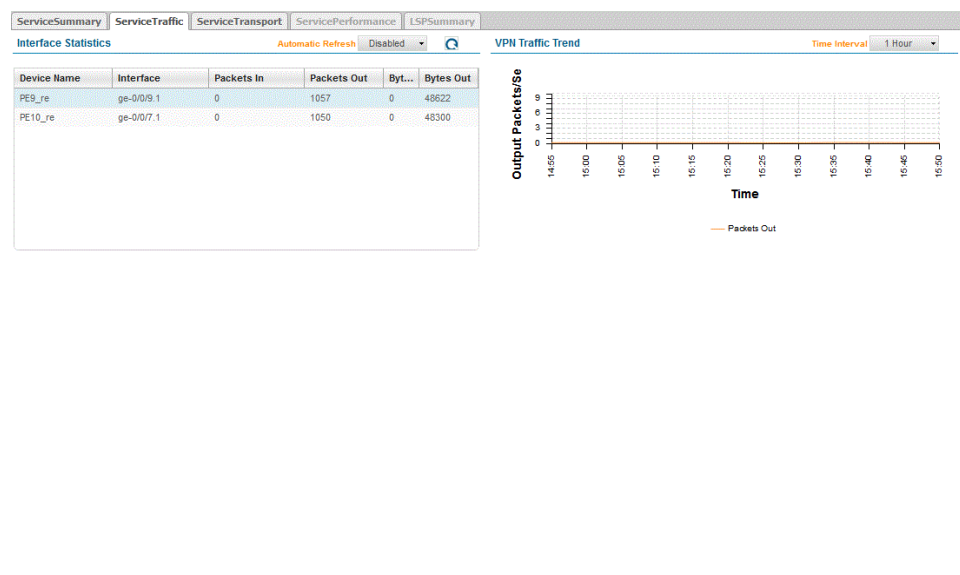
1. Select **Service View** from the View Selector.
The workspaces that are applicable to routing and tunneling services are displayed on the View pane.
2. From the Junos Space user interface, click the **Monitor** icon on the Connectivity Services Director banner.
The functionalities that you can configure in this mode are displayed on the task pane.
3. From the Service View pane, on the left, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
The Network Services tree is expanded and displayed on the View pane.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
The Connectivity tree is expanded and displayed on the View pane.
5. Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
6. Click the **ServiceTraffic** tab.
The Service Traffic page is displayed.

The following widgets are displayed on the Service Traffic tab.

- [Interface Traffic Statistics/Endpoint Users on page 1212](#)
- [VPN Traffic Trend on page 1217](#)

[Figure 56 on page 1217](#) shows the Service Traffic tab for an L3VPN service.

Figure 56: Service Traffic Page for an L3VPN Service



Interface Statistics

This monitor is displayed for Layer 3 VPN services. In this monitor, the interface statistics denote the traffic data on all the UNI or site interfaces associated with the service. These values are on-demand statistical values and the data is retrieved from the device directly without being cached (polling at periodic intervals and displaying a snapshot). It is supported for L3VPN services. The following fields are displayed in a table:

- Device Name—Name of the device
- Interface—Name of the interface
- Packets In—Number of packets received on the interface
- Packets Out—Number of packets sent from the interface
- Bytes In—Number of bytes received on the interface
- Bytes Out—Number of bytes sent from the interface

From the Automatic Refresh list, select **Disabled**, **Every 30 Seconds**, **Every 45 Seconds**, or **Every 1 Minute** to specify the frequency at which the statistics in the table must be updated and displayed. When you disable the auto-refresh capability, the page is not refreshed periodically by itself; instead you can click the **Refresh** icon to update the table contents for viewing.

VPN Traffic Trend

This monitor is displayed for L3VPN services. A line chart is displayed with time on the horizontal axis and the number of output packets on the vertical axis.

From the Time Interval drop-down box, select **1 Hour**, **8 Hours**, **1 Day**, **1 Week**, **1 Month**, **3 Months**, **6 Months**, **1 Year**, or **Custom** to specify the duration for which the data polled from devices needs to be displayed. If you select the **Custom** option, the Time range

popup dialog box is displayed. Specify the date from the calendar, and select the **Time From** (Start time in the 24-hour time format of collection of data), and **Time To** (End time in the 24-hour time format of collection of data). Click **OK** to save the settings. Else, click **Cancel** to discard the configuration.

**Related
Documentation**

- [Monitoring the Service Traffic Statistics of P2P Services for Correlating Device Counters on page 1209](#)
- [Monitoring the Service Traffic Statistics of VPLS Services for Correlating Device Counters on page 1213](#)
- [Monitoring the Service Transport Details of P2P Services for Easy Analysis on page 1218](#)
- [Monitoring the Service Transport Details of VPLS Services for Easy Analysis on page 1221](#)
- [Monitoring the Service Transport Details of Layer 3 VPN Services for Easy Analysis on page 1225](#)

Monitoring the Service Transport Details of P2P Services for Easy Analysis

You can view the Service Transport page of a particular service to obtain detailed and granular information on the high-level statistics that are displayed on the Service Summary page. The VPN routes learned by a provider edge (PE) device from all other PE devices are displayed. The PE routers in the provider's core network are the only routers that are configured to support VPNs and hence are the only routers to have information about the VPNs. From the point of view of VPN functionality, the provider (P) routers in the core—those P routers that are not directly connected to CE routers—are merely routers along the tunnel between the ingress and egress PE routers. The accounting information about configured and active label-switched paths (LSPs) is also displayed. Statistics are not available for LSPs on the egress routing device, because the penultimate routing device in the LSP sets the label to 0. Also, as the packet arrives at the egress routing device, the hardware removes its MPLS header and the packet reverts to being an IPv4 packet. Therefore, it is counted as an IPv4 packet, not an MPLS packet.



NOTE: The values and statuses of the parameters displayed in the graphs and tables of different widgets are refreshed, based on the polling interval configured on the Monitoring tab of the Preferences page (accessible by clicking the down arrow beside the System button on the Connectivity Services Director banner and selecting Preferences).

To view the Service Transport page for a P2P service:

1. Select **Service View** from the View Selector.

The workspaces that are applicable to routing and tunneling services are displayed on the View pane.

2. From the Junos Space user interface, click the **Monitor** icon on the Connectivity Services Director banner.

The functionalities that you can configure in this mode are displayed on the task pane.

- From the Service View pane, on the left, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.

The Network Services tree is expanded and displayed on the View pane.

- Click the plus sign (+) beside Connectivity to view services based on protocols.

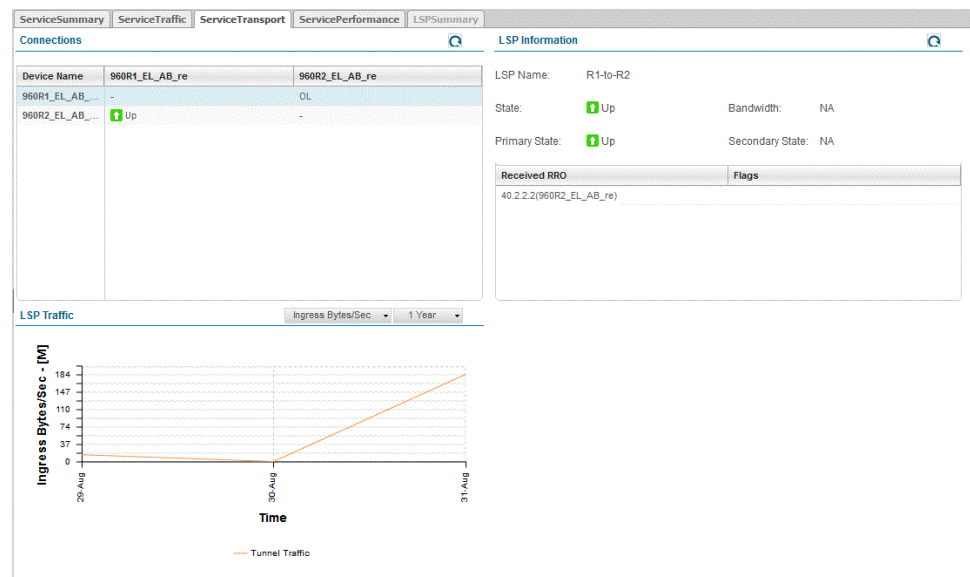
The Connectivity tree is expanded and displayed on the View pane.

- Expand the **P2P Services** tree to select a point-to-point service.

- Click the **ServiceTransport** tab.

The Service Transport page is displayed.

This widget provides details on Summary Monitors, which are shown in Service Summary Tab under Monitor functionality of “Service View”.



- [Connections on page 1219](#)
- [LSP Information on page 1220](#)
- [LSP Traffic on page 1221](#)

Connections

This monitor shows the status of connections between peer devices. In the tabular view, the row represents the source device and the columns denote the neighboring and destination devices. This monitor is applicable for P2P services. A green up-arrow in the indicates that the adjoining device in the network path to the destination device is

operationally up. A red down-arrow indicates that the device is down. For the device for which the connection status is displayed, a value of NA is displayed under its own corresponding column to denote that it is not applicable.

LSP Information

For a destination address that contains LSP names, the corresponding LSP details, such as the name, state, and bandwidth of the LSP, are displayed in this monitor. The details displayed in this monitor depend on the device selected in the Connections Matrix widget. The following fields are displayed:

- Name— Name of the LSP
- State— State of the LSP handled by this RSVP session: Up, Dn (down), or Restart
- Bandwidth—Specifies the bandwidth in bits per second for the LSP.
- Primary State— State of the LSP that is a primary path: Up, Down, or Restart
- Secondary State— State of the LSP that is a secondary path: Up, Down, or Restart
- Received RRO—(Ingress LSP) Received record route. A series of hops, each with an address followed by a flag. (In most cases, the received record route is the same as the computed explicit route. If Received RRO is different from Computed ERO, there is a topology change in the network, and the route is taking a detour.) The following flags identify the protection capability and status of the downstream node:
 - 0x01—Local protection available. The link downstream from this node is protected by a local repair mechanism. This flag can be set only if the Local protection flag was set in the SESSION_ATTRIBUTE object of the corresponding Path message.
 - 0x02—Local protection in use. A local repair mechanism is in use to maintain this tunnel (usually because of an outage of the link it was routed over previously).
 - 0x03—Combination of 0x01 and 0x02.
 - 0x04—Bandwidth protection. The downstream routing device has a backup path providing the same bandwidth guarantee as the protected LSP for the protected section.
 - 0x08—Node protection. The downstream routing device has a backup path providing protection against link and node failure on the corresponding path section. If the downstream routing device can set up only a link-protection backup path, the Local protection available bit is set but the Node protection bit is cleared.
 - 0x09—Detour is established. Combination of 0x01 and 0x08.
 - 0x10—Preemption pending. The preempting node sets this flag if a pending preemption is in progress for the traffic engine LSP. This flag indicates to the ingress legacy edge router (LER) of this LSP that it should be rerouted.
 - 0xb—Detour is in use. Combination of 0x01, 0x02, and 0x08.

- **Total Packets**—Total number of packets and Total number of bytes transmitted over the LSP. This counter is reset to zero whenever the LSP path is optimized (for example, during an automatic bandwidth allocation).
- **Total Bytes**—Total number of bytes transmitted over the LSP. This counter is reset to zero whenever the LSP path is optimized (for example, during an automatic bandwidth allocation).

LSP Traffic

This widget displays a line chart with the bytes per second (bps) or rate on the y-axis and time on the x-axis to denote the LSP bandwidth utilization in bps.

From the Time Interval drop-down box, select **1 Hour**, **8 Hours**, **1 Day**, **1 Week**, **1 Month**, **3 Months**, **6 Months**, **1 Year**, or **Custom** to specify the duration for which the data polled from devices needs to be displayed. If you select the **Custom** option, the Time range popup dialog box is displayed. Specify the date from the calendar, and select the **Time From** (Start time in the 24-hour time format of collection of data), and **Time To** (End time in the 24-hour time format of collection of data). Click **OK** to save the settings. Else, click **Cancel** to discard the configuration.

Related Documentation

- [Monitoring the Service Traffic Statistics of P2P Services for Correlating Device Counters on page 1209](#)
- [Monitoring the Service Traffic Statistics of Layer 3 VPN Services for Correlating Device Counters on page 1215](#)
- [Monitoring the Service Transport Details of P2P Services for Easy Analysis on page 1218](#)
- [Monitoring the Service Transport Details of VPLS Services for Easy Analysis on page 1221](#)
- [Monitoring the Service Transport Details of Layer 3 VPN Services for Easy Analysis on page 1225](#)

Monitoring the Service Transport Details of VPLS Services for Easy Analysis

You can view the Service Transport page of a particular service to obtain detailed and granular information on the high-level statistics that are displayed on the Service Summary page. The VPN routes learned by a provider edge (PE) device from all other PE devices are displayed. The PE routers in the provider's core network are the only routers that are configured to support VPNs and hence are the only routers to have information about the VPNs. From the point of view of VPN functionality, the provider (P) routers in the core—those P routers that are not directly connected to CE routers—are merely routers along the tunnel between the ingress and egress PE routers. The accounting information about configured and active label-switched paths (LSPs) is also displayed. Statistics are not available for LSPs on the egress routing device, because the penultimate routing device in the LSP sets the label to 0. Also, as the packet arrives at the egress routing device, the hardware removes its MPLS header and the packet reverts to being an IPv4 packet. Therefore, it is counted as an IPv4 packet, not an MPLS packet.



NOTE: The values and statuses of the parameters displayed in the graphs and tables of different widgets are refreshed, based on the polling interval configured on the Monitoring tab of the Preferences page (accessible by clicking the down arrow beside the System button on the Connectivity Services Director banner and selecting Preferences).

To view the Service Transport page for a VPLS service:

1. Select **Service View** from the View Selector.

The workspaces that are applicable to routing and tunneling services are displayed on the View pane.

2. From the Junos Space user interface, click the **Monitor** icon on the Connectivity Services Director banner.

The functionalities that you can configure in this mode are displayed on the task pane.

3. From the Service View pane, on the left, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.

The Network Services tree is expanded and displayed on the View pane.

4. Click the plus sign (+) beside Connectivity to view services based on protocols.

The Connectivity tree is expanded and displayed on the View pane.

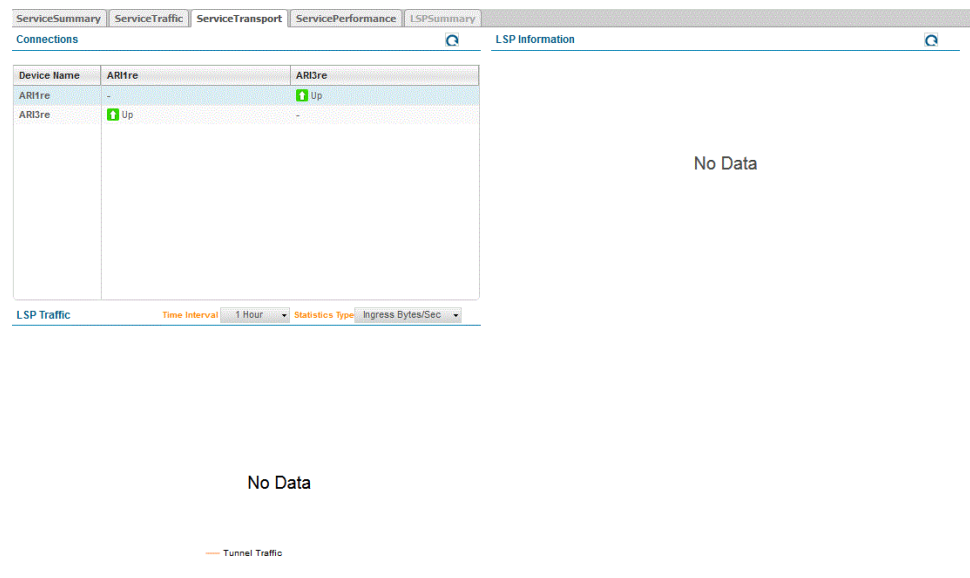
5. Expand the **VPLS Services** tree to select a VPLS service.

6. Click the **ServiceTransport** tab. The Service Transport page is displayed.

This widget provides details on Summary Monitors, which are shown in Service Summary Tab under Monitor functionality of “Service View”.

[Figure 57 on page 1223](#) shows the Service Transport tab for a VPLS service.

Figure 57: Service Transport Page for a VPLS Service



- [Connections on page 1223](#)
- [LSP Information on page 1223](#)
- [LSP Traffic on page 1224](#)

Connections

This monitor shows the status of connections between peer devices. In the tabular view, the row represents the source device and the columns denote the neighboring and destination devices. This monitor is applicable for P2P and VPLS services. A green up-arrow in the indicates that the adjoining device in the network path to the destination device is operationally up. A red down-arrow indicates that the device is down. For the device for which the connection status is displayed, a value of NA is displayed under its own corresponding column to denote that it is not applicable.

LSP Information

For a destination address that contains LSP names, the corresponding LSP details, such as the name, state, and bandwidth of the LSP, are displayed in this monitor. The details displayed in this monitor depend on the device selected in the Connection Matrix widget. The following fields are displayed:

- Name— Name of the LSP
- State— State of the LSP handled by this RSVP session: Up, Dn (down), or Restart
- Bandwidth—Specifies the bandwidth in bits per second for the LSP.
- Primary State— State of the LSP that is a primary path: Up, Down, or Restart
- Secondary State— State of the LSP that is a secondary path: Up, Down, or Restart
- Received RRO—(Ingress LSP) Received record route. A series of hops, each with an address followed by a flag. (In most cases, the received record route is the same as

the computed explicit route. If Received RRO is different from Computed ERO, there is a topology change in the network, and the route is taking a detour.) The following flags identify the protection capability and status of the downstream node:

- 0x01—Local protection available. The link downstream from this node is protected by a local repair mechanism. This flag can be set only if the Local protection flag was set in the SESSION_ATTRIBUTE object of the corresponding Path message.
- 0x02—Local protection in use. A local repair mechanism is in use to maintain this tunnel (usually because of an outage of the link it was routed over previously).
- 0x03—Combination of 0x01 and 0x02.
- 0x04—Bandwidth protection. The downstream routing device has a backup path providing the same bandwidth guarantee as the protected LSP for the protected section.
- 0x08—Node protection. The downstream routing device has a backup path providing protection against link and node failure on the corresponding path section. If the downstream routing device can set up only a link-protection backup path, the Local protection available bit is set but the Node protection bit is cleared.
- 0x09—Detour is established. Combination of 0x01 and 0x08.
- 0x10—Preemption pending. The preempting node sets this flag if a pending preemption is in progress for the traffic engine LSP. This flag indicates to the ingress legacy edge router (LER) of this LSP that it should be rerouted.
- 0xb—Detour is in use. Combination of 0x01, 0x02, and 0x08.

LSP Traffic

This widget displays a line chart with the bytes per second (bps) or rate on the y-axis and time on the x-axis to denote the LSP bandwidth utilization in bps.

From the Time Interval drop-down box, select **1 Hour**, **8 Hours**, **1 Day**, **1 Week**, **1 Month**, **3 Months**, **6 Months**, **1 Year**, or **Custom** to specify the duration for which the data polled from devices needs to be displayed. If you select the **Custom** option, the Time range popup dialog box is displayed. Specify the date from the calendar, and select the **Time From** (Start time in the 24-hour time format of collection of data), and **Time To** (End time in the 24-hour time format of collection of data). Click **OK** to save the settings. Else, click **Cancel** to discard the configuration.

Related Documentation

- [Monitoring the Service Traffic Statistics of P2P Services for Correlating Device Counters on page 1209](#)
- [Monitoring the Service Traffic Statistics of VPLS Services for Correlating Device Counters on page 1213](#)
- [Monitoring the Service Traffic Statistics of Layer 3 VPN Services for Correlating Device Counters on page 1215](#)
- [Monitoring the Service Transport Details of P2P Services for Easy Analysis on page 1218](#)

- [Monitoring the Service Transport Details of Layer 3 VPN Services for Easy Analysis on page 1225](#)

Monitoring the Service Transport Details of Layer 3 VPN Services for Easy Analysis

You can view the Service Transport page of a particular service to obtain detailed and granular information on the high-level statistics that are displayed on the Service Summary page. The VPN routes learned by a provider edge (PE) device from all other PE devices are displayed. The PE routers in the provider's core network are the only routers that are configured to support VPNs and hence are the only routers to have information about the VPNs. From the point of view of VPN functionality, the provider (P) routers in the core—those P routers that are not directly connected to CE routers—are merely routers along the tunnel between the ingress and egress PE routers. The accounting information about configured and active label-switched paths (LSPs) is also displayed. Statistics are not available for LSPs on the egress routing device, because the penultimate routing device in the LSP sets the label to 0. Also, as the packet arrives at the egress routing device, the hardware removes its MPLS header and the packet reverts to being an IPv4 packet. Therefore, it is counted as an IPv4 packet, not an MPLS packet.



NOTE: The values and statuses of the parameters displayed in the graphs and tables of different widgets are refreshed, based on the polling interval configured on the Monitoring tab of the Preferences page (accessible by clicking the down arrow beside the System button on the Connectivity Services Director banner and selecting Preferences).

To view the Service Transport page for an L3VPN service:

1. Select **Service View** from the View Selector.
The workspaces that are applicable to routing and tunneling services are displayed on the View pane.
2. From the Junos Space user interface, click the **Monitor** icon on the Connectivity Services Director banner.
The functionalities that you can configure in this mode are displayed on the task pane.
3. From the Service View pane, on the left, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
The Network Services tree is expanded and displayed on the View pane.
4. Click the plus sign (+) beside Connectivity to view services based on protocols.
The Connectivity tree is expanded and displayed on the View pane.

5. Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.

6. Click the **ServiceTransport** tab.

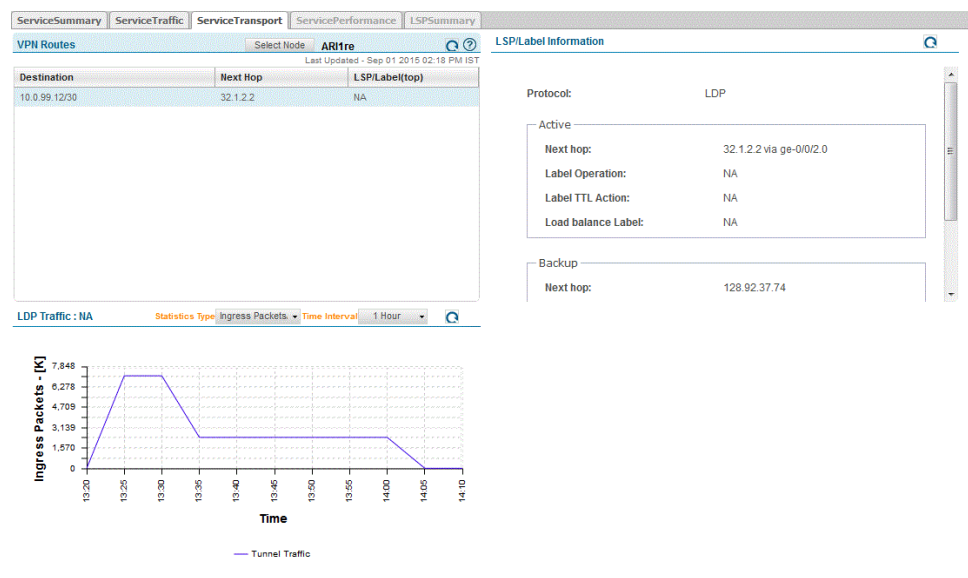
The Service Transport page is displayed.

This widget provides details on Summary Monitors, which are shown in Service Summary Tab under Monitor functionality of “Service View”.

- [Transport Statistics on page 1226](#)
- [VPN Routes on page 1208](#)
- [Label/LSP Information on page 1227](#)
- [LSP Traffic on page 1221](#)

Figure 58 on page 1226 shows the Service Transport tab for an L3VPN service.

Figure 58: Service Transport Page for an L3VPN Service



Transport Statistics

The Transport Statistics monitor shows the statistical counts for the selected data against time between the source device and the specified peer or destination device, and the LSP being used by the endpoint. The source device is the row selected in the Connection Matrix widget. The destination device is based on the device that you chose in the Traffic Statistics widget. By default, destination devices are empty. This monitor is valid for P2P services. A line graph is displayed with time on the horizontal axis and the type of statistical parameter on the vertical axis. In the Peer Device list, all Devices from the Connection Matrix except the source device are available for selection. In the Statistics Type list, you can select Ingress Packets or Ingress Bytes. Color-coded legends are used to indicate tunnel and device traffic. The purple line denotes tunnel traffic and the brown

line signifies the device (service) traffic. Because the LSP does not provide any metric if it is down, there might be variations in the data point for the LSP and device.

VPN Routes

This widget displays information about the path through which the packets traverse in LSPs in a VPN tunnel. Select a node for which you want to view the VPN routing information from the Select Node list at the top of the monitor. Alternatively, enter the name of the node for which you want to view the VPN routing details as the match criterion in the Search box and click the Search icon. The page refreshes to display the nodes that match with the search criterion. Click **Refresh** to update the contents of the table.

- Destination— Destination (egress routing device) of the session
- Next Hop— Address of the next-hop (downstream) routing device or client, interface used to reach this neighbor, and number of packets sent to the downstream routing
- LSP/Label— Name of the LSP. For LDP signaling, NA is shown.

Label/LSP Information

Label Information

For a destination address that you select in the VPN Routes monitor that contain LDP-established LSPs, the corresponding label details for active and backup LSPs are displayed in this monitor. The following fields are displayed:

- Protocol—LDP is the mechanism used to establish LSPs
- Next-hop—Network layer address of the directly reachable neighboring system.
- via—Interface used to reach the next hop. If there is more than one interface available to the next hop, the name of the interface that is actually used is followed by the word Selected. This field can also contain the following information:
 - Weight—Value used to distinguish primary, secondary, and fast reroute backup routes. Weight information is available when MPLS label-switched path (LSP) link protection, node-link protection, or fast reroute is enabled, or when the standby state is enabled for secondary paths. A lower weight value is preferred. Among routes with the same weight value, load balancing is possible.
 - Balance—Balance coefficient indicating how traffic of unequal cost is distributed among next hops when a routing device is performing unequal-cost load balancing. This information is available when you enable BGP multipath load balancing.
- Label Operation—MPLS label and operation occurring at this routing device. The operation can be pop (where a label is removed from the top of the stack), push (where another label is added to the label stack), or swap (where a label is replaced by another label).
- Label TTL Action—State of the TTL propagation attribute, such as prop-ttl (propagate the TTL value), prop-ttl (top) (propagate the TTL value of the outermost or top label),

no-prop-ttl (do not propagate the TTL value), or no-prop-ttl (top) (do not transmit the TTL value of the top label)

- Load Balance label—Whether the load-balancing capability based on labels is enabled.

LSP Information

For a destination address that you select in the VPN Routes monitor that contain LSP names, the corresponding LSP details, such as the name, state, and bandwidth of the LSP, are displayed in this monitor. The details displayed in this monitor depend on the device selected in the Connection Matrix widget. The following fields are displayed:

- Name— Name of the LSP
- State— State of the LSP handled by this RSVP session: Up, Dn (down), or Restart
- Bandwidth—Specifies the bandwidth in bits per second for the LSP.
- Primary State— State of the LSP that is a primary path: Up, Down, or Restart
- Secondary State— State of the LSP that is a secondary path: Up, Down, or Restart
- Received RRO—(Ingress LSP) Received record route. A series of hops, each with an address followed by a flag. (In most cases, the received record route is the same as the computed explicit route. If Received RRO is different from Computed ERO, there is a topology change in the network, and the route is taking a detour.) The following flags identify the protection capability and status of the downstream node:
 - 0x01—Local protection available. The link downstream from this node is protected by a local repair mechanism. This flag can be set only if the Local protection flag was set in the SESSION_ATTRIBUTE object of the corresponding Path message.
 - 0x02—Local protection in use. A local repair mechanism is in use to maintain this tunnel (usually because of an outage of the link it was routed over previously).
 - 0x03—Combination of 0x01 and 0x02.
 - 0x04—Bandwidth protection. The downstream routing device has a backup path providing the same bandwidth guarantee as the protected LSP for the protected section.
 - 0x08—Node protection. The downstream routing device has a backup path providing protection against link and node failure on the corresponding path section. If the downstream routing device can set up only a link-protection backup path, the Local protection available bit is set but the Node protection bit is cleared.
 - 0x09—Detour is established. Combination of 0x01 and 0x08.
 - 0x10—Preemption pending. The preempting node sets this flag if a pending preemption is in progress for the traffic engine LSP. This flag indicates to the ingress legacy edge router (LER) of this LSP that it should be rerouted.
 - 0xb—Detour is in use. Combination of 0x01, 0x02, and 0x08.

- **Total Packets**—Total number of packets and Total number of bytes transmitted over the LSP. This counter is reset to zero whenever the LSP path is optimized (for example, during an automatic bandwidth allocation).
- **Total Bytes**—Total number of bytes transmitted over the LSP. This counter is reset to zero whenever the LSP path is optimized (for example, during an automatic bandwidth allocation).

LSP Traffic

This widget displays a line chart with the bytes per second (bps) or rate on the y-axis and time on the x-axis to denote the LSP bandwidth utilization in bps.

From the Time Interval drop-down box, select **1 Hour**, **8 Hours**, **1 Day**, **1 Week**, **1 Month**, **3 Months**, **6 Months**, **1 Year**, or **Custom** to specify the duration for which the data polled from devices needs to be displayed. If you select the **Custom** option, the Time range popup dialog box is displayed. Specify the date from the calendar, and select the **Time From** (Start time in the 24-hour time format of collection of data), and **Time To** (End time in the 24-hour time format of collection of data). Click **OK** to save the settings. Else, click **Cancel** to discard the configuration.

Related Documentation

- [Monitoring the Service Traffic Statistics of P2P Services for Correlating Device Counters on page 1209](#)
- [Monitoring the Service Traffic Statistics of VPLS Services for Correlating Device Counters on page 1213](#)
- [Monitoring the Service Traffic Statistics of Layer 3 VPN Services for Correlating Device Counters on page 1215](#)
- [Monitoring the Service Transport Details of P2P Services for Easy Analysis on page 1218](#)
- [Monitoring the Service Transport Details of VPLS Services for Easy Analysis on page 1221](#)

Viewing Y.1731 Performance Monitoring Statistics for Point-to-Point Services

The Y.1731 monitoring functionality is not enabled by default. You must explicitly start the PM collection mechanism by selecting **PM Statistics > Start** from the Tasks pane after selecting the specified service on the View pane. The graphical representation of the retrieved statistical details for the service is displayed, based on data availability. The data collected is retained after you stop the PM collection utility for future reference and correlation.

If you are upgrading from the older version of Services Activation Director to Connectivity Services Director 1.0, you must stop any performance monitoring and restart the collection of PM statistics on the endpoints.



NOTE: The values and statuses of the parameters displayed in the graphs and tables of different widgets are refreshed, based on the polling interval configured on the Monitoring tab of the Preferences page (accessible by clicking the down arrow beside the System button on the Connectivity Services Director banner and selecting Preferences).

To view the performance monitoring statistics for the point-to-point service:

1. Select **Service View** from the View Selector.

The workspaces that are applicable to routing and tunneling services are displayed on the View pane.

2. From the Junos Space user interface, click the **Monitor** icon on the Connectivity Services Director banner.

The functionalities that you can configure in this mode are displayed on the task pane.

3. From the Service View pane, on the left, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.

The Network Services tree is expanded and displayed on the View pane.

4. Click the plus sign (+) beside P2P Services to view the P2P service orders.

5. Select the P2P service order for which you want to monitor performance statistics.

The P2P Services tree is expanded and displayed on the View pane.

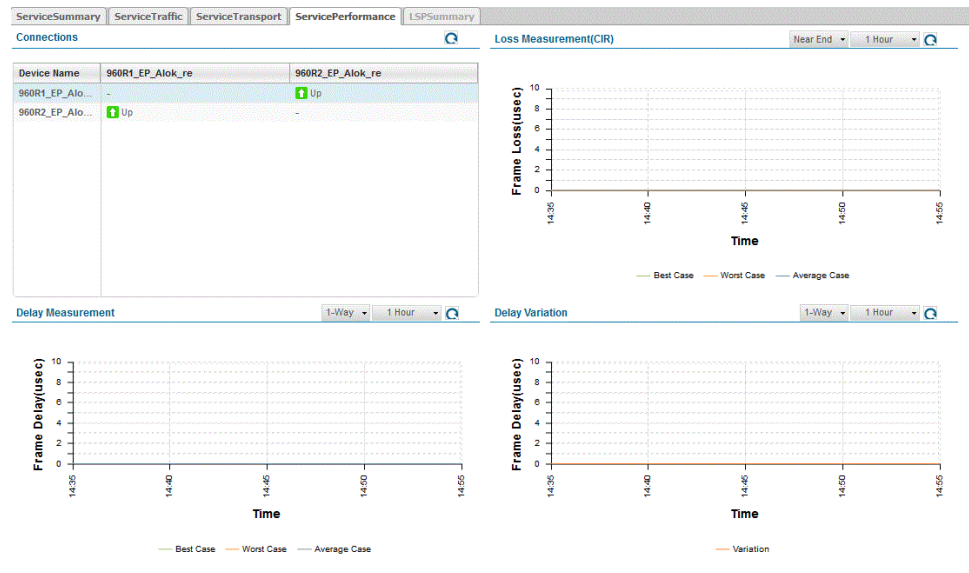
6. Select the **ServicePerformance** tab.

The Service Performance page is displayed.



NOTE: You can view performance management statistics only after you start the collection of performance monitoring (PM) statistics by selecting **PM Statistics > Start** from the Tasks pane.

7. View and analyze the respective graph.



The following widgets are displayed:

- [Connections on page 1231](#)
- [Loss Measurement on page 1231](#)
- [Delay Measurement on page 1232](#)
- [Delay Variation on page 1232](#)

Connections

This monitor shows the status of connections between peer devices. In the tabular view, the row represents the source device and the columns denote the neighboring and destination devices. This monitor is applicable for P2P and VPLS services. A green up-arrow in the indicates that the adjoining device in the network path to the destination device is operationally up. A red down-arrow indicates that the device is down. For the device for which the connection status is displayed, a value of NA is displayed under its own corresponding column to denote that it is not applicable. Click **Refresh** at the top of the monitor to update and display the contents of the table.

From the Time Interval drop-down box, select **1 Hour**, **8 Hours**, **1 Day**, **1 Week**, **1 Month**, **3 Months**, **6 Months**, **1 Year**, or **Custom** to specify the duration for which the data polled from devices needs to be displayed. If you select the **Custom** option, the Time range popup dialog box is displayed. Specify the date from the calendar, and select the **Time From** (Start time in the 24-hour time format of collection of data), and **Time To** (End time in the 24-hour time format of collection of data). Click **OK** to save the settings. Else, click **Cancel** to discard the configuration.

Loss Measurement

The Loss Measurement graph displays a real-time linear plot of delay value with respect to the time. The x-axis represents the time and the y-axis represents the frame loss ratio. Near-end frame loss refers to the count of frame loss associated with ingress data frames.

Far-end frame loss refers to the count of frame loss associated with egress data frames. The lines represent the best case frame loss or the lowest frame loss, the worst case frame loss or the highest frame loss, and the average frame loss or the median of the highest and lowest frame losses. The frame loss is calculated by collecting the counter values applicable for ingress and egress service frames. The counters maintain a count of transmitted and received data frames between a pair of MEPs. The loss measurement statistics are retrieved as the output of the monitor ethernet loss-measurement command and are also stored at the initiator. The frame counts are stored at both the initiator and the receiver MEPs for later retrieval. The on-demand loss measurement statistics is collected for point-to-point service only. There are two linear charts: Near-End-CIR and Far-End-CIR. For each interval, the graph plots three values: Average case, best case, and worst case frame loss. From the Loss End drop-down list, select **Near-end (CIR)** to display frame loss statistics associated with ingress data frames or **Far-end (CIR)** to display frame loss statistics associated with egress data frames. Mouse over the legends to view the lines corresponding to best-case, average, and worst-case frame loss statistics.

Delay Measurement

The Delay Measurement graph displays a real-time linear plot of delay value with respect to the time. The x-axis represents the time and the y-axis represents frame delay in microseconds. The legends reference average one-way delay, best-case one-way delay, and worst-case one way delay for one-way delay measurement. The green line denotes the lowest one-way frame delay for the statistics displayed, the orange line denotes the highest one-way frame delay for the statistics displayed, and the blue line denotes the average one-way frame delay for the statistics displayed. The legends reference average two-way delay, best-case two-way delay, and worst-case two-way delay for two-way delay measurement. The green line denotes the lowest two-way frame delay for the statistics displayed, the orange line denotes the highest two-way frame delay for the statistics displayed, and the blue line denotes the average two-way frame delay for the statistics displayed. From the Delay End drop-down box, select **1-Way** or **2-Way** to display the one-way or two-way frame delay measurement protocols respectively.

Delay Variation

The Delay Variation graph displays the difference between the consecutive frame delay values. The x-axis represents the time and the y-axis represents delay variation in microseconds. The line denotes the average one-way delay variation or the average one-way “frame jitter” for the statistics displayed for one-way frame delay measurement. The line denotes the average two-way delay variation or the average two-way “frame jitter” for the statistics displayed for two-way delay measurement.

By default, the total time duration is ten minutes. If the duration of statistics collection exceeds ten minutes, the graph scrolls and shows the data of latest ten minutes.

Related Documentation

- [Performance Management Overview on page 1113](#)
- [Monitoring Performance Management Statistics on page 1115](#)
- [Viewing Performance Management Statistics on page 1121](#)
- [Service Troubleshooting Overview on page 1129](#)

- [Performing a Configuration Audit on page 1077](#)

Viewing Y.1731 Performance Monitoring Statistics for VPLS Services

The Y.1731 monitoring functionality is not enabled by default. You must explicitly start the PM collection mechanism by selecting **PM Statistics > Start** from the Tasks pane after selecting the specified service on the View pane. The graphical representation of the retrieved statistical details for the service is displayed, based on data availability. The data collected is retained after you stop the PM collection utility for future reference and correlation.

If you are upgrading from the older version of Services Activation Director to Connectivity Services Director 1.0, you must stop any performance monitoring and restart the collection of PM statistics on the endpoints.



NOTE: The values and statuses of the parameters displayed in the graphs and tables of different widgets are refreshed, based on the polling interval configured on the Monitoring tab of the Preferences page (accessible by clicking the down arrow beside the System button on the Connectivity Services Director banner and selecting Preferences).

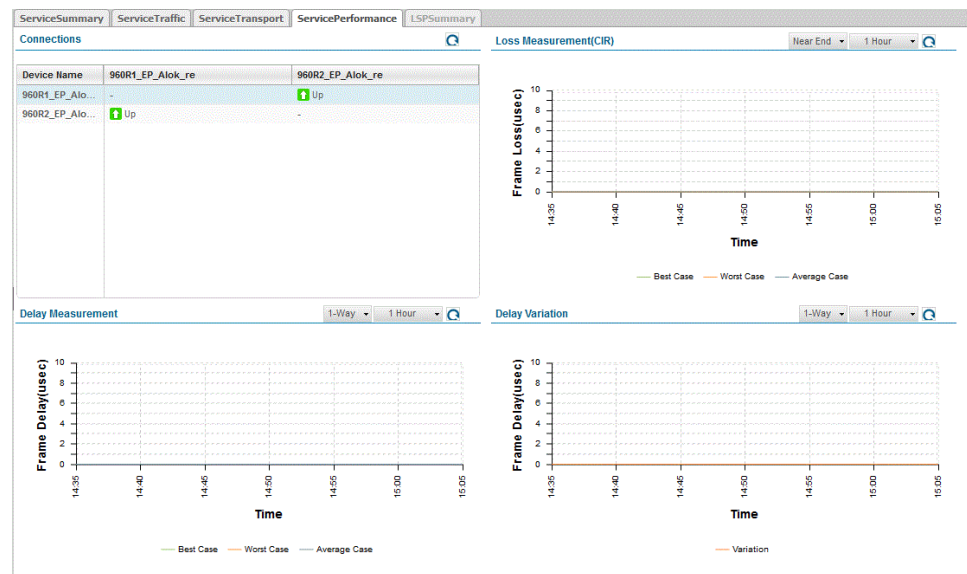
To view the performance monitoring statistics for the VPLS service:

1. Select **Service View** from the View Selector.
The workspaces that are applicable to routing and tunneling services are displayed on the View pane.
2. From the Junos Space user interface, click the **Monitor** icon on the Connectivity Services Director banner.
The functionalities that you can configure in this mode are displayed on the task pane.
3. From the Service View pane, on the left, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
The Network Services tree is expanded and displayed on the View pane.
4. Click the plus sign (+) beside VPLS Services to view the VPLS service orders.
The VPLS Services tree is expanded and displayed on the View pane.
5. Select the VPLS service order for which you want to monitor performance statistics.
6. Select the **ServicePerformance** tab.
The Service Performance page is displayed.



NOTE: You can view performance management statistics only after you start the collection of performance monitoring (PM) statistics by selecting **PM Statistics > Start** from the Tasks pane.

7. View and analyze the respective graph.



The following widgets are displayed:

- [Connections on page 1234](#)
- [Loss Measurement on page 1235](#)
- [Delay Measurement on page 1235](#)
- [Delay Variation on page 1235](#)

Connections

This monitor shows the status of connections between peer devices. In the tabular view, the row represents the source device and the columns denote the neighboring and destination devices. This monitor is applicable for P2P and VPLS services. A green up-arrow in the indicates that the adjoining device in the network path to the destination device is operationally up. A red down-arrow indicates that the device is down. For the device for which the connection status is displayed, a value of NA is displayed under its own corresponding column to denote that it is not applicable. Click **Refresh** at the top of the monitor to update and display the contents of the table.

From the Time Interval drop-down box, select **1 Hour**, **8 Hours**, **1 Day**, **1 Week**, **1 Month**, **3 Months**, **6 Months**, **1 Year**, or **Custom** to specify the duration for which the data polled from devices needs to be displayed. If you select the **Custom** option, the Time range popup dialog box is displayed. Specify the date from the calendar, and select the **Time From** (Start time in the 24-hour time format of collection of data), and **Time To** (End

time in the 24-hour time format of collection of data). Click **OK** to save the settings. Else, click **Cancel** to discard the configuration.

Loss Measurement

The Loss Measurement graph displays a real-time linear plot of delay value with respect to the time. The x-axis represents the time and the y-axis represents the frame loss ratio. Near-end frame loss refers to the count of frame loss associated with ingress data frames. Far-end frame loss refers to the count of frame loss associated with egress data frames. The lines represent the best case frame loss or the lowest frame loss, the worst case frame loss or the highest frame loss, and the average frame loss or the median of the highest and lowest frame losses. The frame loss is calculated by collecting the counter values applicable for ingress and egress service frames. The counters maintain a count of transmitted and received data frames between a pair of MEPs. The loss measurement statistics are retrieved as the output of the monitor ethernet loss-measurement command and are also stored at the initiator. The frame counts are stored at both the initiator and the receiver MEPs for later retrieval. The on-demand loss measurement statistics is collected for point-to-point service only. There are two linear charts: Near-End-CIR and Far-End-CIR. For each interval, the graph plots three values: Average case, best case, and worst case frame loss. From the Loss End drop-down list, select **Near-end (CIR)** to display frame loss statistics associated with ingress data frames or **Far-end (CIR)** to display frame loss statistics associated with egress data frames. Mouse over the legends to view the lines corresponding to best-case, average, and worst-case frame loss statistics.

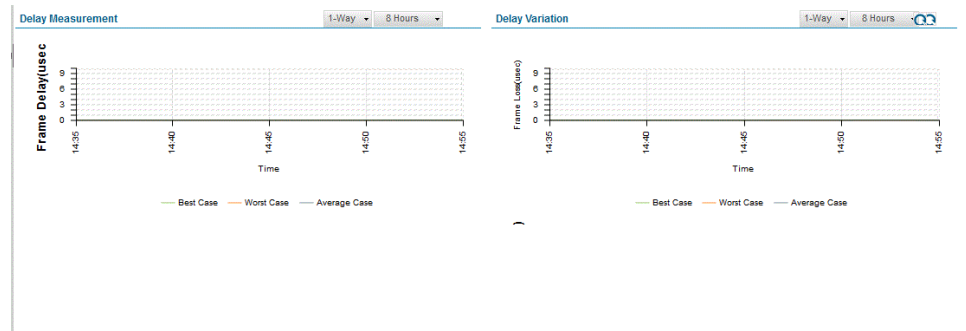
Delay Measurement

The Delay Measurement graph displays a real-time linear plot of delay value with respect to the time. The x-axis represents the time and the y-axis represents frame delay in microseconds. The legends reference average one-way delay, best-case one-way delay, and worst-case one way delay for one-way delay measurement. The green line denotes the lowest one-way frame delay for the statistics displayed, the orange line denotes the highest one-way frame delay for the statistics displayed, and the blue line denotes the average one-way frame delay for the statistics displayed. The legends reference average two-way delay, best-case two-way delay, and worst-case two-way delay for two-way delay measurement. The green line denotes the lowest two-way frame delay for the statistics displayed, the orange line denotes the highest two-way frame delay for the statistics displayed, and the blue line denotes the average two-way frame delay for the statistics displayed. From the Delay End drop-down box, select **1-Way** or **2-Way** to display the one-way or two-way frame delay measurement protocols respectively.

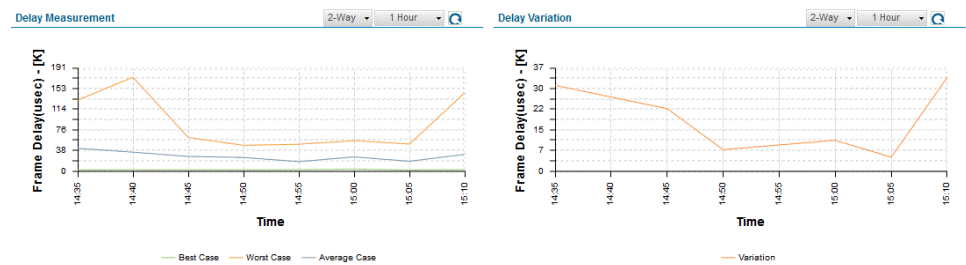
Delay Variation

The Delay Variation graph displays the difference between the consecutive frame delay values. The x-axis represents the time and the y-axis represents delay variation in microseconds. The line denotes the average one-way delay variation or the average one-way “frame jitter” for the statistics displayed for one-way frame delay measurement. The line denotes the average two-way delay variation or the average two-way “frame jitter” for the statistics displayed for two-way delay measurement.

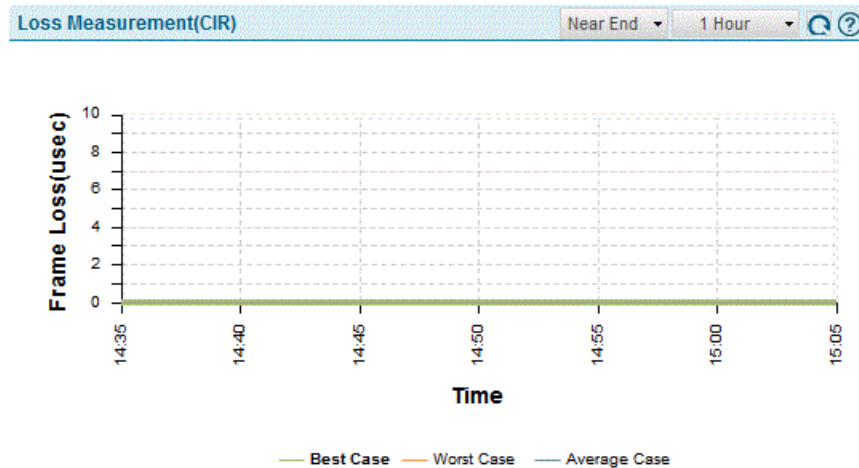
If the delay measurement is one-way, the following graph is displayed.

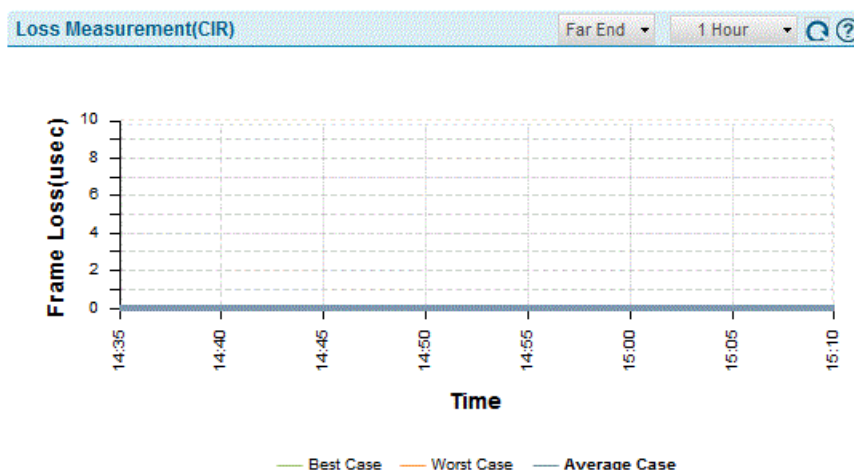


If the delay measurement is two-way, the following graph is displayed.



The Loss Measurement monitor displays two real-time linear plots: Near End (CIR) and Far End (CIR). The three parameters in each graph plot are average case, best case, and worst case of frame-loss.





The graph is plotted in real-time. By default, the total time duration is ten minutes. If the duration of statistics collection exceeds ten minutes, the graph scrolls and shows the data of latest ten minutes.

Related Documentation

- [Performance Management Overview on page 1113](#)
- [Monitoring Performance Management Statistics on page 1115](#)
- [Viewing Performance Management Statistics on page 1121](#)
- [Service Troubleshooting Overview on page 1129](#)
- [Performing a Configuration Audit on page 1077](#)

Clearing Interface Statistics

By resetting interface statistics, you ensure that previous input and output errors and packet statistics do not interfere with the current efforts to diagnose a problem. After a graceful Routing Engine switchover, we recommend that you use the functionality to clear interface statistics to reset the cumulative values for local statistics on the new master Routing Engine. Sometimes, you might require a baseline for interface statistics to be set for computation and reporting purposes. In such cases, before you set the baseline, you might need to clear or restart the accumulated statistics. The system implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved.

To clear interface statistics:

1. From the View selector, select **Service View**.

The functionalities that you can configure in this view are displayed on the View pane on the View pane.

2. Click the **Monitor** mode icon in the Service View on the Connectivity Services Director banner.

The workspaces that are applicable to this mode are displayed on the Tasks pane.

- From the Service View pane, select the type of service for which you want to clear interface statistics.

The statistics for the service type are displayed on the middle pane of the main display area.

- From the Tasks pane, which is displayed on the right, select **Tasks > Clear Interface Statistics**.

The Clear Interface Statistics option is displayed on the Tasks pane for P2P, VPLS, and L3VPN services to delete all the interface statistics associated with the selected service.

A dialog box appears, prompting you to confirm the deletion. The names of the devices and respective interfaces configured on the devices are shown. In this dialog box, you can also choose to delete the interface statistics on the devices.



NOTE: You can clear interface statistics on managed endpoints only. For a P2P service with unmanaged endpoints, only managed endpoints are shown in the endpoints table and corresponding statistics. To clear the statistics of unmanaged endpoints, you must clear the statistics using the Junos CLI on the corresponding devices.

Confirmation?

Are you sure you want to go ahead and clear all interface statistics associated with service p2P_BGP_Res0066 ?

Service Details	
Name	Interfaces
Service: Merg1_008_re (1 Item)	
Merg1_008_re	ge-0/0/3.444
Service: Merg1_009_re (1 Item)	
Merg1_009_re	ge-0/0/3.444
Service: Merg1_010_re (1 Item)	
Merg1_010_re	ge-0/0/2.444

☒ Clear statistics from Devices

OK Cancel

- Select the **Clear statistics from Devices** check box to clear the statistics from the devices. This operation is equivalent to the **clear interface statistics** command that you can run from the Junos OS CLI. If you select the **Clear statistics from Devices** check box, the statistics are cleared on the device for all the interfaces in the service, in

addition to being removed from the Connectivity Services director database. If you do not select this check box, the interface statistics are reset only in the application database and not on the device.

6. Click **OK** to confirm; alternatively, click **Cancel** to discard this operation.

The interface statistics are cleared.

Related Documentation

- [Viewing MAC Table Details on page 1239](#)
- [Viewing Interface Statistics on page 1241](#)
- [Viewing Interface Status Details on page 1243](#)
- [MPLS Connectivity Verification and Troubleshooting Methods on page 1245](#)
- [Using MPLS Ping on page 1247](#)
- [Pinging VPNs, VPLS, and Layer 2 Circuits on page 1249](#)
- [Monitoring Network Reachability by Using the MPLS Ping Capability on page 1250](#)
- [Monitoring Network Reachability by Using the Layer 3 VPN Ping Capability on page 1253](#)
- [Routing Table Overview on page 1256](#)

Viewing MAC Table Details

The router learns unicast media access control (MAC) addresses to avoid flooding the packets to all the ports in a bridge domain. The router creates a source MAC entry in its source and destination MAC tables for each MAC address learned from packets received on ports that belong to the bridge domain. If the bridge domain receives a control protocol data unit (PDU) which does not have a corresponding protocol configured, then the control PDU is considered as an unknown multicast data packet and the packets are flooded across all the ports that are part of the same bridge domain. If the bridge domain has the protocol corresponding to the PDU configured, then the control PDU is considered as a control packet and is processed by the routing engine.

MAC table aging ensures that a device tracks only active nodes on the network and that it is able to flush out network nodes that are no longer available. To manage MAC entries more efficiently, you can configure an entry's aging time, which is the maximum time that an entry can remain in the MAC address table before it is deleted because it has reached its maximum age.

To view the learned MAC address information for a device associated with a particular service:

1. From the View selector, select **Service View**.

The functionalities that you can configure in this view are displayed on the View pane.

2. Click the **Monitor** mode icon in the Service View of the Connectivity Services Director banner.

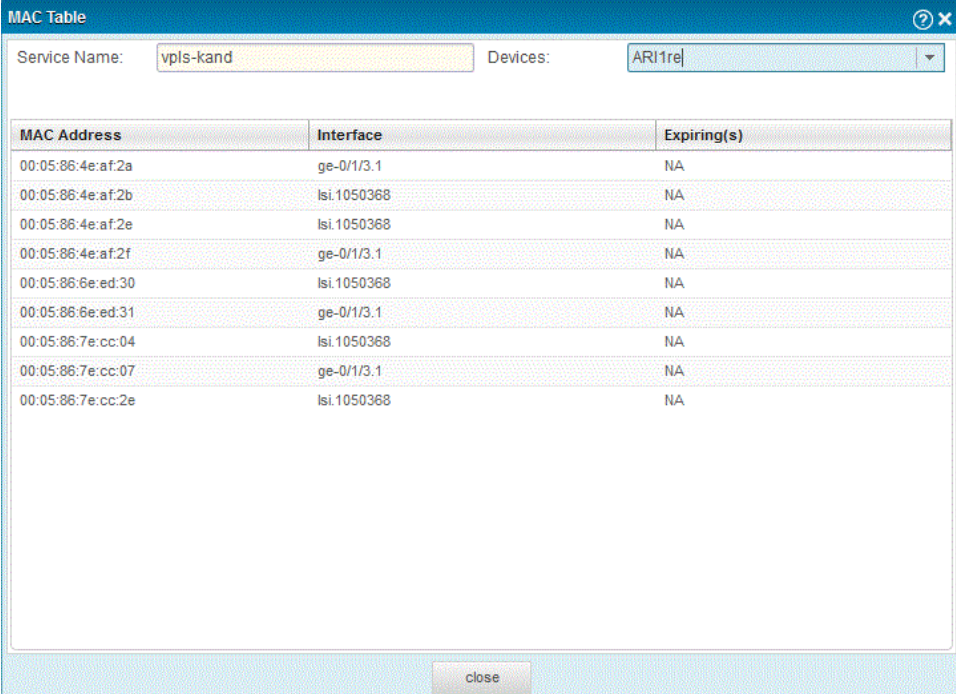
The workspaces that are applicable to this mode are displayed on the Tasks pane.

- From the Service View pane, select the type of service for which you want to view interface statistics.

The service statistical details are displayed in the middle pane.

- From the Tasks pane, which is displayed on the right, select **Tasks > Show MAC Table**.

The MAC Table dialog box is displayed. The name of the service is displayed in the Service Name field.



MAC Address	Interface	Expiring(s)
00:05:86:4e:af:2a	ge-0/1/3.1	NA
00:05:86:4e:af:2b	lsi.1050368	NA
00:05:86:4e:af:2e	lsi.1050368	NA
00:05:86:4e:af:2f	ge-0/1/3.1	NA
00:05:86:6e:ed:30	lsi.1050368	NA
00:05:86:6e:ed:31	ge-0/1/3.1	NA
00:05:86:7e:cc:04	lsi.1050368	NA
00:05:86:7e:cc:07	ge-0/1/3.1	NA
00:05:86:7e:cc:2e	lsi.1050368	NA

- From the Devices drop-down list, select the device for which you want to view the MAC table statistical details.

The following information is displayed in the lower pane of the dialog box in a tabular grid.

- MAC address—MAC address or addresses learned on a logical interface.
 - Interface—Name of the logical interface
 - Packets—Number of processed packets corresponding to the MAC address
 - Bytes—Number of processed bytes corresponding to the MAC address
 - Expiring—Aging time after which the MAC address expires and is not retained in the MAC table
- Click **Close** after you complete viewing the details.

You are returned to the main or home page in Monitor Mode of Service View, which is the Service Summary tab.

Viewing Interface Statistics

Packets that need to be forwarded to the adjacent network element or a neighboring device along a routing path might be dropped by a router owing to several factors. Some of the causes for such a loss of traffic or a block in transmission of data packets include overloaded system conditions, profiles and policies that restrict the bandwidth or priority of traffic, network outages, or disruption with physical cable faults. You can use a number of **show** commands to determine and analyze the statistical counters and metrics related to any traffic loss and take an appropriate corrective measure. The fields displayed in the View Interface Statistics dialog box help in diagnosing and debugging network performance and traffic-handling efficiency problems.

To view interface statistical details:

1. From the View selector, select **Service View**.

The functionalities that you can configure in this view are displayed on the View pane.

2. Click the **Monitor** mode icon in the Service View of the Connectivity Services Director banner.

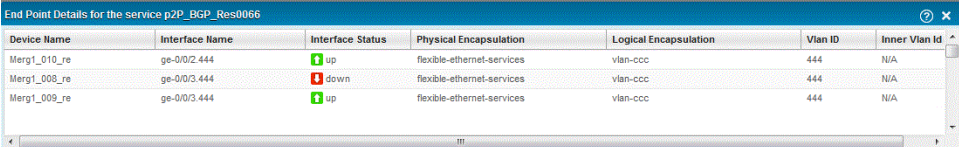
The workspaces that are applicable to this mode are displayed on the Tasks pane.

3. From the Service View pane, select the type of service for which you want to view interface statistics.

The service statistical details are displayed in the middle pane.

4. From the Tasks pane, which is displayed on the right, select **Tasks > Show Interface Statistics**.

The End Point Details dialog box is displayed for the selected service.



Device Name	Interface Name	Interface Status	Physical Encapsulation	Logical Encapsulation	Vlan ID	Inner Vlan ID
Merg1_010_re	ge-0/0/2.444	up	flexible-ethernet-services	vlan-ccc	444	N/A
Merg1_008_re	ge-0/0/3.444	down	flexible-ethernet-services	vlan-ccc	444	N/A
Merg1_009_re	ge-0/0/3.444	up	flexible-ethernet-services	vlan-ccc	444	N/A



NOTE: The Interface Traffic Statistics dialog box displays only the managed endpoints of the P2P service. Unmanaged device endpoints are not shown in the grid, and therefore the charts are also not applicable for unmanaged endpoints of the P2P service.

A graphical view and a tabular view of interface statistics are displayed. You can view the interface statuses, such as errors and the operational conditions of the interfaces, that enables you in analyzing, troubleshooting, and rectifying problems with dropped packets or untransmitted bytes. Some of the causes for such a loss of traffic or a block in transmission of data packets include overloaded system conditions, profiles and

policies that restrict the bandwidth or priority of traffic, network outages, or disruption with physical cable faults. This operation is equivalent to the `show interface statistics` command that you can run from the Junos OS CLI interface. You can search for specific devices or interfaces by entering a search item and clicking the Search icon. A line graph is displayed with the input packets and errors, and output packets and errors shown on the vertical axis and the time shown on the horizontal axis. The following color-coded legends reference the line graphs:

- Packets In (Orange)—Number of packets received on the interface
- Packets Out (Green)—Number of packets sent from the interface
- Errors In (Blue)—Number of inbound errors received on the interface
- Errors Out (Purple)—Number of outbound errors transmitted from the interface

The Interface Details table displays all the UNI parts of the service. Also, the physical interface for the logical interface participating in the service is displayed.

- Device Name—Name of the device
- Interface—Name of the interface
- Interface Type—Whether the interface is physical or logical
- Encapsulation—Physical or logical encapsulation configured on the interface.
- Operational Status—Operational status of the physical interface: Up, Down.
- Admin Status—Administrative state of the interface: Enabled or Disabled.
- MAC Address—MAC address of the physical interface.
- Input Packets—Number of packets received on the interface.
- Output Packets—Number of packets sent from the interface.
- Last Poll Time—Date and time at which the statistical detail was obtained by polling and retrieving from the device for the specified interface.

The Packet Counter tab on the right side of the page displays the following fields in a table. It is applicable for physical interfaces only. The values displayed are in rates of packets per second.

- Input Unicasts—Number of input unicast packets for the physical interface
- Output Unicasts—Number of output unicast packets for the physical interface
- Input Multicast—Number of input multicast packets for the physical interface
- Output Multicast—Number of output multicast packets for the physical interface
- Input Broadcast—Number of input broadcast packets for the physical interface
- Output Broadcast—Number of output broadcast packets for the physical interface

The Error Counter tab on the right side of the page displays the following fields in a table. It is available for physical interfaces only. The values displayed are in rates of packets per second.

- Input Errors—Number of errors packets received on the physical interface
- Output Drops—Number of outgoing packets that are dropped by the physical interface
- Input Framing Errors—Number of packets with framing errors that are received on the physical interface
- Input Drops—Number of incoming packets that are dropped by the physical interface
- Input Discards—Number of incoming packets discarded by the physical interface
- Output Errors—Number of error packets sent out from the physical interface

Related Documentation

- [Clearing Interface Statistics on page 1237](#)
- [Viewing Interface Statistics on page 1241](#)
- [Viewing Interface Status Details on page 1243](#)
- [MPLS Connectivity Verification and Troubleshooting Methods on page 1245](#)
- [Using MPLS Ping on page 1247](#)
- [Pinging VPNs, VPLS, and Layer 2 Circuits on page 1249](#)
- [Monitoring Network Reachability by Using the MPLS Ping Capability on page 1250](#)
- [Monitoring Network Reachability by Using the Layer 3 VPN Ping Capability on page 1253](#)
- [Routing Table Overview on page 1256](#)

Viewing Interface Status Details

You can use the monitoring functionality to view interface status or to monitor interface bandwidth utilization and traffic statistics on the device. When you view the interface status for a particular service, all the interfaces configured on the different devices associated the service are retrieved and displayed. The operational status of the interface, the encapsulation type configured for the interface, and the VLAN ID specified for the interface enable you to determine whether any changes are needed to the interface settings to correct discrepancies with services and traffic forwarding.

To view interface status details:

1. From the View selector, select **Service View**.
The functionalities that you can configure in this view are displayed on the View pane.
2. Click the **Monitor** mode icon in the Service View of the Connectivity Services Director banner.
The workspaces that are applicable to this mode are displayed on the Tasks pane.
3. From the Service View pane, select the type of service for which you want to view interface status information.

The service statistical details are displayed in the middle pane.

- From the Tasks pane, which is displayed on the right, select **Tasks > Show Interface Status**.

A graphical view and a tabular view of interface configuration details are displayed.



TIP: You can also open the Interface Traffic Status dialog box by selecting **Troubleshoot > Service Audit** from the Tasks pane for a specific service.

Figure 59: Interface Traffic Status for a P2P Service

End Point Details for the Service BGP_FM

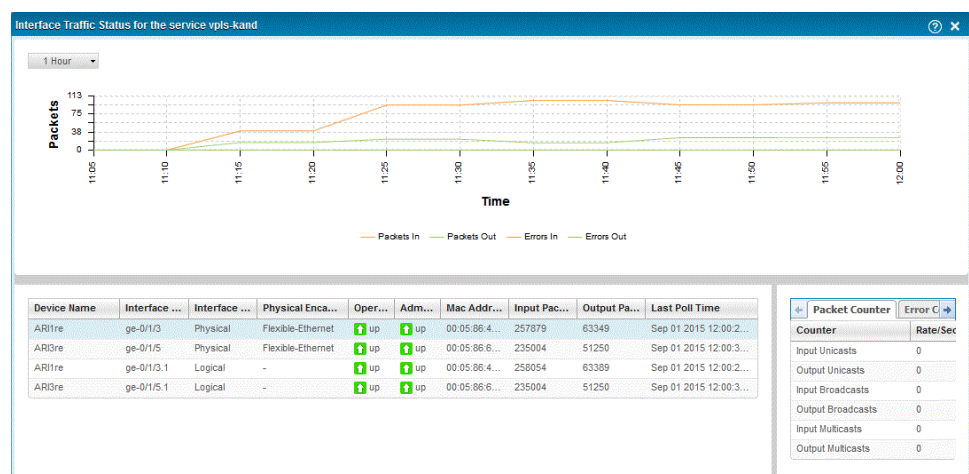
Device Name	Interface Name	Interface Status	Physical Encapsulation	Logical Encapsulation	Vlan ID	Inner Vlan	Port Mode
Merg1_002_re	ge-0/0/6.2002	up	flexible-ethernet-services	vlan-vpls	2002	N/A	N/A
400R4_EP_Alok_re	ge-0/0/6.2002	down	flexible-ethernet-services	vlan-vpls	2002	N/A	N/A
400R4_EP_Alok_re	ge-0/0/6.2002	down	flexible-ethernet-services	vlan-vpls	2002	N/A	N/A
Merg1_003_re	ge-0/0/6.2002	up	flexible-ethernet-services	vlan-vpls	2002	N/A	N/A
Merg1_008_re	ge-0/0/6.2002	up	flexible-ethernet-services	vlan-vpls	2002	N/A	N/A
Merg1_008_re	ge-0/0/6.2002	up	flexible-ethernet-services	vlan-vpls	2002	N/A	N/A
Merg1_004_re	ge-0/0/6.2002	up	flexible-ethernet-services	vlan-vpls	2002	N/A	N/A
Merg1_001_re	ge-0/0/6.2002	up	flexible-ethernet-services	vlan-vpls	2002	N/A	N/A
400R3_EP_Alok_re	ge-0/0/6.2002	down	flexible-ethernet-services	vlan-vpls	2002	N/A	N/A
960R1_EP_Alok_re	ge-0/0/6.2002	down	flexible-ethernet-services	vlan-vpls	2002	N/A	N/A
960R1_EP_Alok_re	ge-0/0/6.2002	down	flexible-ethernet-services	vlan-vpls	2002	N/A	N/A
Merg1_007_re	ge-0/0/6.2002	up	flexible-ethernet-services	vlan-vpls	2002	N/A	N/A
Merg1_005_re	ge-0/0/6.2002	up	flexible-ethernet-services	vlan-vpls	2002	N/A	N/A
960R2_EP_Alok_re	ge-0/0/6.2002	down	flexible-ethernet-services	vlan-vpls	2002	N/A	N/A
960R2_EP_Alok_re	ge-0/0/6.2002	down	flexible-ethernet-services	vlan-vpls	2002	N/A	N/A

Page 1 of 1

Displaying 1 - 15 of 15

Show 25 items

Figure 60: Interface Traffic Status for a VPLS Service





NOTE: Viewing interface information is valid on a P2P service with unmanaged endpoints. However, the task results are shown only for the managed endpoint. Unmanaged endpoints are not listed in the table.

This operation is equivalent to the **show interface** command that you can run from the Junos OS CLI interface. The following interface information is displayed in a tabular form:

- Device Name—Name of the Device
- Interface—Name of the UNI interface
- Interface Status—Operational status of the interface: Up, Down
- Physical Encapsulation—Physical encapsulation configured on the Interface
- Logical Encapsulation—Logical encapsulation configured on the interface; else it is not applicable
- Vlan Id—VLAN ID of the logical unit number of the interface; else it is not applicable
- Inner Vlan Id—Inner VLAN or customer VLAN tag of the interface; else it is not applicable
- Port Mode—Operating mode for an interface can be one of the following:
 - access—In this mode, the interface can be in a single VLAN only. Access interfaces typically connect to single network devices such as PCs, printers, IP telephones, and IP cameras.
 - tagged-access—In this mode, the interface can accept tagged packets from one access device. Tagged-access interfaces typically connect to servers running Virtual machines using VEPA technology.
 - trunk—In this mode, the interface can be in multiple VLANs and accept tagged packets from multiple devices. Trunk interfaces typically connect to other switches and to routers on the LAN.
- NA—Not applicable

Related Documentation

- [Clearing Interface Statistics on page 1237](#)
- [Viewing MAC Table Details on page 1239](#)
- [Viewing Interface Statistics on page 1241](#)
- [MPLS Connectivity Verification and Troubleshooting Methods on page 1245](#)

MPLS Connectivity Verification and Troubleshooting Methods

You can use the MPLS ping application to examine the network reachability and identify any broken links for diagnostic purposes. Before using the ping MPLS feature, make sure that the receiving interface on the VPN or LSP remote endpoint has MPLS enabled, and

that the loopback interface on the outbound node is configured as 127.0.0.1. The source address for MPLS probes must be a valid address on the device. When you use the ping MPLS feature from a J Series device operating as the inbound (ingress) node at the entry point of an LSP or VPN, the router sends probe packets into the LSP or VPN. Based on how the LSP or VPN outbound (egress) node at the remote endpoint of the connection replies to the probes, you can determine the connectivity of the LSP or VPN. Each probe is an echo request sent to the LSP or VPN exit point as an MPLS packet with a UDP payload. If the outbound node receives the echo request, it checks the contents of the probe and returns a value in the UDP payload of the response packet. If the device receives the response packet, it reports a successful ping response. Responses that take longer than 2 seconds are identified as failed probes.

In IP networks, the ping and traceroute commands enable you to verify network connectivity and find broken links or loops. In MPLS-enabled networks, you can use the **ping** command to determine whether IP connectivity exists to a destination even when the ping packets must traverse multiple LSPs. You can use the **traceroute** command to determine the labels that data packets use when traversing LSPs to the destination. In an MPLS-enabled network, however, you cannot use these IP commands to determine MPLS connectivity to a destination. You can use the MPLS ping and trace features to detect data plane failures in LSPs. Specific **mpls ping** and **trace mpls** commands enable you to target different types of MPLS applications and network topologies. The various **ping mpls** and **trace mpls** commands send UDP packets, known as MPLS echo requests, to the egress LSR of MPLS packets in a given FEC. Each echo request is forwarded along the same data path as the MPLS packets in that FEC. The echo request packets use a destination address in the 127.0.0.0/8 range and port 3503. The default address is 127.0.0.1. This address range prevents IP from forwarding the packet, so that the echo request must follow the MPLS data path. This behavior is different from that of the IP **ping** and **traceroute** commands, which send ICMP packets to the actual destination. Each MPLS echo request packet contains information about the FEC stack that is being validated. LSRs that receive an MPLS echo request respond with MPLS echo reply packets. (Even when MPLS is not enabled on that router, echo reply packets are sent by routers that receive an echo request packet. This situation is a transient condition when the router is receiving labeled packets. A return code in the echo replies indicates to the sending router that no label mapping exists on the receiving router.)

The **ping mpls** commands perform a basic connectivity check. When the echo request exits the tunnel at the egress LSR, the LSR sends the packet to the control plane. The egress router validates the FEC stack to determine whether that LSR is the actual egress for the FEC. The egress router sends an echo reply packet back to the source address of the echo request packet. The egress router can send the packet back by means of either the IP path or the MPLS path. The **trace mpls** commands isolate faults in the LSP. For these commands, successive echo request packets are sent along the path. The first packet has a TTL of one; the TTL value is incremented by one for each successive packet. The first packet therefore reaches only the next hop on the path; the second packet reaches the next router after that. Echo request packets are sent until either an echo reply is received from the egress router for the FEC or a TTL of 32 is reached.

When a TTL expires on an LSR, that LSR sends an echo reply packet back to the source. For transit routers, the echo reply indicates that downstream mapping exists for the FEC, meaning that the packet would have been forwarded if the TTL had not expired. The

egress router sends an echo reply packet verifying that it is the egress. Although you cannot send IPv6 UDP packets for MPLS ping, you can use the **ping mpls l3vpn** command with an IPv6 prefix to investigate IPv6 VPNs.

For L3VPN services, the **ping mpls l3vpn** command is used to examine the operability of a MPLS Layer 3 VPN connection. For VPLS routing instances, the **ping vpls instance** command is used to examine the reachability of a VPLS instance. The **ping vpls instance** command uses a difference command structure and operates in a different fashion than the **ping mpls** command used for VPNs and Layer 2 circuits. For point-to-point services, the pseudowire ping mechanism is used to verify the network accessibility and identify any problems in the link.

Related Documentation

- [Clearing Interface Statistics on page 1237](#)
- [Viewing MAC Table Details on page 1239](#)
- [Viewing Interface Statistics on page 1241](#)
- [Viewing Interface Status Details on page 1243](#)
- [Using MPLS Ping on page 1247](#)
- [Pinging VPNs, VPLS, and Layer 2 Circuits on page 1249](#)
- [Monitoring Network Reachability by Using the MPLS Ping Capability on page 1250](#)
- [Monitoring Network Reachability by Using the Layer 3 VPN Ping Capability on page 1253](#)
- [Routing Table Overview on page 1256](#)

Using MPLS Ping

Use the MPLS ping functionality to diagnose the state of label-switched paths (LSPs), Layer 2 and Layer 3 virtual private networks (VPNs), and Layer 2 circuits. You can ping an MPLS endpoint using various options. You can send variations of ICMP echo request packets to the specified MPLS endpoint.

When you use the ping MPLS task from a Junos OS operating as the inbound (ingress) node at the entry point of an LSP or VPN, the routing platform sends probe packets into the LSP or VPN. Based on how the LSP or VPN outbound (egress) node at the remote endpoint of the connection replies to the probes, you can determine the connectivity of the LSP or VPN.

Each probe is an echo request sent to the LSP or VPN exit point as an MPLS packet with a UDP payload. If the outbound node receives the echo request, it checks the contents of the probe and returns a value in the UDP payload of the response packet. If the Junos OS receives the response packet, it reports a successful ping response.

Responses that take longer than 2 seconds are identified as failed probes.

[Table 175 on page 1248](#) lists the ping MPLS tasks, summarizes their functions, and identifies corresponding CLI **show** commands you can enter in the CLI interface of a device.

Table 175: Ping MPLS Tasks Summary and the Corresponding CLI show Commands

Ping MPLS Task	Corresponding CLI Command	Function	Additional Information
Ping RSVP-signaled LSP	<code>ping mpls rsvp</code>	Checks the operability of an LSP that has been set up by the Resource Reservation Protocol (RSVP). The Junos OS pings a particular LSP using the configured LSP name.	When an RSVP-signaled LSP has several paths, the Junos OS sends the ping requests on the path that is currently active.
Ping LDP-signaled LSP	<code>ping mpls ldp</code>	Checks the operability of an LSP that has been set up by the Label Distribution Protocol (LDP). The Junos OS pings a particular LSP using the forwarding equivalence class (FEC) prefix and length.	When an LDP-signaled LSP has several gateways, the Junos OS sends the ping requests through the first gateway. Ping requests sent to LDP-signaled LSPs use only the master routing instance.
Ping LSP to Layer 3 VPN prefix	<code>ping mpls l3vpn</code>	Checks the operability of the connections related to a Layer 3 VPN. The Junos OS tests whether a prefix is present in a provider edge (PE) router's VPN routing and forwarding (VRF) table, by means of a Layer 3 VPN destination prefix.	The Junos OS does not test the connection between a PE router and a customer edge (CE) router.
Ping LSP for a Layer 2 VPN connection by interface	<code>ping mpls l2vpn interface</code>	Checks the operability of the connections related to a Layer 2 VPN. The Junos OS directs outgoing request probes out the specified interface.	For information about interface names, see the CLI Explorer .
Ping LSP for a Layer 2 VPN connection by instance	<code>ping mpls l2vpn instance</code>	Checks the operability of the connections related to a Layer 2 VPN. The Junos OS pings on a combination of the Layer 2 VPN routing instance name, the local site identifier, and the remote site identifier, to test the integrity of the Layer 2 VPN circuit (specified by the identifiers) between the inbound and outbound PE routers.	
Ping LSP to a Layer 2 circuit remote site by interface	<code>ping mpls l2circuit interface</code>	Checks the operability of the Layer 2 circuit connections. The Junos OS directs outgoing request probes out the specified interface.	
Ping LSP to a Layer 2 circuit remote site by VCI	<code>ping mpls l2circuit virtual-circuit</code>	Checks the operability of the Layer 2 circuit connections. The Junos OS pings on a combination of the IPv4 prefix and the virtual circuit identifier on the outbound PE router, testing the integrity of the Layer 2 circuit between the inbound and outbound PE routers.	

Table 175: Ping MPLS Tasks Summary and the Corresponding CLI show Commands (continued)

Ping MPLS Task	Corresponding CLI Command	Function	Additional Information
Ping end point of LSP	<code>ping mpls lsp-end-point</code>	Checks the operability of an LSP endpoint. The Junos OS pings an LSP endpoint using either an LDP FEC prefix or an RSVP LSP endpoint address.	

- Related Documentation**
- [Clearing Interface Statistics on page 1237](#)
 - [Viewing MAC Table Details on page 1239](#)
 - [Viewing Interface Statistics on page 1241](#)
 - [Viewing Interface Status Details on page 1243](#)
 - [MPLS Connectivity Verification and Troubleshooting Methods on page 1245](#)
 - [Monitoring Network Reachability by Using the MPLS Ping Capability on page 1250](#)
 - [Monitoring Network Reachability by Using the Layer 3 VPN Ping Capability on page 1253](#)
 - [Routing Table Overview on page 1256](#)

Pinging VPNs, VPLS, and Layer 2 Circuits

For testing purposes, you can ping Layer 2 VPNs, Layer 3 VPNs, and Layer 2 circuits by using the `ping mpls` command. The `ping mpls` command helps to verify that a VPN or circuit has been enabled and tests the integrity of the VPN or Layer 2 circuit connection between the PE routers. It does not test the connection between a PE router and a CE router. To ping a VPLS routing instance, you issue a `ping vpls instance` command.

You issue the `ping mpls` command from the ingress PE router of the VPN or Layer 2 circuit to the egress PE router of the same VPN or Layer 2 circuit. When you execute the `ping mpls` command, echo requests are sent as MPLS packets.

The payload is a User Datagram Protocol (UDP) packet forwarded to the address `127.0.0.1`. The contents of this packet are defined in RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*. The label and interface information for building and sending this information as an MPLS packet is the same as for standard VPN traffic, but the time-to-live (TTL) of the innermost label is set to 1.

When the echo request arrives at the egress PE router, the contents of the packet are checked, and then a reply that contains the correct return is sent by means of UDP. The PE router sending the echo request waits to receive an echo reply after a timeout of 2 seconds (you cannot configure this value).

You must configure MPLS at the `[edit protocols mpls]` hierarchy level on the egress PE router (the router receiving the MPLS echo packets) to be able to ping the VPN or Layer 2 circuit. You must also configure the address `127.0.0.1/32` on the egress PE router's `lo0`

interface. If this is not configured, the egress PE router does not have this forwarding entry and therefore simply drops the incoming MPLS pings.

The **ping mpls** command has the following limitations:

- You cannot ping an IPv6 destination prefix.
- You cannot ping a VPN or Layer 2 circuit from a router that is attempting a graceful restart.
- You cannot ping a VPN or Layer 2 circuit from a logical system.

You can also determine whether an LSP linking two PE routers in a VPN is up by pinging the end point address of the LSP. The command you use to ping an MPLS LSP end point is **ping mpls lsp-end-point address**. This command tells you what type of LSP (RSVP or LDP) terminates at the address specified and whether that LSP is up or down.

Related Documentation

- [Clearing Interface Statistics on page 1237](#)
- [Viewing MAC Table Details on page 1239](#)
- [Viewing Interface Statistics on page 1241](#)
- [Viewing Interface Status Details on page 1243](#)
- [MPLS Connectivity Verification and Troubleshooting Methods on page 1245](#)
- [Using MPLS Ping on page 1247](#)
- [Monitoring Network Reachability by Using the MPLS Ping Capability on page 1250](#)
- [Monitoring Network Reachability by Using the Layer 3 VPN Ping Capability on page 1253](#)
- [Routing Table Overview on page 1256](#)

Monitoring Network Reachability by Using the MPLS Ping Capability

In IP networks, you can use the **ping** and **traceroute** commands to verify network connectivity and find broken links or loops. In an MPLS-enabled network, you can use the **mpls ping** and **trace mpls** commands to detect plane failures in different types of MPLS applications and network topologies.

To perform an MPLS ping operation:

1. From the View selector, select **Service View**.
The functionalities that you can configure in this view are displayed on the View pane in the GUI window.
2. Click the **Monitor** mode icon in the Service View on the Connectivity Services Director banner.
The workspaces that are applicable to this mode are displayed in the GUI window.
3. On the Service View pane, on the left, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.

4. Click the plus sign (+) beside Connectivity to view services based on protocols.
 - Expand the **P2P Services** tree to select a point-to-point service.
 - Expand the **VPLS Services** tree to select a VPLS service.
5. From the Tasks pane, select **MPLS Ping**.

The MPLS Ping Service Type - Service Name window appears.



NOTE: A warning message is displayed in the window stating that the MPLS echo request to the device might be timed out if the response is delayed from the device.

The screenshot shows the 'MPLS Ping-P2P-P2P_Traffic_R1-R4' window. It has a blue title bar with a help icon and a close button. The window is divided into several sections:

- Endpoint Device:** Contains two dropdown menus. 'Source Device' is set to '480R4_SV_Alok_re' and 'Destination Device' is set to '960R1_SV_Alok_re'.
- Advance Options:** Contains four input fields and one checkbox. 'Ping Count(packets):' is set to '1..1000000 packets'. 'Ping Size(bytes):' is set to '1..65468 bytes'. 'Forwarding Class:' is set to '(0..7)'. 'Reply Mode:' is a dropdown menu. There is an unchecked checkbox labeled 'Sweep'.
- Reply:** Contains a 'Format:' dropdown menu set to 'ASCII'.
- Ping Button:** A button labeled 'Ping' is located below the 'Reply' section.
- Response Console:** A large text area showing the results of the ping. The text reads:


```
Results for - MPLS Ping (L2Circuit)
Packets Transmitted :
5

Packets Received :
5

Packet Loss :
0

Error Packets :
0
```
- Close Button:** A button labeled 'close' is located at the bottom right of the window.



NOTE: MPLS ping is supported only from managed endpoints to unmanaged endpoints. Therefore, unmanaged endpoints are not listed in the Source column.

For a BGP-based P2P service, with one endpoint as an unmanaged device, the MPLS ping utility is not supported because the remote site ID of the unmanaged device is not available as part of the service configuration. The remote site ID is required for MPLS ping from a managed to an unmanaged endpoint.

6. In the Endpoint Device section, do the following:

The source device sends an MPLS echo request packet to the specified IP or IPv6 address or, alternatively, sends MPLS echo packets to the egress node in a point-to-multipoint LSP. The MPLS echo request packets and echo reply packets created by this command use the LDP IPv4 LSP sub-TLV described in RFC 4379—Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures (February 2006).

- a. From the Source Device list, select the source device, whose IP address is to be used as the packet source address.
- b. From the Destination Device list, select the target endpoint, whose IP address is used as the target IP address for MPLS ping packets or echo requests.

7. On the Advance Options list, do the following:

- a. In the Ping count (packets) field, enter the number of packets to send to the destination address, in the range 0–4294967295. The default value is 5 and 0 (zero) means ping forever.
- b. In the Ping size (bytes) field, specify the number of bytes comprising the MPLS packet, including the header, in the range 0–64000. The default value is 100 bytes.
- c. In the Forwarding Class field, specify the value of the forwarding class for the MPLS ping packets.
- d. In the Sweep field, configure the payload size, which enables you to vary the sizes of the echo packets being sent. This capability is useful for determining the minimum sizes of the MTUs configured on the nodes along the path to the destination address. This reduces packet fragmentation, which contributes to performance problems. The default is not to sweep; all packets are of the same size.
- e. From the Reply Mode field, select the reply mode for the echo request packet:
 - **IP-UDP**—Specifies that the echo request packet is an IPv4 UDP packet
 - **Application Level Control Channel**—Specifies that the echo request packet is replied using the application-level control channel connection.

8. From the Format list, select **XML** to display the result or the response of the MPLS ping operation in XML format. Alternatively, select **ASCII** to display the output in the format in which it is displayed on the CLI. The Junos XML API is an XML representation of Junos configuration statements and operational mode commands. Junos XML configuration tag elements are the contents to which the Junos XML protocol operations apply. Junos XML operational tag elements are equivalent in function to operational mode commands on the CLI, which administrators use to retrieve status information for a device.
9. Click **Ping** to start the ping operation and to send the MPLS echo requests from the source to the destination device.

The results of the ping operation are displayed in the Response Console pane at the bottom of the MPLS Ping Service Type - Service Name window.

Related Documentation

- [MPLS Connectivity Verification and Troubleshooting Methods on page 1245](#)
- [Using MPLS Ping on page 1247](#)
- [Pinging VPNs, VPLS, and Layer 2 Circuits on page 1249](#)
- [Monitoring Network Reachability by Using the MPLS Ping Capability on page 1250](#)
- [Monitoring Network Reachability by Using the Layer 3 VPN Ping Capability on page 1253](#)

Monitoring Network Reachability by Using the Layer 3 VPN Ping Capability

In IP networks, you can use the **ping** and **traceroute** commands to verify network connectivity and find broken links or loops. In an MPLS-enabled network, you can use the **mpls ping** and **trace mpls** commands to detect plane failures in different types of MPLS applications and network topologies.

1. From the View selector, select Service View.
The functionalities that you can configure in this view are displayed on the View pane.
2. Click the **Monitor** mode icon in the Service View of the Connectivity Services Director banner.
The workspaces that are applicable to this mode are displayed on the Tasks pane.
3. Click the plus sign (+) beside Connectivity to view services based on protocols.
4. Expand the **L3VPN Services** tree to select a Layer 3 VPN Ethernet service.
5. From the Tasks pane, select **MPLS Ping**.
The MPLS Ping Service Type - Service Name window appears.

MPLS Traceroute-LSP(RSVP)-Fullmesh

Endpoint Device

Ingress Device: 480R4_SV_Alok_re

Egress Device: 960R1_SV_Alok_re

LSP Name: Fullmesh_480R4_SV_Alok_re_to_128_102_163_58

Advance Options

Hop Limit: (1..255)

Probe Retries: (1..9)

Class Of Service: (0..7)

Reply

Format: ASCII

Traceroute

Response Console:

```
Results for - MPLS Traceroute (RSVP)
Hop Depth : Current Hop : Previous Hop :
1 : 40.2.4.1 : (null) :
2 : 40.1.2.1 : 40.2.4.1 :
```

close

6. In the Endpoint Device section, do the following:

The source device sends an MPLS echo request packet to the specified IP or IPv6 address or, alternatively, sends MPLS echo packets to the egress node in a point-to-multipoint LSP. The MPLS echo request packets and echo reply packets created by this command use the LDP IPv4 LSP sub-TLV described in RFC 4379—Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures (February 2006).

- a. From the Source Device list, select the source device, whose IP address is to be used as the packet source address.
- b. From the Destination Device list, select the target endpoint, whose IP address is used as the target IP address for MPLS ping packets or echo requests.

7. On the Advance Options list, do the following:

- a. In the Ping count (packets) field, enter the number of packets to send to the destination address, in the range 0–4294967295. The default value is 5 and 0 (zero) means ping forever.
 - b. In the Ping size (bytes) field, specify the number of bytes comprising the MPLS packet, including the header, in the range 0–64000. The default value is 100 bytes.
 - c. In the Forwarding Class field, specify the value of the forwarding class for the MPLS ping packets.
 - d. In the Sweep field, configure the payload size, which enables you to vary the sizes of the echo packets being sent. This capability is useful for determining the minimum sizes of the MTUs configured on the nodes along the path to the destination address. This reduces packet fragmentation, which contributes to performance problems. The default is not to sweep; all packets are of the same size.
 - e. From the Reply Mode field, select the reply mode for the echo request packet:
 - **IP-UDP**—Specifies that the echo request packet is an IPv4 UDP packet
 - **Application Level Control Channel**—Specifies that the echo request packet is replied using the application-level control channel connection.
8. From the Format list, select **XML** to display the result or the response of the MPLS ping operation in XML format. Alternatively, select **ASCII** to display the output in the format in which it is displayed on the CLI. The Junos XML API is an XML representation of Junos configuration statements and operational mode commands. Junos XML configuration tag elements are the contents to which the Junos XML protocol operations apply. Junos XML operational tag elements are equivalent in function to operational mode commands on the CLI, which administrators use to retrieve status information for a device.
 9. Click **Ping** to start the ping operation and to send the MPLS echo requests from the source to the destination device.

The results of the ping operation are displayed in the Response Console pane at the bottom of the MPLS Ping Service Type - Service Name window.

Related Documentation

- [Clearing Interface Statistics on page 1237](#)
- [Viewing MAC Table Details on page 1239](#)
- [Viewing Interface Statistics on page 1241](#)
- [Viewing Interface Status Details on page 1243](#)
- [MPLS Connectivity Verification and Troubleshooting Methods on page 1245](#)
- [Using MPLS Ping on page 1247](#)
- [Pinging VPNs, VPLS, and Layer 2 Circuits on page 1249](#)
- [Monitoring Network Reachability by Using the MPLS Ping Capability on page 1250](#)

Routing Table Overview

Typically, routers are attached to multiple networks and are responsible for directing traffic across these networks. Each router maintains a routing table, which is a list of known networks and directions on how to reach them. While processing an incoming packet on a security device, the router performs a routing table lookup to find the appropriate interface that leads to the destination address.

Each entry in a routing table—called a *route entry* or *route*—is identified by the destination network to which traffic can be forwarded. The destination network, in the form of an IP address and netmask, can be an IP network, subnet, supernet, or a host. Routing table entries can originate from the following sources:

- Directly connected networks (the destination network is the IP address that you assign to an interface in Route mode)
- Dynamic routing protocols, such as OSPF, BGP, or RIP
- Routes that are imported from other routers or virtual routers
- Statically configured routes

You can configure three types of static routes: destination-based, source-based, and source-interface-based routing. For each type of static route, you configure the following information:



NOTE: Source-interface-based routing is supported in ScreenOS 5.1 and later.

- The interface on the security device on which traffic for the destination network is forwarded.
- The next-hop, which can be either another virtual router on the security device or a gateway IP address (usually a router address).
- The protocol from which the route is derived.

Related Documentation

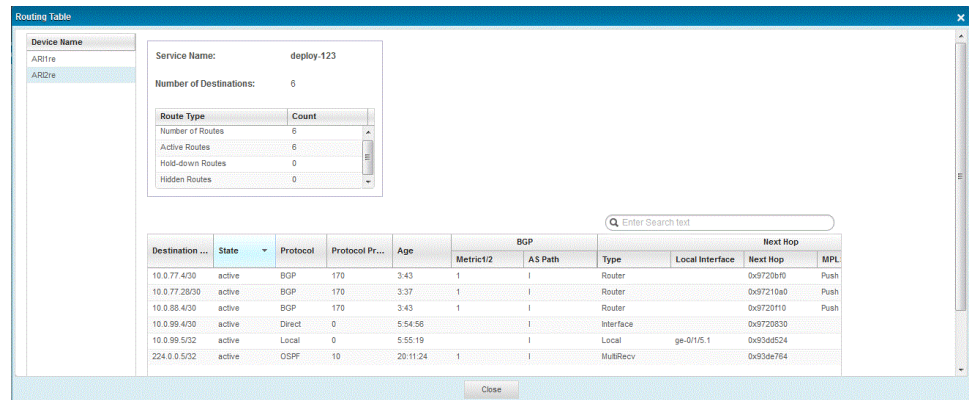
- [MPLS Connectivity Verification and Troubleshooting Methods on page 1245](#)
- [Using MPLS Ping on page 1247](#)
- [Pinging VPNs, VPLS, and Layer 2 Circuits on page 1249](#)

Viewing Routing Table Details

The Routing Table window enables you view the routing table information for the selected virtual routing instance. For L3VPN services, you can determine which LSPs or tunnels are being used by looking at the routing tables.

To view extensive information about the active entries in the routing tables for a device associated with a particular service:

1. From the View selector, select Service View. The functionalities that you can configure in this view are displayed.
2. Click the Monitor mode icon in the Service View of the Connectivity Services Director banner. The workspaces that are applicable to this mode are displayed.
3. From the Service View pane, select the L3VPN service for which you want to view interface statistics. The service statistical details are displayed in the middle pane.
4. From the task pane, which is displayed on the rightmost pane, select Tasks > Routing Table. The Routing Table window is displayed. The left pane of the window displays the names of the devices that are associated with the particular service.



5. From the Device Name pane, select the device for which you want to view the routing table information. The following information is displayed in the right pane of the window in a tabular grid.

Table 176: Routing Table Window Field Descriptions

Name	Description
Service Name	Name of the service for which routing table statistics are displayed.
Number of Destinations	Number of destinations for which routes are present in the routing table.
Number of Routes	Total number of routes in the routing table.
Active Routes	Number of routes that are active.
Hidden Routes	Number of routes that are not used because of routing policy.
Hold-down Routes	Number of routes that are in the hold-down state before being declared inactive.

Table 176: Routing Table Window Field Descriptions (continued)

Name	Description
Destination Prefix	<p>Route destination (for example:10.0.0.1/24). Sometimes the route information is presented in another format, such as:</p> <ul style="list-style-type: none"> • MPLS-label (for example, 80001). • interface-name (for example, ge-1/0/2). • neighbor-address:control-word-status:encapsulation type:vc-id:source (Layer 2 circuit only. For example, 10.1.1.195:NoCtrlWord:1:1:Local/96): <ul style="list-style-type: none"> • neighbor-address—Address of the neighbor. • control-word-status—Whether the use of the control word has been negotiated for this virtual circuit: NoCtrlWord or CtrlWord. • encapsulation type—Type of encapsulation, represented by a number: (1) Frame Relay DLCI, (2) ATM AAL5 VCC transport, (3) ATM transparent cell transport, (4) Ethernet, (5) VLAN Ethernet, (6) HDLC, (7) PPP, (8) ATM VCC cell transport, (10) ATM VPC cell transport. • vc-id—Virtual circuit identifier. • source—Source of the advertisement: Local or Remote.
State	State of the route.
Protocol	Name of the protocol from which the route was learned. For example, OSPF , RSVP , and Static .
Protocol Preference	Preferred protocol for this routing instance. Junos OS uses this preference to choose which routes become active in the routing table.
Age	Displays how long since the route was learned.
BGP Metric	Cost value of the indicated route. For routes within an AS, the cost is determined by the IGP and the individual protocol metrics. For external routes, destinations, or routing domains, the cost is determined by a preference value.
BGP Local Preference	A metric used by BGP sessions to indicate the degree of preference for an external route. The route with the highest local preference value is preferred.
AS Path	<p>AS path through which the route was learned. The letters at the end of the AS path indicate the path origin, providing an indication of the state of the route at the point at which the AS path originated:</p> <ul style="list-style-type: none"> • I—IGP. • E—EGP. • Recorded—The AS path is recorded by the sample process (sampled). • ?—Incomplete; typically, the AS path was aggregated. <p>When AS path numbers are included in the route, the format is as follows:</p> <ul style="list-style-type: none"> • []—Brackets enclose the local AS number associated with the AS path if more than one AS number is configured on the routing device, or if AS path prepending is configured. • { }—Braces enclose AS sets, which are groups of AS numbers in which the order does not matter. A set commonly results from route aggregation. The numbers in each AS set are displayed in ascending order. • ()—Parentheses enclose a confederation. • ([])—Parentheses and brackets enclose a confederation set.

Table 176: Routing Table Window Field Descriptions (continued)

Name	Description
Next Hop Type	Next hop to the destination. An angle bracket (>) indicates that the route is the selected route. If the destination is Discard, traffic is dropped.
Local Interface	The local interface used to reach the next hop.
Next Hop	Next-hop address of the interface.
MPLS Label	MPLS label and operation occurring at the next hop. The operation can be pop (where a label is removed from the top of the stack), push (where another label is added to the label stack), or swap (where a label is replaced by another label).

6. Click Close after you complete viewing the details. You are returned to the main or home page in Monitor Mode of Service View, which is the Service Summary tab.

PART 14

Working in Fault Mode

- [About Fault Mode on page 1263](#)
- [Using Fault Mode on page 1267](#)
- [Fault Reference on page 1277](#)

About Fault Mode

- [About Fault Mode in All Views of Connectivity Services Director on page 1263](#)
- [Understanding the Tasks Pane in Fault Mode on page 1264](#)

About Fault Mode in All Views of Connectivity Services Director

Fault mode in Connectivity Services Director provides you visibility into your network status and performance by displaying alarms and events generated on devices and configured services on devices. Connectivity Services Director monitors its managed devices and maintains the information it collects from the devices in a database. Fault mode displays this information in easy-to-understand graphs and in tables that you can sort and filter, allowing you to quickly visualize the state of your network, spot trends developing over time, and find important details. When certain types of events are persistent, or when the condition causing the event crosses a threshold, SNMP sends a notification, also called a trap to Connectivity Services Director.

Connectivity Services Director correlates traps, describing a condition, into an alarm. For example, multiple power supply traps coming from a device are correlated into a single power supply alarm for the device. The main purpose and benefit of monitoring functionalities is to allow the operators to quickly monitor the health (working condition), operating efficiency, traffic-handling capacity, and performance status of the managed devices and configured services such as P2P, VPLS, and L3VPN.

The monitoring mechanism is tool that enables the operator to understand the network health and status by drilling down to all the components of a device. The device status is marked as green, red, orange, or blue, based on the health, availability, performance and other important key performance indicators.

- Red denotes an emergency condition, which is a system panic or other conditions that cause the routing platform to stop functioning. It also indicates that the device is offline or turned down.
- Orange denotes an alert, which can be conditions that must be corrected immediately, such as a corrupted system database.

- Yellow indicates a notice, which signifies conditions that are not error conditions but are of interest or might warrant special handling. It can also include a severity level equivalent to informational or debugging messages.
- Blue denotes an informational message; no action is necessary. Informational alarms do not necessarily indicate an error. It could indicate that a device or entity has changed state.

**Related
Documentation**

- [About Build Mode in Service View of Connectivity Services Director on page 41](#)
- [About Deploy Mode in Service View of Connectivity Services Director on page 43](#)
- [About Monitor Mode in Service View of Connectivity Services Director on page 45](#)

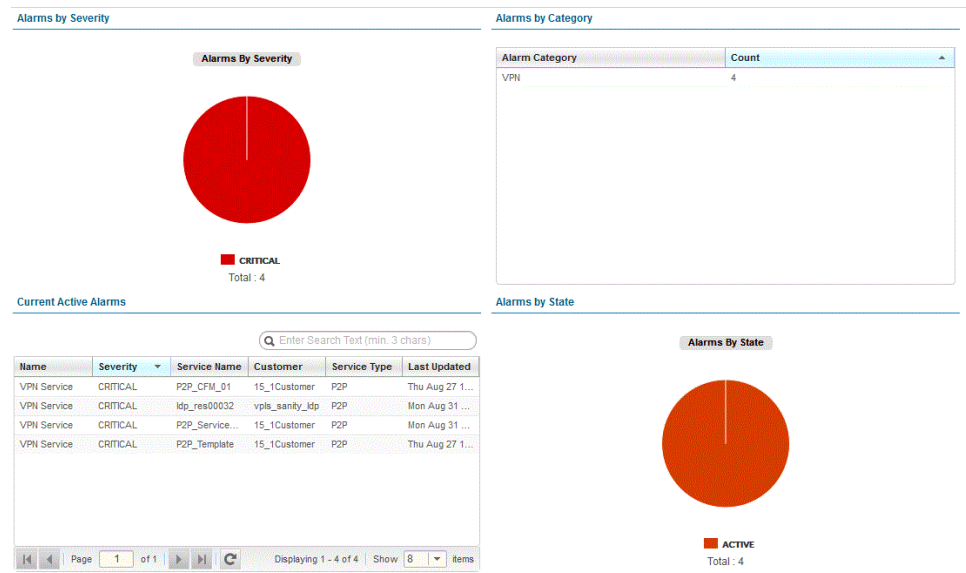
Understanding the Tasks Pane in Fault Mode

The Tasks pane in Fault mode provides you with a set of tools for effectively managing alarms on your system.

From the Tasks pane, you can:

- Filter known alarms to locate a specific alarm or error condition by clicking Search Alarms. Use this task to isolate alarms that occurred during a known time-frame or that have annotations associated with them. Although each of the Fault mode monitors can sort the alarms, Search Alarms enable you to submit multiple search and sort arguments as part of your search query.

In addition, Connectivity Services Director enables you to group the tasks that you perform frequently and create a list of key tasks. You can add any task from the Tasks pane to the Key Tasks list by selecting a task and clicking the plus (+) sign that appears adjacent to the task. For some modes, you can see that Connectivity Services Director has predefined some key tasks for you. You can modify this set of tasks to suit your requirements. This feature is available in Task pane irrespective of your current mode, scope, or view.



Related Documentation

- [Understanding the Service View Tasks Pane in Build Mode on page 33](#)
- [Understanding the Service View Tasks Pane in Deploy Mode on page 36](#)
- [Understanding the Service View Tasks Pane in Monitor Mode on page 38](#)
- [About Build Mode in Service View of Connectivity Services Director on page 41](#)
- [About Deploy Mode in Service View of Connectivity Services Director on page 43](#)
- [About Fault Mode in All Views of Connectivity Services Director on page 45](#)
- [About Monitor Mode in Service View of Connectivity Services Director on page 45](#)

CHAPTER 46

Using Fault Mode

- [Using Fault Management Monitors on page 1267](#)
- [Alarm Severities and States Overview on page 1270](#)
- [Events and Alarms Overview on page 1271](#)
- [Customizing Alarms on page 1272](#)
- [Changing Alarm State on page 1272](#)
- [Searching Alarms on page 1273](#)

Using Fault Management Monitors

The Fault mode shows you information about the health of your network and changing conditions of your equipment. Use Fault mode to find problems with equipment, pinpoint security attacks, or to analyze trends and categories of errors.

This topic describes:

- [What Are Events and Alarms? on page 1267](#)
- [Alarm Severity on page 1268](#)
- [Alarm Classification on page 1268](#)
- [Alarm State on page 1269](#)
- [Alarm Notifications on page 1269](#)
- [Threshold Alarms on page 1270](#)

What Are Events and Alarms?

Activity on a network device consists of a series of *events*. A software component on the network device, called an *entity*, is responsible for running the Simple Network Management Protocol (SNMP) to log and monitor these events. When certain types of events are persistent, or when the condition causing the event crosses a threshold, SNMP sends a notification, also called a *trap* to Connectivity Services Director. Connectivity Services Director correlates traps, describing a condition, into an *alarm*. For example, multiple power supply traps coming from a device are correlated into a single power supply alarm for the device.

There are many types of alarms. An alarm can be as routine as when the device changes state or as serious as when a power supply has failed. When an alarm is sent, or *raised*,

it stays raised until the triggering condition is resolved or *cleared*. The system can clear the alarm when the state changes again or an administrator can clear it manually, which indicates that the condition is now resolved.

SNMP also plays another role in Connectivity Services Director. Enabling devices for SNMP with the appropriate read-only V1/V2/V3 credentials, can speed up device discovery.

Alarm Severity

Alarms are ranked by their impact to the network. The following list shows the ranking of alarms in Connectivity Services Director from alarms that have the most impact to alarms that have the least impact on the network. It also shows the color scheme associated with each level of severity that is reflected in related graphs.

Critical (Red)—A critical condition exists; immediate action is necessary.

Major (Orange)—A major error has occurred; escalate or notify as necessary.

Minor (Yellow)—A minor error has occurred; notify or monitor the condition.

Info (Blue)—An informational message; no action is necessary. Informational alarms do not necessarily indicate an error. It could indicate that a device or entity has changed state.

Administrators can override the default severity of an alarm and set the severity to match their inhouse guidelines. Changing the severity level for an alarm is done on the Fault tab of System Preferences.

Alarm Classification

Connectivity Services Director organizes alarms into categories so you can view trends in the types of errors occurring on a network. These categories, shown in [Table 177 on page 1268](#) are derived from the SNMP Management Information Base (MIB) that is the information database or module containing the trap information for the event.

Table 177: Connectivity Services Director Alarm Classifications

Category	Description
BFD	Indicates alarms for Bidirectional Forwarding Detection sessions. These alarms are generated from routing devices.
BGP	Indicates alarms for BGP4.
Chassis	Indicates alarms for device hardware, in this case, routers.
Cluster/Modo	Indicates alarms about wireless network clusters and mobility domains.
Configuration	Indicates alarms for configuration management.
Controllers	Indicate device alarms.

Table 177: Connectivity Services Director Alarm Classifications (continued)

Category	Description
CoS	Indicates class of service alarms.
DHCP	Indicates local server DHCP alarms.
DOM	Indicates Digital Optical Monitoring alarms that are generated from optical interfaces.
General	Indicates alarms that are common to all network devices, such as link up/down or authentication.
L2ALD	Indicates MAC address alarms generated from the Layer 2 Address Learning Daemon (L2ALD).
L2CP	Indicates alarms generated by Layer 2 Control Protocol features.
MACFDB	Indicates an alarm for when MAC addresses are learned or removed from the forwarding database of the monitored device.
Misc	Indicates alarms that do not fit into the other categories.
Network Service	Indicates alarms generated when LSP or VPN services are impacted
PassiveMonitoring	Indicates alarms that occur on a passive monitoring interface.
Ping	Indicates alarms that are generated during a Ping request.
RMon	Indicates RMON alarms

Alarm State

Once an alarm is active, it has one of these states:

- **Active**—Alarms that are current and not yet acknowledged or cleared.
- **Cleared**—Alarms that are resolved and the device or entity has returned to normal operation.

Some alarm states go directly from active to cleared state and require little to no administrative effort. However, other alarms with a high severity should be acknowledged and investigated.

In addition to acknowledging and clearing an alarm, you can assign an alarm to someone and you can append a note or annotation to an alarm. Annotations are helpful for documenting the resolution of an alarm or time estimates for a fix. Changes to an alarm's state are made through the Alarm State monitor in Fault mode.

Alarm Notifications

Alarms can be enabled for email notification. When an alarm with notification enabled is generated, an email is sent to a set of specified addresses. There is a list of global email

addresses that receive notifications from all alarms with notification enabled. Each alarm type can also have a list of addresses that receive notification when that alarm type is generated. Administrators can enable notification for alarm types and specify addresses to receive email notifications. These tasks are done on the Fault tab of System Preferences.

Threshold Alarms

Threshold alarms are alarms that are generated when a monitored value crosses the configured threshold. They provide enhanced visibility into potential issues on the network. Administrators configure and manage threshold alarms the same way as other alarms, and can set the threshold level of individual threshold alarms on the Fault tab of System Preferences.

Related Documentation

- [Alarm Severities and States Overview on page 1270](#)
- [Events and Alarms Overview on page 1271](#)
- [Customizing Alarms on page 1272](#)
- [Changing Alarm State on page 1272](#)
- [Searching Alarms on page 1273](#)
- [Alarm Detail Monitor \(Service View\) on page 1280](#)
- [Alarm Trend Monitor \(Service View\) on page 1287](#)
- [Alarms by Category Monitor on page 1285](#)
- [Alarms by Severity Monitor \(Service View\) on page 1285](#)
- [Alarms by State Monitor on page 1286](#)
- [Current Active Alarms Monitor \(Service View\) on page 1284](#)

Alarm Severities and States Overview

By default, the Junos Space Network Management Platform is monitored using a built-in SNMP manager. The Junos Space Network Management Platform node is listed in the node list (Network Monitoring > Node List), and is referred to as the Junos Space Network Management Platform node.

Alarm Severity

Alarms are ranked by their impact to the network. The following list shows the ranking of alarms in Connectivity Services Director from alarms that have the most impact to alarms that have the least impact on the network. It also shows the color scheme associated with each level of severity that is reflected in related graphs.

Critical (Red)—A critical condition exists; immediate action is necessary.

Major (Orange)—A major error has occurred; escalate or notify as necessary.

Minor (Yellow)—A minor error has occurred; notify or monitor the condition.

Info (Blue)—An informational message; no action is necessary. Informational alarms do not necessarily indicate an error. It could indicate that a device or entity has changed state.

Administrators can override the default severity of an alarm and set the severity to match their inhouse guidelines. Changing the severity level for an alarm is done on the Fault tab of System Preferences.

Alarm State

Once an alarm is active, it has one of these states:

- **Active**—Alarms that are current and not yet acknowledged or cleared.
- **Cleared**—Alarms that are resolved and the device or entity has returned to normal operation.

Some alarm states go directly from active to cleared state and require little to no administrative effort. However, other alarms with a high severity should be acknowledged and investigated.

In addition to acknowledging and clearing an alarm, you can assign an alarm to someone and you can append a note or annotation to an alarm. Annotations are helpful for documenting the resolution of an alarm or time estimates for a fix. Changes to an alarm's state are made through the Alarm State monitor in Fault mode.

Events and Alarms Overview

Activity on a network device consists of a series of events. A software component on the network device, called an entity, is responsible for running the Simple Network Management Protocol (SNMP) to log and monitor these events. When certain types of events are persistent, or when the condition causing the event crosses a threshold, SNMP sends a notification, also called a trap to Connectivity Services Director. Connectivity Services Director correlates traps, describing a condition, into an alarm. For example, multiple power supply traps coming from a device are correlated into a single power supply alarm for the device. There are many types of alarms. An alarm can be as routine as when the device changes state or as serious as when a power supply has failed. When an alarm is sent, or raised, it stays raised until the triggering condition is resolved or cleared. The system can clear the alarm when the state changes again or an administrator can clear it manually, which indicates that the condition is now resolved. SNMP also plays another role in Connectivity Services Director. Enabling devices for SNMP with the appropriate read-only V1/V2/V3 credentials, can speed up device discovery.

Alarm Severity

Alarms are ranked by their impact to the network. The following list shows the ranking in Connectivity Services Director from most impact to least impact on the network. It also shows the color scheme associated with each level of severity that is reflected in related graphs.

- Critical (Red)—A critical condition exists; immediate action is necessary.
- Major (Orange)—A major error has occurred; escalate or notify as necessary.
- Minor (Yellow)—A minor error has occurred; notify or monitor the condition.
Administrators can override the default severity of an alarm and set the severity to match their inhouse guidelines. Changing the severity level for an alarm is done on the Alarm Settings page in system Preferences.

Customizing Alarms

Ensure that all devices are enabled for SNMP trap forwarding. This task, Set SNMP Trap Configuration, is found in Deploy mode.

Connectivity Services Director enables you to tailor alarms by:

- Enabling or disabling individual alarms.
- Setting the amount of time alarms are retained in the system.

You can customize alarms using Preferences in the Connectivity Services Director banner.

Related Documentation

- *Setting Up User and System Preferences*

Changing Alarm State

When an alarm becomes active, it remains active until either the system determines that the condition is resolved or system personnel change the status. Critical alarms always need immediate attention and seldom resolve on their own, but informational messages are often expected actions and results. When a condition is severe or persistent and needs attention, follow these steps:

1. Locate the alarm.
 - a. Click **Fault** in the Connectivity Services Director banner to enter Fault mode.
 - b. Click the Alarm Details icon on any of the monitors to open the Alarm Details page. Scroll or sort the alarms to find the alarm in question. As an alternate method, click **Search Alarms** in the Tasks pane and filter the active alarm list.
 - c. Select the alarm.
2. Review the Event Details that triggered the trap for the alarm. These events provide insight into the cause or location of the problem.

3. Click **Acknowledge** to indicate that the problem is now known. You should receive a message saying the alarm is acknowledged.
4. Depending whether you can resolve the alarm with the information at hand or not, either assign the alarm to a member of your staff or clear the alarm. Click **Clear** to clear the alarm or click **Assign** and fill in the assignee's name.

At any time in the life cycle of an alarm, you can attach information about the alarm to the alarm record by clicking **Annotate**. Fill in your name in the **Notes By** field and add the note description in the **Notes** field. Click **Add** to record the annotation.

Related Documentation

- [Using Fault Management Monitors on page 1267](#)
- [Alarm Severities and States Overview on page 1270](#)
- [Events and Alarms Overview on page 1271](#)
- [Customizing Alarms on page 1272](#)
- [Searching Alarms on page 1273](#)
- [Alarm Detail Monitor \(Service View\) on page 1280](#)
- [Alarm Trend Monitor \(Service View\) on page 1287](#)
- [Alarms by Category Monitor on page 1285](#)
- [Alarms by Severity Monitor \(Service View\) on page 1285](#)
- [Alarms by State Monitor on page 1286](#)
- [Current Active Alarms Monitor \(Service View\) on page 1284](#)

Searching Alarms

Use Search Alarms, available from the Tasks pane, to filter and isolate information about a specific alarm. Use this page to specify complex sorting and filtering criteria for all alarms.

Each field in the Search Alarm window helps narrow the current list of alarms. The more search items you specify, the more specific your results. All fields are optional.

1. Select or type the known descriptors for the alarm. These fields are described in [Table 178 on page 1274](#).
2. Click **Search** to run the query. The Alarms Details page opens with the results of your search.
3. Review the alarm. From this page you can change the state of the alarm, annotate, or assign the alarm to personnel. For more information about changing the state of an alarm, view ["Changing Alarm State" on page 1272](#).

Table 178: Alarm Search Fields

Search Criteria	Description
State	<p>Use the list to select which alarm states to search for:</p> <ul style="list-style-type: none"> • All—Alarms of all states. • Active—Alarms that are current and not yet acknowledged or cleared. • Clear—Alarms that are resolved and the device or entity has returned to normal operation.
Category	<p>Fill in one of the available alarm categories:</p> <ul style="list-style-type: none"> • AP/Radio • BFD • BGP • Chassis • ClientAndUserSession • Cluster/Modo • Configuration • Controllers • CoS • DHCP • DOM • FlowCollection • GENERAL • GenericEvent • L2ALD • L2CP • MACFDB • Misc • PassiveMonitoring • Ping • RFDetect • RMon • SONET • SONETAPS • VirtualChassis • VNetwork
Severity	<p>Pull down the list to select the severity level. Not all possible alarm severities are listed. Only the severity levels of your current active alarms are shown. Possible selections are:</p> <ul style="list-style-type: none"> • Critical • Major • Minor • Info
Advanced Search Criteria	
(from) Date	Pull down the calendar and select the starting date of the search.

Table 178: Alarm Search Fields (continued)

Search Criteria	Description
(from) Time	Pull down the list to select the starting time of the search. Search times are in military (24-hour) clock format in 30 minute intervals.
(to) Date	Pull down the calendar and select the ending date of the search.
(to) Time	Pull down the list to select the ending time of the search. Search times are in military (24-hour) clock format in 30 minute intervals.
Notes	Enter any keywords or phases that were listed in an existing annotation.

**Related
Documentation**

- [Using Fault Management Monitors on page 1267](#)
- [Alarm Severities and States Overview on page 1270](#)
- [Events and Alarms Overview on page 1271](#)
- [Customizing Alarms on page 1272](#)
- [Changing Alarm State on page 1272](#)
- [Alarm Detail Monitor \(Service View\) on page 1280](#)
- [Alarm Trend Monitor \(Service View\) on page 1287](#)
- [Alarms by Category Monitor on page 1285](#)
- [Alarms by Severity Monitor \(Service View\) on page 1285](#)
- [Alarms by State Monitor on page 1286](#)
- [Current Active Alarms Monitor \(Service View\) on page 1284](#)

CHAPTER 47

Fault Reference

- [Alarm Detail Monitor \(All Views Except Service View\) on page 1277](#)
- [Alarm Detail Monitor \(Service View\) on page 1280](#)
- [Current Active Alarms Monitor \(Service View\) on page 1284](#)
- [Alarms by Category Monitor on page 1285](#)
- [Alarms by Severity Monitor \(Service View\) on page 1285](#)
- [Alarms by State Monitor on page 1286](#)
- [Alarm Trend Monitor \(Service View\) on page 1287](#)
- [Alarms by Severity Monitor \(All Views Except Service View\) on page 1287](#)
- [Alarms by State Monitor \(All Views Except Service View\) on page 1288](#)
- [Current Active Alarms Monitor \(All Views Except Service View\) on page 1288](#)
- [Alarm Trend Monitor \(All Views Except Service View\) on page 1289](#)

Alarm Detail Monitor (All Views Except Service View)

Use the Alarm Detail monitor to sort alarms, view an alarm in depth, and to assign a disposition to an alarm.

By clicking the Details icon, you can access the Alarm Detail monitor from any of the four alarm monitors available on the main page in Fault mode (Severity, Category, Current, or State). It is also available from the Current Active Monitors available from the Summary tab in Monitor mode.

This topic describes:

- [Finding Specific Alarms on page 1277](#)
- [Sorting Alarms on page 1279](#)
- [Reading Events on page 1279](#)
- [Investigating Event Attributes on page 1280](#)
- [Changing the Alarm State on page 1280](#)

Finding Specific Alarms

Use the Alarm Detail monitor to locate a specific alarm, research the events causing the alarm, and to assign a disposition to the alarm. When an alarm is highlighted in the sorting

sequence, the events contributing to the alarm are listed in Event Details and the variable settings are shown in Event Attribute Detail.

To locate an alarm and to assign a disposition to the alarm:

1. Sort the list using the Display list. Sorting choices vary depending on how you arrived here. View [“Sorting Alarms” on page 1279](#) for details on sorting options.
2. Review the sorted list. Each entry shows a minimum of one to a maximum of nine fields. These fields are described in [Table 179 on page 1278](#).
3. Examine the events and event attributes that contributed to sending the alarm. Events and event attributes are discussed in [“Reading Events” on page 1279](#) and [“Investigating Event Attributes” on page 1280](#).

Table 179: Alarm Detail Fields

Field	Value	Shown in Detailed View by Default
Name	The alarm name.	Yes
ID	A system and sequentially-generated identification number.	No
Assigned To	If assigned to an individual, it shows the name of the person assigned; otherwise, it shows System to mark that the alarm is still unassigned.	Yes
Severity	The severity of the alarm. Severity levels are: <ul style="list-style-type: none"> • Critical—A critical condition exists; immediate action is necessary. • Major—A major error has occurred; escalate or notify as necessary. • Minor—A minor error has occurred; notify or monitor the condition. • Info—An informational message; no action is necessary. 	Yes
Acknowledged	Indicates if the alarm has been acknowledged.	Yes
Entity ID	The identification of the entity responsible for causing this alarm. The Entity ID is the key for correlation of events into an alarm. The Entity ID could be a MAC address of a radio or an IP address of the device.	Yes
Source	The IP address of the device or network element that generated the alarm. The SNMP agent is located at the source IP. In most cases, the source IP is the IP address of the switch or controller.	No
Reporting Device	The hostname of the reporting device.	Yes
Creation Date	The date and time the alarm was first reported.	No
Last Updated	The date and time that the information for the alarm was last modified.	Yes
Updated By	Either the system or the last user who modified the alarm.	No

Sorting Alarms

Depending on the monitor you chose to access Alarm Detail, your sorting options change to reflect the summary monitor. The different sort options are listed in [Table 180 on page 1279](#).

Table 180: Sort Options for Alarms

Alarms by Severity Sort	Alarms by Category Sort	Alarms by State and Current Active Alarms Sort
Minor	BGP	
Major	Chassis	
	Config	
	CoS	
	DHCP	
	GENERAL	
	GenericEvent	
	Ping	

You can also use Searching Alarms in the Tasks pane to perform searches using multiple arguments. With multiple arguments, you can isolate a single alarm from a long alarm list.

Reading Events

When you select an alarm in Alarm Detail, the Event Detail table updates with information about the events that are associated with the alarm. [Table 181 on page 1279](#) lists the fields in Event Detail.

Table 181: Event Detail Fields

Field	Value
Name	The event name; also known as the SNMP trap name.
ID	A system-generated, hexadecimal code that uniquely identifies the event.
Description	If the event is an SNMP event, it is shown as a system-generated event.
Type	The type of event, either fault or system alert.

Table 181: Event Detail Fields (continued)

Field	Value
Category	<p>The category of the event message. The category corresponds to the alarm categories shown in the Alarms by Category monitor and the Alarm Settings window. These categories are:</p> <ul style="list-style-type: none"> • General • Chassis
Source	The identification of the entity that is the cause of this event ; it is not necessarily the ID of the event that generated the event.
Originator	The identification of the entity that generated this event, for example, the switch IP or controller IP address.
Time Updated	The date and time of the last update to the event.

Investigating Event Attributes

The Event Attribute Detail window reflects the variables set during the event. In SNMP terminology, these attributes are known as variable bindings or varbinds. These attributes can provide key information about triggers. For example, if a fan fails, the attribute field could indicate the location of the fan in the chassis.

Changing the Alarm State

When an alarm is first reported, it is considered an active alarm. To change the alarm state, to assign the alarm to a person, or simply to record notes about the alarm, use the buttons on Alarm Details. These buttons are:

- Acknowledge—Use this button to acknowledge or record that the alarm is known and is being addressed.
- Clear—Use this button to clear or remove the alarm. The clear state says that the issue sending the alarm has been resolved and no long requires attention.
- Annotate—Use this button to record actions taken to resolve the alarm.
- Assign—Use this button to assign active or acknowledged alarms to staff.

Alarm Detail Monitor (Service View)

Use the Alarm Detail monitor to sort alarms, view an alarm in depth, and to assign a disposition to an alarm.

By clicking the Details icon, you can access the Alarm Detail monitor from any of the four alarm monitors available on the main page in Fault mode (Severity, Category, Current, or State). It is also available from the Current Active Monitors available from the Summary tab in Monitor mode.

This topic describes:

- [Finding Specific Alarms on page 1281](#)
- [Sorting Alarms on page 1282](#)
- [Reading Events on page 1282](#)
- [Investigating Event Attributes on page 1283](#)
- [Changing the Alarm State on page 1283](#)

Finding Specific Alarms

Use the Alarm Detail monitor to locate a specific alarm, research the events causing the alarm, and to assign a disposition to the alarm. When an alarm is highlighted in the sorting sequence, the events contributing to the alarm are listed in Event Details and the variable settings are shown in Event Attribute Detail.

To locate an alarm and to assign a disposition to the alarm:

1. Sort the list using the Display list. Sorting choices vary depending on how you arrived here. View [“Sorting Alarms” on page 1279](#) for details on sorting options.
2. Review the sorted list. Each entry shows a minimum of one to a maximum of nine fields. These fields are described in [Table 179 on page 1278](#).
3. Examine the events and event attributes that contributed to sending the alarm. Events and event attributes are discussed in [“Reading Events” on page 1279](#) and [“Investigating Event Attributes” on page 1280](#).

Table 182: Alarm Detail Fields

Field	Value	Shown in Detailed View by Default
Name	The alarm name.	Yes
ID	A system and sequentially-generated identification number.	No
Assigned To	If assigned to an individual, it shows the name of the person assigned; otherwise, it shows System to mark that the alarm is still unassigned.	Yes
Severity	The severity of the alarm. Severity levels are: <ul style="list-style-type: none"> • Critical—A critical condition exists; immediate action is necessary. • Major—A major error has occurred; escalate or notify as necessary. • Minor—A minor error has occurred; notify or monitor the condition. • Info—An informational message; no action is necessary. 	Yes
Service Name	The name of the service for which the alarm was generated.	Yes
Customer	The name of the customer associated with the service for which the alarm was generated.	Yes

Table 182: Alarm Detail Fields (continued)

Field	Value	Shown in Detailed View by Default
Service Type	The type or protocol of the service for which the alarm was generated.	Yes
Entity ID	The identification of the entity responsible for causing this alarm. The Entity ID is the key for correlation of events into an alarm. The Entity ID could be a MAC address of a radio or an IP address of the device.	Yes
Source	The IP address of the device or network element that generated the alarm. The SNMP agent is located at the source IP. In most cases, the source IP is the IP address of the switch or controller.	No
Acknowledged	Indicates if the alarm has been acknowledged.	Yes
Source	The IP address of the device or network element that generated the alarm. The SNMP agent is located at the source IP. In most cases, the source IP is the IP address of the switch or controller.	No
Creation Date	The date and time the alarm was first reported.	No
Last Updated	The date and time that the information for the alarm was last modified.	Yes
Updated By	Either the system or the last user who modified the alarm.	No

Sorting Alarms

Sort the alarms based on the following parameters from the drop-down lists:

- Severity
- State
- Service
- Time (You can choose only time spans ending now, for example, Last 12 hours.)

Click Search to filter the alarms and display the alarms based on the search criteria.

You can also use Searching Alarms in the Tasks pane to perform searches using multiple arguments. With multiple arguments, you can isolate a single alarm from a long alarm list.

Reading Events

When you select an alarm in Alarm Detail, the Event Detail table updates with information about the events that are associated with the alarm. [Table 181 on page 1279](#) lists the fields in Event Detail.

Table 183: Event Detail Fields

Field	Value
Name	The event name; also known as the SNMP trap name.
ID	A system-generated, hexadecimal code that uniquely identifies the event.
Description	If the event is an SNMP event, it is shown as a system-generated event.
Type	The type of event, either fault or system alert.
Category	The category of the event message. The category corresponds to the alarm categories shown in the Alarms by Category monitor and the Alarm Settings window.
Source	The identification of the entity that is the cause of this event ; it is not necessarily the ID of the event that generated the event.
Originator	The identification of the entity that generated this event, for example, the switch IP or controller IP address.
Time Updated	The date and time of the last update to the event.

Investigating Event Attributes

The Event Attribute Detail window reflects the variables set during the event. In SNMP terminology, these attributes are known as variable bindings or varbinds. These attributes can provide key information about triggers. For example, if a fan fails, the attribute field could indicate the location of the fan in the chassis.

Changing the Alarm State

When an alarm is first reported, it is considered an active alarm. To change the alarm state, to assign the alarm to a person, or simply to record notes about the alarm, use the buttons on Alarm Details. These buttons are:

- **Acknowledge**—Use this button to acknowledge or record that the alarm is known and is being addressed.
- **Clear**—Use this button to clear or remove the alarm. The clear state says that the issue sending the alarm has been resolved and no longer requires attention.
- **Annotate**—Use this button to record actions taken to resolve the alarm.
- **Assign**—Use this button to assign active or acknowledged alarms to staff.

Related Documentation

- [Alarm Trend Monitor \(Service View\) on page 1287](#)
- [Alarms by Category Monitor on page 1285](#)
- [Alarms by Severity Monitor \(Service View\) on page 1285](#)
- [Alarms by State Monitor on page 1286](#)

- [Current Active Alarms Monitor \(Service View\) on page 1284](#)

Current Active Alarms Monitor (Service View)

The Current Active Alarms monitor shows any active alarm that has not yet been cleared. It is one of the four standard monitors available in Alarm mode. Current Active Alarms is a table that has four fields and appear by default. However, nine fields are available for selection. View [Table 162 on page 1179](#) for a description of the table.

Table 184: Current Active Alarms Monitor

Table Column	Description	Shown in Summary by Default	Shown in Detailed View by Default
Name	The alarm name.	Yes	Yes
ID	A system and sequentially-generated identification number.	No	No
Assigned To	If assigned to an individual, it shows the name of the person assigned; otherwise, it shows System to mark that the alarm is still unassigned.	No	Yes
Severity	The severity of the alarm. Severity levels are: <ul style="list-style-type: none"> • Critical—A critical condition exists; immediate action is necessary. • Major—A major error has occurred; escalate or notify as necessary. • Minor—A minor error has occurred; notify or monitor the condition. • Info—An informational message; no action is necessary. 	Yes	Yes
Service Name	The name of the service for which the alarm was generated.	Yes	Yes
Customer	The name of the customer associated with the service for which the alarm was generated.	Yes	Yes
Service Type	The type or protocol of the service for which the alarm was generated.	Yes	Yes
Entity ID	The identification of the entity responsible for causing this alarm. The Entity ID is the key for correlation of events into an alarm. The Entity ID could be a MAC address of a radio or an IP address of the device.	Yes	Yes
Source	The IP address of the device or network element that generated the alarm. The SNMP agent is located at the source IP. In most cases, the source IP is the IP address of the switch or controller.	No	No
Creation Date	The date and time the alarm was first reported.	No	No

Table 184: Current Active Alarms Monitor (continued)

Table Column	Description	Shown in Summary by Default	Shown in Detailed View by Default
Last Updated	The date and time that the information for the alarm was last modified.	Yes	Yes
Updated By	Either the system or the last user who modified the alarm.	No	No

Clicking the Details icon opens Alarm Details where you can sort and disposition alarms by state (Acknowledged, Clear, Active).

Related Documentation

- [Alarm Detail Monitor \(Service View\) on page 1280](#)
- [Alarm Trend Monitor \(Service View\) on page 1287](#)
- [Alarms by Category Monitor on page 1285](#)
- [Alarms by Severity Monitor \(Service View\) on page 1285](#)
- [Alarms by State Monitor on page 1286](#)

Alarms by Category Monitor

Alarms by Category is a table of all active alarms sorted by category. Use this monitor to view where errors are trending. These categories are the same categories shown in the Alarm Settings page.

This monitor is available in all views in the main window when in Fault mode.

The table shows the active categories and the number of alarms per category. Clicking the Details icon on Alarms by Category opens Alarm Details where you can sort these categories and change the state of the alarms.

To create a similar report for a specific period of time, use the Alarm Summary report in Report mode.

Related Documentation

- [Alarm Detail Monitor \(Service View\) on page 1280](#)
- [Alarm Trend Monitor \(Service View\) on page 1287](#)
- [Alarms by Severity Monitor \(Service View\) on page 1285](#)
- [Alarms by State Monitor on page 1286](#)
- [Current Active Alarms Monitor \(Service View\) on page 1284](#)

Alarms by Severity Monitor (Service View)

Alarms by Severity is a pie-chart that shows the breakdown of all alarms since the last system restart. It is available on the main page when in Fault mode.

If you mouse over each segment, the total number of alerts for those alarms is shown. Alarm severity levels are:

- Critical (Red)—A critical condition exists; immediate action is necessary.
- Major (Orange)—A major error has occurred; escalate or notify as necessary.
- Minor (Yellow)—A minor error has occurred; notify or monitor the condition.
- Info (Wedgewood Blue)—An informational message; no action is necessary. Informational alarms do not necessarily indicate an error. It could indicate that a device or entity has changed state.

Clicking the Details icon on Alarms by Severity opens Alarm Details where you can sort and disposition individual.

Related Documentation

- [Alarm Detail Monitor \(Service View\) on page 1280](#)
- [Alarm Trend Monitor \(Service View\) on page 1287](#)
- [Alarms by Category Monitor on page 1285](#)
- [Alarms by State Monitor on page 1286](#)
- [Current Active Alarms Monitor \(Service View\) on page 1284](#)

Alarms by State Monitor

The Alarms by State monitor is a pie-chart representation of the states of an alarm: active and cleared. Use this graph to get an overall perspective of the amount of alarms that are active compare to those that are cleared. The Alarms by State monitor is on the main pane when in Fault mode.

Mouse over each segment of the pie-chart shows the number of alarms in these states:

- Active—Alarms that are current and not yet cleared.
- Cleared—Alarms that are resolved and the device or entity has returned to normal operation.

You can create an Alarms by State report for a specified node or a period of time using the Alarms Summary Report in Repot mode.

Changing the state of an alarm using Connectivity Services Director is performed on the Alarm Detail page. Clicking the Details icon on Alarms by State opens Alarm Details where you can sort and set the disposition of the alarms.

Related Documentation

- [Alarm Detail Monitor \(Service View\) on page 1280](#)
- [Alarm Trend Monitor \(Service View\) on page 1287](#)
- [Alarms by Category Monitor on page 1285](#)
- [Alarms by Severity Monitor \(Service View\) on page 1285](#)

- [Current Active Alarms Monitor \(Service View\) on page 1284](#)

Alarm Trend Monitor (Service View)

The Alarm Trend monitor provides trend information about alarms. The trend information is shown on a line chart, where each alarm severity is shown as a colored line. The legend for the line colors is displayed below the chart. The alarm count is shown on the vertical axis. The time of the data samples is shown on the horizontal axis. This monitor includes tabs that show alarm trend information for active alarms and for new alarms. You can select the time period to display from the list in the title bar.

Related Documentation

- [Alarm Detail Monitor \(Service View\) on page 1280](#)
- [Alarms by Category Monitor on page 1285](#)
- [Alarms by Severity Monitor \(Service View\) on page 1285](#)
- [Alarms by State Monitor on page 1286](#)
- [Current Active Alarms Monitor \(Service View\) on page 1284](#)

Alarms by Severity Monitor (All Views Except Service View)

Alarms by Severity is a pie-chart that shows the breakdown of all alarms since the last system restart. It is available on the main page when in Fault mode.

If you mouse over each segment, the total number of alerts for those alarms is shown. Alarm severity levels are:

- Critical (Red)—A critical condition exists; immediate action is necessary.
- Major (Orange)—A major error has occurred; escalate or notify as necessary.
- Minor (Yellow)—A minor error has occurred; notify or monitor the condition.
- Info (Wedgewood Blue)—An informational message; no action is necessary. Informational alarms do not necessarily indicate an error. It could indicate that a device or entity has changed state.

Clicking the Details icon on Alarms by Severity opens Alarm Details where you can sort and disposition individual.

Related Documentation

- [Alarm Detail Monitor \(Service View\) on page 1280](#)
- [Alarm Trend Monitor \(Service View\) on page 1287](#)
- [Alarms by Category Monitor on page 1285](#)
- [Alarms by State Monitor on page 1286](#)
- [Current Active Alarms Monitor \(Service View\) on page 1284](#)

Alarms by State Monitor (All Views Except Service View)

The Alarms by State monitor is a pie-chart representation of the states of an alarm: active and cleared. Use this graph to get an overall perspective of the amount of alarms that are active compare to those that are cleared. The Alarms by State monitor is on the main pane when in Fault mode.

Mouse over each segment of the pie-chart shows the number of alarms in these states:

- Active—Alarms that are current and not yet cleared.
- Cleared—Alarms that are resolved and the device or entity has returned to normal operation.

You can create an Alarms by State report for a specified node or a period of time using the Alarms Summary Report in Repot mode.

Changing the state of an alarm using Connectivity Services Director is performed on the Alarm Detail page. Clicking the Details icon on Alarms by State opens Alarm Details where you can sort and set the disposition of the alarms.

Related Documentation

- [Alarm Detail Monitor \(Service View\) on page 1280](#)
- [Alarm Trend Monitor \(Service View\) on page 1287](#)
- [Alarms by Category Monitor on page 1285](#)
- [Alarms by Severity Monitor \(Service View\) on page 1285](#)
- [Current Active Alarms Monitor \(Service View\) on page 1284](#)

Current Active Alarms Monitor (All Views Except Service View)

The Current Active Alarms monitor shows any active alarm that has not yet been cleared. It is one of the four standard monitors available in Alarm mode. Current Active Alarms is a table that has four fields and appear by default. However, nine fields are available for selection. View [Table 162 on page 1179](#) for a description of the table.

Table 185: Current Active Alarms Monitor

Table Column	Description	Shown in Summary by Default	Shown in Detailed View by Default
Name	The alarm name.	Yes	Yes
ID	A system and sequentially-generated identification number.	No	No
Assigned To	If assigned to an individual, it shows the name of the person assigned; otherwise, it shows System to mark that the alarm is still unassigned.	No	Yes

Table 185: Current Active Alarms Monitor (continued)

Table Column	Description	Shown in Summary by Default	Shown in Detailed View by Default
Severity	<p>The severity of the alarm. Severity levels are:</p> <ul style="list-style-type: none"> Critical—A critical condition exists; immediate action is necessary. Major—A major error has occurred; escalate or notify as necessary. Minor—A minor error has occurred; notify or monitor the condition. Info—An informational message; no action is necessary. 	Yes	Yes
Entity ID	The identification of the entity responsible for causing this alarm. The Entity ID is the key for correlation of events into an alarm. The Entity ID could be a MAC address of a radio or an IP address of the device.	Yes	Yes
Source	The IP address of the device or network element that generated the alarm. The SNMP agent is located at the source IP. In most cases, the source IP is the IP address of the switch or controller.	No	No
Reporting Device	The hostname or IP address of the reporting device.	Yes	Yes
Creation Date	The date and time the alarm was first reported.	No	No
Last Updated	The date and time that the information for the alarm was last modified.	Yes	Yes
Updated By	Either the system or the last user who modified the alarm.	No	No

Clicking the Details icon opens Alarm Details where you can sort and disposition alarms by state (Acknowledged, Clear, Active).

Alarm Trend Monitor (All Views Except Service View)

The Alarm Trend monitor provides trend information about alarms. The trend information is shown on a line chart, where each alarm severity is shown as a colored line. The legend for the line colors is displayed below the chart. The alarm count is shown on the vertical axis. The time of the data samples is shown on the horizontal axis. This monitor includes tabs that show alarm trend information for active alarms and for new alarms. You can select the time period to display from the list in the title bar.

Related Documentation

- [Alarm Detail Monitor \(Service View\) on page 1280](#)
- [Alarms by Category Monitor on page 1285](#)
- [Alarms by Severity Monitor \(Service View\) on page 1285](#)
- [Alarms by State Monitor on page 1286](#)

- [Current Active Alarms Monitor \(Service View\) on page 1284](#)

PART 15

End-to-End Configuration Examples

- [Configuration Scenarios on page 1293](#)

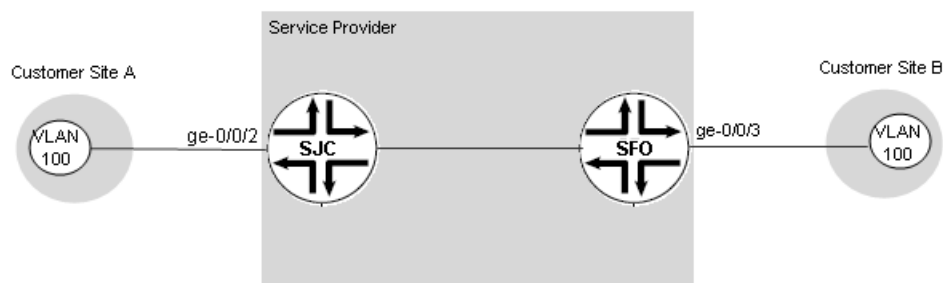
Configuration Scenarios

- [Example: Configuring and Deploying a Point-to-Point Ethernet Service on page 1293](#)
- [Example: Configuring and Deploying a Multipoint-to-Multipoint VPLS Service on page 1305](#)
- [Example: Configuring and Deploying a Layer 3 VPN Full-Mesh Service on page 1319](#)

Example: Configuring and Deploying a Point-to-Point Ethernet Service

This example deploys and verifies a point-to-point Ethernet service starting with two MX Series devices. [Figure 61 on page 1293](#) shows the service.

Figure 61: Simple Point-to-Point Service



This service provides connectivity for one VLAN, using 802.1Q interface endpoints. Customer site A connects to the network through UNI ge-0/0/2 on an N-PE device named SJC. Customer site B connects to the network through UNI ge-0/0/3 on an N-PE device named SFO.

The bandwidth for each UNI is limited to 1000 Mbps.

You can create this service by performing the following tasks, in order:

- [Preparing Devices for Discovery on page 1294](#)
- [Discovering Devices on page 1294](#)
- [Preparing Devices for Prestaging on page 1296](#)
- [Discovering and Assigning N-PE Roles on page 1297](#)
- [Choosing or Creating a Service Definition on page 1298](#)
- [Creating a Customer on page 1300](#)

- [Creating and Deploying a Point-to-Point Service Order on page 1301](#)
- [Performing a Functional Audit and a Configuration Audit on page 1303](#)

Preparing Devices for Discovery

Before you can add a device using device discovery, the following conditions must be met:

- SSH v2 is enabled on the device. To enable SSH v2 on a device, issue the following CLI command:

```
set system services ssh protocol-version v2
```

- The NETCONF protocol over SSH is enabled on the device. To enable the NETCONF protocol over SSH on a device, issue the following CLI command:

```
set system services netconf ssh
```

- The device is configured with a static management IP address that is reachable from the Junos Space server. The IP address can be in-band or out-of-band.
- A user with full administrative privileges is created on the device for the Junos Space administrator.
- If you plan to use SNMP to probe devices as part of device discovery, ensure that SNMP is enabled on the device with appropriate read-only V1/V2C/V3 credentials.

Discovering Devices

Device discovery is a process that Junos Space uses to bring network devices under its control. This example brings two MX Series routers under Junos Space management:

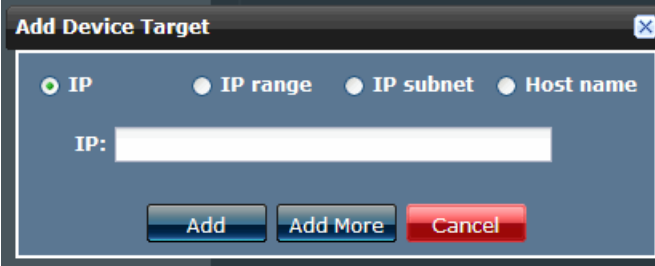


.....

NOTE: Alternatively, you can import devices using the Connectivity Services Director GUI. See [“Discovering Devices in a Physical Network” on page 177](#) for instructions on discovering devices from Build mode of Connectivity Services Director.

.....

1. Log in to Junos Space using your credentials.
2. From the Junos Space Network Management Platform user interface, select **Devices** > **Discover Devices** > **Discover Targets**.
3. In the **Discover Targets** window, click **+**.
The **Add Device Target** window appears.

A screenshot of a web-based dialog box titled "Add Device Target". At the top, there are four radio buttons: "IP" (which is selected), "IP range", "IP subnet", and "Host name". Below these buttons is a text input field labeled "IP:". At the bottom of the dialog, there are three buttons: "Add" (blue), "Add More" (blue), and "Cancel" (red). The dialog has a standard window border with a close button in the top right corner.

4. Select **IP range**.
5. Enter the IP address information. This example uses a range of two addresses.
6. Click **Add**, and then click **Next**.
7. In the **Devices: Specify Probes** window, select both **Ping** and **SNMP** as probes.
8. Click **Next**.
9. In the **Devices: Specify Credentials** window, click **+** and enter the device login credentials.
10. Click **Finish**.

Device discovery begins. It displays a graph showing the status of the discovery operation. Initially, two devices are discovered. When Junos Space has accessed both devices and brought them under its management, both devices move from the Discovered column of the graph to the Managed column.
11. To check the results of the device discovery operation, select the **Devices** workspace again, then select **Device Management**. The **Manage Devices** page shows the added devices.

Devices > Manage Devices

0 Items Selected

Actions

Name	Physic...	Logical...	OS Ver...	Platform	Vendor	Schem...	IP Add...	Connec...	Manag...	Authen...
access-bt750	View	View	3.0.0	B-7510	Juniper Networ...	3.0.0	10.216...	up	In Sync	Crede... Based
access-hcl-bgm	View	View	3.0.0	C-2030	Juniper Networ...	3.0.0	10.216...	up	In Sync	Crede... Based
access1-bt750	View	View	3.0.0	B-7510	Juniper Networ...	3.0.0	10.216...	up	In Sync	Crede... Based
embassy	View	View	12.1R2.9	MX80	Juniper Networ...	11.4R2....	10.216...	up	In Sync	Crede... Based
exora	View	View	10.0-201103...	M71	Juniper Networ...	11.4R2....	10.216...	up	In Sync	Crede... Based
jaipur	View	View	12.2R1.8	M10I	Juniper Networ...	11.4R2....	10.216...	up	In Sync	Crede... Based
junos-m10-1-space	View	View	12.2R1.8	M10I	Juniper Networ...	11.4R2....	10.216...	up	In Sync	Crede... Based
junos-m10-2-space	View	View	12.2R1.8	M10I	Juniper Networ...	11.4R2....	10.216...	up	In Sync	Crede... Based
junos-mx240-space	View	View	12.2R1.8	MX240	Juniper Networ...	11.4R2....	10.216...	up	In Sync	Crede... Based
junos-mx480-space	View	View	12.2R1.8	MX480	Juniper Networ...	11.4R2....	10.216...	up	In Sync	Crede... Based

Page 1 of 1

Displaying 1 - 19 of 19 | Show 30 items

- See Also**
- *Device Discovery Overview* in the *Junos Space Network Application Platform User Guide*
 - *Discovering Devices* in the *Junos Space Network Application Platform User Guide*

Preparing Devices for Prestaging

Before prestaging devices for point-to-point services, the following entities must be configured:

- MPLS must run on each N-PE device.
- LDP signaling must be established between N-PE devices that you want to participate in the same point-to-point service.

To satisfy these configurations, ensure that the following configuration exists on each N-PE device:

```

interfaces {
  ge-0/0/0 {
    unit 0 {
      family inet {
        address 10.1.18.2/30;
      }
      family mpls;
    }
  }
}
lo0 {
  unit 0 {
    family inet {

```



```

        address 192.168.1.20/32;
    }
}
}
protocols {
    mpls {
        interface ge-0/0/0.0;
        interface lo0.0;
    }
    ospf {
        traffic-engineering;
        area 0.0.0.0 {
            interface lo0.0 {
                passive;
            }
            interface ge-0/0/0.0;
        }
    }
    ldp {
        interface ge-0/0/0.0;
        interface lo0.0;
    }
}

```



NOTE: The OSPF configuration is not required in prestaging.

Discovering and Assigning N-PE Roles

Before you can provision services, you must prestage the devices. Prestaging includes assigning device roles and designating interfaces on those devices as UNIs. This example provides the steps to accept the recommendations of the Network Services application for N-PE devices and UNIs.

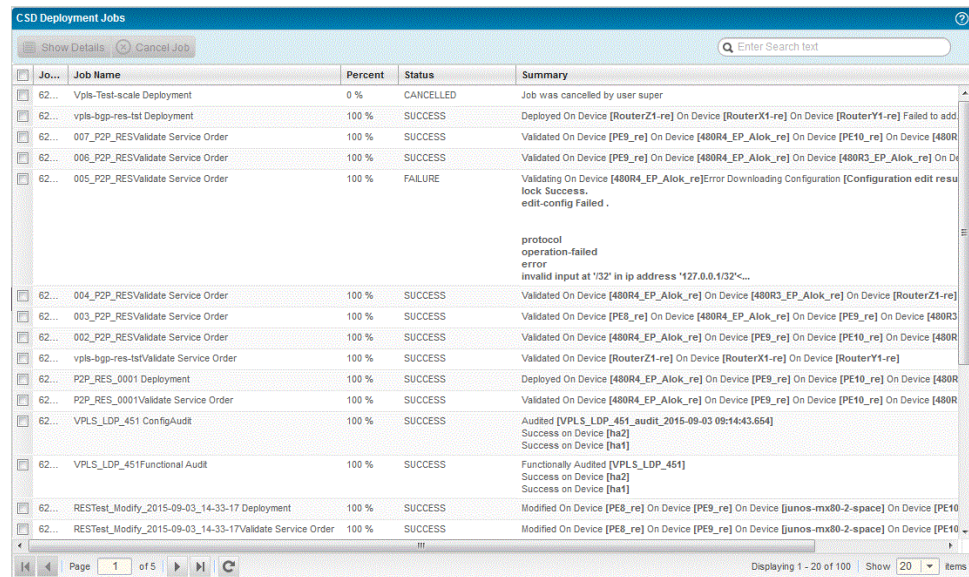
1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. In the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.

View the values displayed under the Roles column of the discovered devices.

This action launches the role discovery process in which the Network Services application examines the devices under Junos Space management looking for devices that match predefined rules that identify N-PE devices. In this example, the Role Discovery Status graph shows that the Network Services application has discovered two such devices.

- Click **Manage Device Roles** and from the drop-down list, select **Discover Roles** to retrieve the roles of the devices. A dialog box is displayed with the job ID of the discovery job that is created to obtain the latest roles of the devices.
- To view the assignment status, in the **CSD Deployment Jobs** window that you can access from Deploy mode of Service View by selecting **View Deployment Jobs** from the task pane, click the job ID of the assignment job.

The **Job Management** page shows the progress and status of the role assignment job.



Job ID	Job Name	Percent	Status	Summary
62...	Vpls-Test-scale Deployment	0 %	CANCELLED	Job was cancelled by user super
62...	vpls-bgp-res-tst Deployment	100 %	SUCCESS	Deployed On Device [RouterZ1-re] On Device [RouterX1-re] On Device [RouterY1-re] Failed to add...
62...	007_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE9_re] On Device [480R4_EP_Alok_re] On Device [PE10_re] On Device [480R...
62...	006_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE9_re] On Device [480R4_EP_Alok_re] On Device [480R3_EP_Alok_re] On Dk...
62...	005_P2P_RESValidate Service Order	100 %	FAILURE	Validating On Device [480R4_EP_Alok_re]Error Downloading Configuration [Configuration edit resu edit-config Failed . protocol operation-failed error invalid input at '32' in ip address '127.0.0.1/32'<...
62...	004_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [480R3_EP_Alok_re] On Device [RouterZ1-re]
62...	003_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE8_re] On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [480R3...
62...	002_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R...
62...	vpls-bgp-res-tstValidate Service Order	100 %	SUCCESS	Validated On Device [RouterZ1-re] On Device [RouterX1-re] On Device [RouterY1-re]
62...	P2P_RES_0001 Deployment	100 %	SUCCESS	Deployed On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R...
62...	P2P_RES_0001Validate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R...
62...	VPLS_LDP_451 ConfigAudit	100 %	SUCCESS	Audited [VPLS_LDP_451_audit_2015-09-03 09:14:43.654] Success on Device [ha2] Success on Device [ha1]
62...	VPLS_LDP_451Functional Audit	100 %	SUCCESS	Functionally Audited [VPLS_LDP_451] Success on Device [ha2] Success on Device [ha1]
62...	REStest_Modify_2015-09-03_14-33-17 Deployment	100 %	SUCCESS	Modified On Device [PE8_re] On Device [PE9_re] On Device [junos-mx80-2-space] On Device [PE10...
62...	REStest_Modify_2015-09-03_14-33-17Validate Service Order	100 %	SUCCESS	Modified On Device [PE8_re] On Device [PE9_re] On Device [junos-mx80-2-space] On Device [PE10...

- To verify the result, in Build mode, select **Prestage Devices > Manage Device Roles** from the tasks pane.

The **Manage Device Roles** window shows two devices that can be used for provisioning.

- To unassign a device from N-PE role assignment, click **Manage Device Roles** and from the drop-down list, select **Unassign Role** to remove the role capability of a network element. You are prompted to confirm the operation. If you click **OK**, a request is submitted to remove the latest role of the network element or device.

- See Also**
- [Discovering and Assigning All N-PE Devices on page 351](#)
 - [Discovering and Assigning N-PE Devices with Exceptions on page 353](#)

Choosing or Creating a Service Definition

A service definition provides a template upon which services are built. It specifies service attributes that are not specific to a service instance. In our example, the service definition provides all service attributes except the N-PE devices, the UNIs, and bandwidth.

The Network Services application ships with standard service definitions. First, we check the standard service definitions to determine whether one already exists that will work.

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. In the **Network Services > Connectivity** task pane, select **Service Design > Manage Service Definitions**.

The **Manage Service Definitions** page lists all service definitions in the system. In a new system, the screen lists only predefined service definitions.

This example requires a service definition with UNIs that use 802.1Q interfaces and allow you to set a bandwidth of 25 Mbps. The standard service definitions have several examples for provisioning 802.1Q UNIs, but none that allow the setting of a 25 Mbps bandwidth limit. You need to create a new service definition.

4. In the **Network Services > Connectivity** task pane, select **Service Design > Manage Service Definitions > New > P2P Service Definition**.

The General window appears.

5. Enter a name for the service definition. For this example, enter **p2p-dot1q-sd-1**.
6. Click **Next**.

The **UNI Settings** window appears.

7. In the **Connectivity Settings** window, to pick the default connectivity settings, click **Next**.

8. In the **UNI Settings** window, in the **Ethernet option** field, select **dot1q**.

9. In the **Customer traffic type** field, select **Transport single VLAN**.

10. In the **VLAN ID selection** field, select **Select manually**.

11. In the **VLAN range for manual input** field, specify the range.

12. In the **Outer Tag protocol ID** field, select **0x88a8**.

13. In the **Physical IF encapsulation** field, select **flexible-ethernet-services**.

14. In the **Logical IF encapsulation** field, select **vlan-ccc**.
15. In the **Bandwidth Settings** panel, select the **Enable rate limiting** check box.
16. In the **Default Bandwidth** field, enter **10**, for a default bandwidth of 10 Mbps.
17. To the right of the value you just entered, select the **Editable in service order** check box.

The **Min Bandwidth (Kbps)**, **Max Bandwidth (Mbps)**, and **Increment (Kbps)** become active.
18. In the **Min Bandwidth (Kbps)** field, enter **100**.
19. In the **Max Bandwidth (Mbps)** field, enter **10000**.
20. In the **increment** field, enter **64**.

These settings of the **Bandwidth range** and **Increment** fields allow the bandwidth to be set in the service to any 64-Kbps increment in the range of 100 Kbps through 10000 Mbps.
21. To save and complete the service definition, click **Finish**.

The **Manage Service Definitions** page includes the new service definition.

You have created a customized Service Definition, but it has not yet been published. Before a service definition can be used in provisioning, it must be published.
22. To publish the service definition, in the **Manage Service Definitions** page, select the **p2p-dot1q-sd-1** service definition; click the **Publish Service Definition** button.

The **Publish Service Definition** window appears.
23. To confirm that you want to publish this service definition, click **Publish**.

In the **Manage Service Definitions** page, the symbol in the upper left corner of the service definition changes to a check mark, indicating that the status has changed to Published.

The service definition is now ready for use in provisioning.

Creating a Customer

Before you can provision the service, customer details must be present in the Junos Space database. To add a customer:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. In the **Network Services > Connectivity** task pane, select **Service Provisioning > Manage Customers > Create Customer**.
4. In the **Name** field, enter **Best Customer**.
5. In the **Account number** field, enter **1234**.
6. Click **Create**.

The **Manage Customers** page shows the new customer.

See Also • [Adding a New Customer on page 737](#)

Creating and Deploying a Point-to-Point Service Order

Now that you have prestaged your devices, created a suitable service definition, and added the customer information to the database, you are ready to create and deploy a service order. To create and deploy a service order:

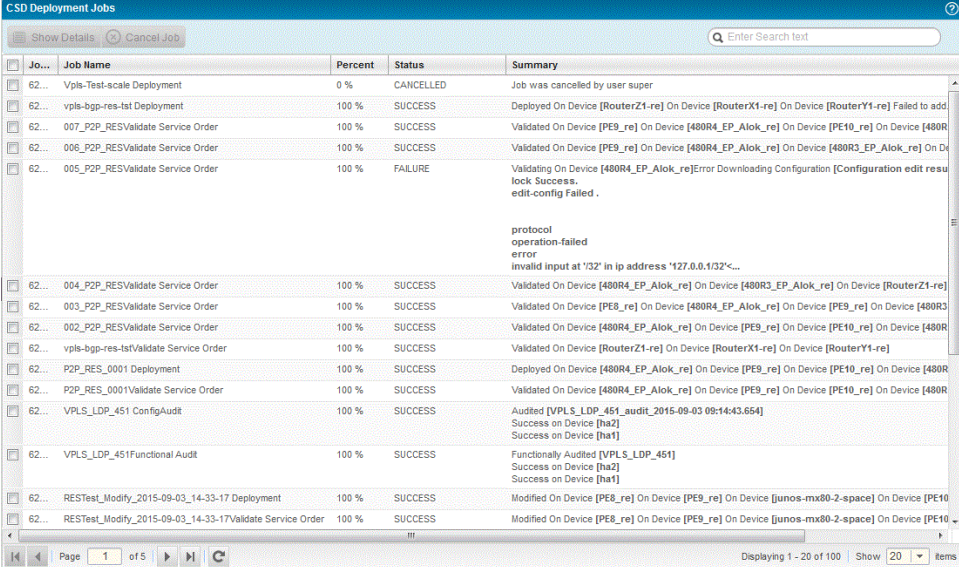
1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. Click the **New** icon at the top of the upper half of the page that displays previously created service orders. The Select Service Type dialog box appears.
4. Select **Point-to-Point** to create a point-to-point service order.

The General/Connectivity Settings panel appears initially in the right panel, as shown in the example.
5. In the **Create P2P Service Order** window, select the service named **p2p-dot1q-sd-1**.

This is the customized service definition you created earlier.
6. Click **Next**.

7. In the **General/Connectivity Settings** window, in the **Name** field, enter **so_1**.
8. In the **Customer** field, select **Best Customer**.
9. Click **Next**.
The **Endpoint Settings** window appears.
10. For endpoint A, in the **PE device** field, select **SJC**.
11. In the **UNI interface** field, select **ge-0/0/2**.
12. In the **VLAN-ID** field, enter **100**.
13. Click **Next**.
14. In the **Endpoint Settings** window for endpoint Z, in the **PE device** field, select **SFO**.
15. In the **UNI interface** field, select **ge-0/0/3**.
16. In the **Bandwidth** field, select **25**.
17. Click **Done**. You are returned to the Manage Network Services page.
18. From the Manage Service Orders page that is displayed in the lower part of the window, select the particular service and click **Deploy now**.
19. Click **OK** to start the deployment.

20. To monitor the progress and status of the deployment, in the Manage Service Orders window, click the link in the Latest Job field. The **Job Management** page shows the status of the job.



Job...	Job Name	Percent	Status	Summary
62...	Vpls-Test-scale Deployment	0 %	CANCELLED	Job was cancelled by user super
62...	vpls-bgp-res-1st Deployment	100 %	SUCCESS	Deployed On Device [RouterZ1-re] On Device [RouterX1-re] On Device [RouterY1-re] Failed to add...
62...	007_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE9_re] On Device [480R4_EP_Alok_re] On Device [PE10_re] On Device [480R3...
62...	006_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE9_re] On Device [480R4_EP_Alok_re] On Device [480R3_EP_Alok_re] On D...
62...	005_P2P_RESValidate Service Order	100 %	FAILURE	Validating On Device [480R4_EP_Alok_re]Error Downloading Configuration [Configuration edit resu lock Success. edit-config Failed . protocol operation-failed error invalid input at '32' in ip address '127.0.0.1/32'<...
62...	004_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [480R3_EP_Alok_re] On Device [RouterZ1-re]
62...	003_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE8_re] On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [480R3...
62...	002_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R...
62...	vpls-bgp-res-1stValidate Service Order	100 %	SUCCESS	Validated On Device [RouterZ1-re] On Device [RouterX1-re] On Device [RouterY1-re]
62...	P2P_RES_0001 Deployment	100 %	SUCCESS	Deployed On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R...
62...	P2P_RES_0001Validate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R...
62...	VPLS_LDP_451 ConfigAudit	100 %	SUCCESS	Audited [VPLS_LDP_451_audit_2015-09-03 09:14:43.654] Success on Device [ha2] Success on Device [ha1]
62...	VPLS_LDP_451Functional Audit	100 %	SUCCESS	Functionally Audited [VPLS_LDP_451] Success on Device [ha2] Success on Device [ha1]
62...	RESTTest_Modify_2015-09-03_14-33-17 Deployment	100 %	SUCCESS	Modified On Device [PE8_re] On Device [PE9_re] On Device [junos-mx80-2-space] On Device [PE10...
62...	RESTTest_Modify_2015-09-03_14-33-17Validate Service Order	100 %	SUCCESS	Modified On Device [PE8_re] On Device [PE9_re] On Device [junos-mx80-2-space] On Device [PE10...



NOTE: Alternatively, to display the Job Management page, from the Junos Space Platform UI, select **Jobs > Manage Jobs** from the Tasks pane. You can also view the CSD Deployment Jobs page in Deploy mode of Service View by selecting the **View Deployment Jobs** option in the task pane.

21. When you see in the **Job Management** window that the deployment is successful, in the **Network Services** task pane in Deploy mode, select **Service Provisioning > Deploy Services**.

The **Manage Network Services** page shows the new service.

Performing a Functional Audit and a Configuration Audit

Now that your new service is deployed, you should validate its configuration and functional integrity. A functional audit runs operational commands on the device to verify that the service is up or down. A configuration audit verifies whether the configuration that was pushed to the device during deployment is actually on the device.

To perform a configuration audit and a functional audit of the service:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.

3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services > P2P Services to expand the tree and display the different service types that you can configure.
4. Select **Deploy Services** from the task pane. The right pane displays two pages. The Manage Network Services page is displayed in the upper half of the right pane. Selecting a service from this page causes the associated service orders for the selected service to be displayed in the Manage Service Orders page in the lower half of the right pane.
5. In the **Manage Network Services** page, select the service instance you just deployed.
6. Select the service instance, and open the **Actions** menu and select **Run Functional Audit**.
7. In the **Schedule Functional Audit** window, you can choose to perform the audit now or schedule it for later. Select **Audit now**, then click **OK**.
8. In the **Order Information** screen, click **OK**.
9. Select the service instance, and open the **Audit** menu and select **Run Configuration Audit**.
10. In the **Schedule Configuration Audit** window, you can choose to perform the audit now or schedule it for later. Select **Audit now**, and then click **OK**.
11. In the **Order Information** window, click **OK**.

When the audit jobs have finished, success is indicated by an up arrow in the top right corner of the service.
12. To view the functional audit results:
 - a. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
 - b. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
 - c. From the **Network Services > Connectivity > P2P Services** View pane, select the **so_1** service instance.

- d. In the tasks pane, select **Audit/Results > Functional Audit**.
 - e. In the **Functional Audit Results** window, select each device to view the results.
13. To view the results of the configuration audit:
- a. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
 - b. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
 - c. From the **Network Services > Connectivity > P2P Services** View pane, select the **so_1** service instance.
 - d. In the tasks pane, select **Audit/Results > Configuration Audit**.
 - e. In the **Configuration Audit Results** window, select each device in turn and review the results. This report indicates any part of the service configuration that is missing on the device, or is inconsistent with the Junos Space database.

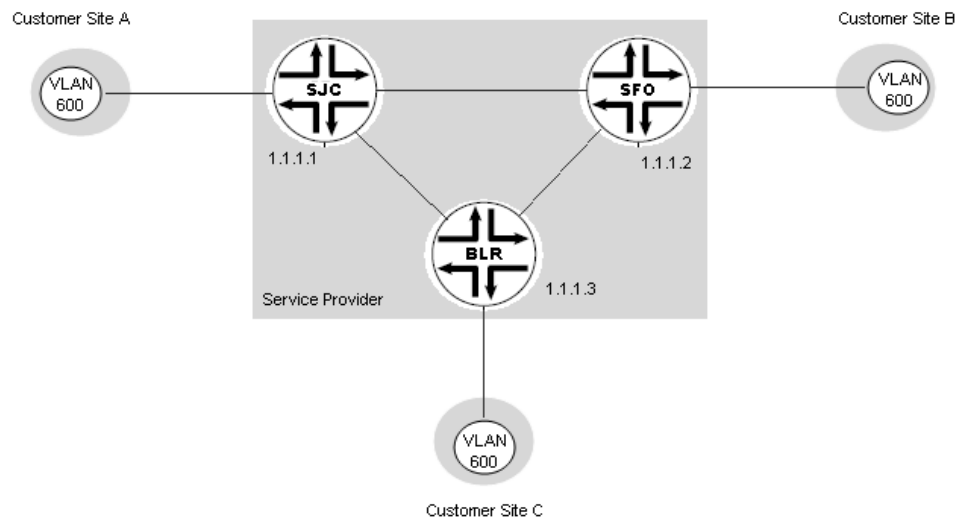
Following successful audit, the service is deployed and ready to be used.

**Related
Documentation**

- *Device Discovery Overview* in the *Junos Space Network Application Platform User Guide*
- *Discovering Devices* in the *Junos Space Network Application Platform User Guide*

Example: Configuring and Deploying a Multipoint-to-Multipoint VPLS Service

This example shows how to deploy and verify a multipoint-to-multipoint VPLS service starting with three MX Series routers. [Figure 62 on page 1306](#) shows the service.

Figure 62: Simple Multipoint-to-Multipoint Service

This service provides connectivity for one VLAN, using 802.1Q interface endpoints. Customer site A connects to the network through an N-PE device named SJC (IP address 1.1.1.1). Customer site B connects to the network through an N-PE device named SFO (IP address 1.1.1.2). Customer site C connects to the network through an N-PE device named BLR (IP address 1.1.1.3). In this example, we allow Network Activate to select each UNI automatically.

Each UNI is to have its bandwidth limited to 25 Mbps.

You can create this service by performing the following tasks:

- [Preparing Devices for Discovery on page 1306](#)
- [Discovering Devices on page 1307](#)
- [Preparing Devices for Prestaging on page 1308](#)
- [Discovering and Assigning N-PE Roles on page 1311](#)
- [Choosing or Creating a Service Definition on page 1312](#)
- [Creating a Customer on page 1315](#)
- [Creating and Deploying a Multipoint-to-Multipoint Service Order on page 1316](#)
- [Performing a Functional Audit and a Configuration Audit on page 1318](#)

Preparing Devices for Discovery

Before you can add a device using device discovery, the following conditions must be met:

- SSH v2 is enabled on the device. To enable SSH v2 on a device, issue the following CLI command:

```
set system services ssh protocol-version v2
```

- The NETCONF protocol over SSH is enabled on the device. To enable the NETCONF protocol over SSH on a device, issue the following CLI command:

```
set system services netconf ssh
```

- The device is configured with a static management IP address that is reachable from the Junos Space server. The IP address can be in-band or out-of-band.
- A user with full administrative privileges is created on the device for the Junos Space administrator.
- If you plan to use SNMP to probe devices as part of device discovery, ensure that SNMP is enabled on the device with appropriate read-only V1/V2C/V3 credentials.

Discovering Devices

Device discovery is a process that Junos Space uses to bring network devices under its control. This example brings two MX Series routers under Junos Space management.



NOTE: Alternatively, you can import devices using the Connectivity Services Director GUI. See [“Discovering Devices in a Physical Network” on page 177](#) for instructions on discovering devices from Build mode of Connectivity Services Director.

1. Log in to Junos Space using your credentials.
2. In the Applications Chooser of the Junos Space Platform user interface, select **Platform > Devices > Device Discovery > Device Discovery Profile**.
The **Device Discovery Profiles** window appears.
3. In the Device Discovery Profiles window, click **+**.
The Device Discovery Target window appears.
4. Select **IP range**.
5. Specify the **Start IP Address** and **End IP Address** information.
6. Click **Next**.
7. In the **Specify Probes** window, select both **Use Ping** and **Use SNMP** as probes.
8. Click **Next**.
9. In the **Specify Credentials** window, select **Authentication Type** and enter the device login credentials.

10. Click **Discover**.

Device discovery begins. It displays a graph showing the status of the discovery operation. Initially, three devices are discovered. When the Junos Space software has accessed all three devices and brought them under its management, all three devices move from the Discovered column of the graph to the Managed column.

11. To check the results of the device discovery operation, select the **Devices** workspace again, then select **Device Management**. The **Manage Devices** page shows the added devices.

- See Also**
- *Device Discovery Overview* in the *Junos Space Network Application Platform User Guide*
 - *Discovering Devices* in the *Junos Space Network Application Platform User Guide*

Preparing Devices for Prestaging

Before prestaging devices for multipoint-to-multipoint services, the following entities must be configured:

- MPLS must run on each N-PE device.
- MPBGP must run on each N-PE device that you want to participate in a multipoint-to-multipoint service.

To satisfy the preceding criteria, ensure that the following configuration exists on each N-PE device:

```
interfaces {
  ge-0/0/0 {
    unit 0 {
      family inet {
        address 10.1.22.2/30;
      }
      family mpls;
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 192.168.1.30/32;
      }
    }
  }
}
routing-options {
  autonomous-system 65410;
}
protocols {
  mpls {
    interface ge-0/0/0.0;
```

```

        interface lo0.0;
    }
    bgp {
        group CA-Peer {
            type internal;
            local-address 192.168.1.30;
            family l2vpn {
                signaling;
            }
            neighbor 192.168.1.40;
            neighbor 192.168.1.10;
            neighbor 192.168.1.20;
            neighbor 192.168.1.50;
            neighbor 192.168.1.60;
        }
    }
    ospf {
        traffic-engineering;
        area 0.0.0.0 {
            interface lo0.0 {
                passive;
            }
            interface ge-0/0/0.0;
        }
    }
    ldp {
        interface ge-0/0/0.0;
        interface lo0.0;
    }
}

```



NOTE: The OSPF configuration is not required in prestaging.

The VPLS service needs to be enabled in a network device, to make the static pseudowire functionality active in the device. You can activate the static pseudowire functionality by configuring the network device through the CLI window. You need to enter the CLI configuration mode of a network element and run the command

set protocols vpls static-vpls no-tunnel-services

commit

If the device is not configured through CLI, a warning message appears in the application server log, that is the **JBOSS Log**:

To discover and assign the roles of devices:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.

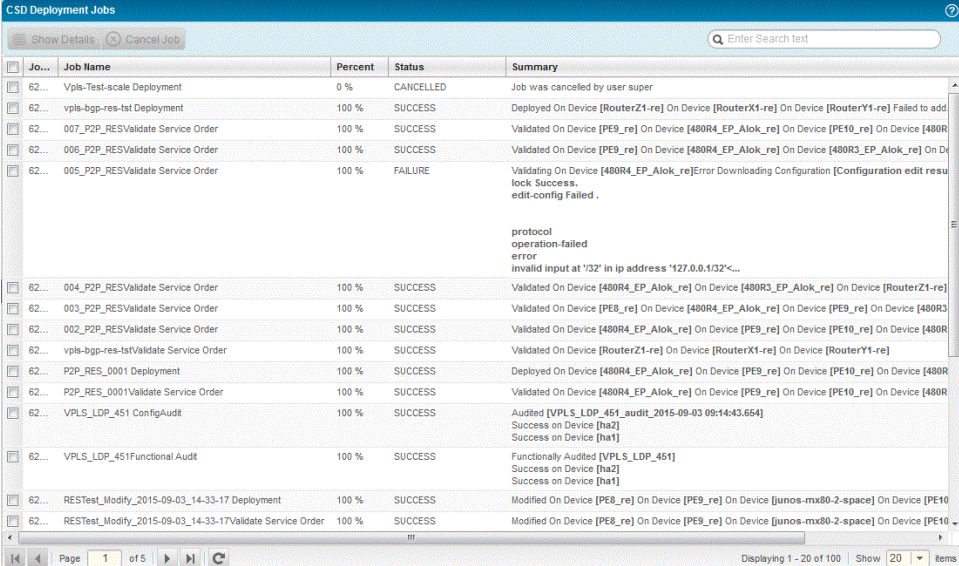
3. In the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.

View the values displayed under the Roles column of the discovered devices.

This action launches the role discovery process in which the Network Services application examines the devices under Junos Space management looking for devices that match predefined rules that identify N-PE devices. In this example, the Role Discovery Status graph shows that the Network Services application has discovered two such devices.

4. Click **Manage Device Roles** and from the drop-down list, select **Discover Roles** to retrieve the roles of the devices. A dialog box is displayed with the job ID of the discovery job that is created to obtain the latest roles of the devices.
5. To view the assignment status, in the **CSD Deployment Jobs** window that you can access from Deploy mode of Service View by selecting **View Deployment Jobs** from the task pane, click the job ID of the assignment job.

The **Job Management** page shows the progress and status of the role assignment job.



Job ID	Job Name	Percent	Status	Summary
62...	Vpls-Test-scale Deployment	0 %	CANCELLED	Job was cancelled by user super
62...	vpls-bgp-res-1st Deployment	100 %	SUCCESS	Deployed On Device [RouterZ1-re] On Device [RouterX1-re] On Device [RouterY1-re] Failed to add
62...	007_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE9_re] On Device [480R4_EP_Alok_re] On Device [PE10_re] On Device [480R3_EP_Alok_re]
62...	006_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE9_re] On Device [480R4_EP_Alok_re] On Device [480R3_EP_Alok_re] On Device [480R4_EP_Alok_re]
62...	005_P2P_RESValidate Service Order	100 %	FAILURE	Validating On Device [480R4_EP_Alok_re]Error Downloading Configuration [Configuration edit resu lock Success. edit-config Failed . protocol operation-failed error invalid input at '02' in ip address '127.0.0.1/32'<...
62...	004_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [480R3_EP_Alok_re] On Device [RouterZ1-re]
62...	003_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE8_re] On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [480R3_EP_Alok_re]
62...	002_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R3_EP_Alok_re]
62...	vpls-bgp-res-1stValidate Service Order	100 %	SUCCESS	Validated On Device [RouterZ1-re] On Device [RouterX1-re] On Device [RouterY1-re]
62...	P2P_RES_0001 Deployment	100 %	SUCCESS	Deployed On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R3_EP_Alok_re]
62...	P2P_RES_0001Validate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R3_EP_Alok_re]
62...	VPLS_LDP_451 ConfigAudit	100 %	SUCCESS	Audited [VPLS_LDP_451_audit_2015-09-03 09:14:43.654] Success on Device [ha2] Success on Device [ha1]
62...	VPLS_LDP_451Functional Audit	100 %	SUCCESS	Functionally Audited [VPLS_LDP_451] Success on Device [ha2] Success on Device [ha1]
62...	RESTTest_Modify_2015-09-03_14-33-17 Deployment	100 %	SUCCESS	Modified On Device [PE8_re] On Device [PE9_re] On Device [junos-mx80-2-space] On Device [PE10_re]
62...	RESTTest_Modify_2015-09-03_14-33-17Validate Service Order	100 %	SUCCESS	Modified On Device [PE8_re] On Device [PE9_re] On Device [junos-mx80-2-space] On Device [PE10_re]

6. To verify the result, in Build mode, select **Prestage Devices > Manage Device Roles** from the tasks pane.

The **Manage Device Roles** window shows two devices that can be used for provisioning.

7. To unassign a device from N-PE role assignment, click **Manage Device Roles** and from the drop-down list, select **Unassign Role** to remove the role capability of a network element. You are prompted to confirm the operation. If you click **OK**, a request is submitted to remove the latest role of the network element or device.

To re-sync the role of the network elements configured:

1. Select **Prestage Devices > Prestage Devices** from the tasks pane. The Devices Chart page is displayed.
2. To re-sync the role capability of a network element, select the network element's name, and open the **Manage Device Roles** menu.
3. Click **Re-sync Role Capability**. The **Re-sync Role Capability** window appears where you can select the device's name and click **Re-sync**.

The role is re-synced with the same device now.

Discovering and Assigning N-PE Roles

Before you can provision services, you must prestage the devices. prestaging includes assigning device roles and designating interfaces on those devices as UNIs. This example provides the steps to accept the recommendations of the Network Services application for N-PE devices and UNIs.

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. In the **Service View** task pane, select **Network Services**.
4. In the **Tasks** task pane, select **Prestage Devices > Prestage Devices**.

View the values displayed under the Roles column of the discovered devices.

This action launches the role discovery process in which the Network Services application examines the devices under Junos Space management looking for devices that match predefined rules that identify N-PE devices. In this example, the Role Discovery Status graph shows that the Network Services application has discovered two such devices.

5. Click **Manage Device Roles** and from the drop-down list, select **Discover Roles** to retrieve the roles of the devices. A dialog box is displayed with the job ID of the discovery job that is created to obtain the latest roles of the devices.
6. To view the assignment status, in the **CSD Deployment Jobs** window that you can access from Deploy mode of Service View by selecting **View Deployment Jobs** from the task pane, click the job ID of the assignment job.

The **Job Management** page shows the progress and status of the role assignment job.

The screenshot shows the 'CSD Deployment Jobs' window. It contains a table with columns: Job Name, Percent, Status, and Summary. The table lists various deployment and validation jobs, including 'Vpls-Test-scale Deployment', 'vpls-bgp-res-tst Deployment', and several 'P2P_RESValidate Service Order' jobs. The status of these jobs varies, with some being 'CANCELLED', 'SUCCESS', or 'FAILURE'. The summary column provides detailed logs for each job, such as 'Job was cancelled by user super' or 'Validated On Device [480R4_EP_Alok_re] On Device [480R3_EP_Alok_re] On Device [480R2_EP_Alok_re] On Device [480R1_EP_Alok_re]'.

Job Name	Percent	Status	Summary
62... Vpls-Test-scale Deployment	0 %	CANCELLED	Job was cancelled by user super
62... vpls-bgp-res-tst Deployment	100 %	SUCCESS	Deployed On Device [RouterZ1-re] On Device [RouterX1-re] On Device [RouterY1-re] Failed to add
62... 007_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE9_re] On Device [480R4_EP_Alok_re] On Device [PE10_re] On Device [480R3_EP_Alok_re] On Device [480R2_EP_Alok_re] On Device [480R1_EP_Alok_re]
62... 008_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE9_re] On Device [480R4_EP_Alok_re] On Device [480R3_EP_Alok_re] On Device [480R2_EP_Alok_re] On Device [480R1_EP_Alok_re]
62... 005_P2P_RESValidate Service Order	100 %	FAILURE	Validating On Device [480R4_EP_Alok_re]Error Downloading Configuration [Configuration edit resu lock Success. edit-config Failed .
62... 004_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [480R3_EP_Alok_re] On Device [RouterZ1-re]
62... 003_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE8_re] On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [480R3_EP_Alok_re] On Device [480R2_EP_Alok_re] On Device [480R1_EP_Alok_re]
62... 002_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R3_EP_Alok_re] On Device [480R2_EP_Alok_re] On Device [480R1_EP_Alok_re]
62... vpls-bgp-res-tstValidate Service Order	100 %	SUCCESS	Validated On Device [RouterZ1-re] On Device [RouterX1-re] On Device [RouterY1-re]
62... P2P_RES_0001 Deployment	100 %	SUCCESS	Deployed On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R3_EP_Alok_re] On Device [480R2_EP_Alok_re] On Device [480R1_EP_Alok_re]
62... P2P_RES_0001Validate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R3_EP_Alok_re] On Device [480R2_EP_Alok_re] On Device [480R1_EP_Alok_re]
62... VPLS_LDP_451 ConfigAudit	100 %	SUCCESS	Audited [VPLS_LDP_451_audit_2015-09-03 09:14:43.654] Success on Device [ha2] Success on Device [ha1]
62... VPLS_LDP_451Functional Audit	100 %	SUCCESS	Functionally Audited [VPLS_LDP_451] Success on Device [ha2] Success on Device [ha1]
62... RESTTest_Modify_2015-09-03_14-33-17 Deployment	100 %	SUCCESS	Modified On Device [PE8_re] On Device [PE9_re] On Device [junos-mx80-2-space] On Device [PE10_re] On Device [480R4_EP_Alok_re] On Device [480R3_EP_Alok_re] On Device [480R2_EP_Alok_re] On Device [480R1_EP_Alok_re]
62... RESTTest_Modify_2015-09-03_14-33-17Validate Service Order	100 %	SUCCESS	Modified On Device [PE8_re] On Device [PE9_re] On Device [junos-mx80-2-space] On Device [PE10_re] On Device [480R4_EP_Alok_re] On Device [480R3_EP_Alok_re] On Device [480R2_EP_Alok_re] On Device [480R1_EP_Alok_re]

- To verify the result, in Build mode, select **Prestage Devices > Manage Device Roles** from the tasks pane.

The **Manage Device Roles** window shows two devices that can be used for provisioning.

- To unassign a device from N-PE role assignment, click **Manage Device Roles** and from the drop-down list, select **Unassign Role** to remove the role capability of a network element. You are prompted to confirm the operation. If you click **OK**, a request is submitted to remove the latest role of the network element or device.

- See Also**
- [Discovering and Assigning All N-PE Devices on page 351](#)
 - [Discovering and Assigning N-PE Devices with Exceptions on page 353](#)

Choosing or Creating a Service Definition

A service definition provides a template upon which services are built. It specifies service attributes that are not specific to a service instance. In this example, the service definition provides all service attributes except the N-PE devices, the UNIs, and bandwidth.

The Network Services application ships with standard service definitions. First, we check the standard service definitions to determine whether one already exists that can work.

- From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
- Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.

3. In the **Network Services** task pane, select **Connectivity** .

4. In the **Tasks** task pane, select **Service Design > Manage Service Definitions**

The **Manage Service Definitions** page lists all service definitions in the system. In a new system, the page lists only predefined service definitions.

This example requires a multipoint-to-multipoint service definition with UNIs that use 802.1Q interfaces and allow you to set a bandwidth of 25 Mbps. The standard service definitions have several examples for provisioning 802.1Q UNIs, but none that allow the setting of a 25 Mbps bandwidth limit. You need to create a new service definition.

5. In the Manage Service Definitions page, click **New > VPLS Service Definition**.

The General Settings window appears.

6. Enter a name for the service definition.

7. Click **Next**.

8. In the **Site Settings** window, in the **VLAN Tagging** field, select **dot1q**.

9. In the **Physical Interface Encapsulation** field, select **flexible-ethernet-service**.

10. In the **Logical Interface Encapsulation** field, select **vlan-vpls**.

11. In the **Traffic type** field, select **Transport single VLAN**.

12. Because we intend to select a specific VLAN for each endpoint in the service—leave the Normalized VLAN setting as the default **Normalization not required**.

13. In the **VLAN ID selection** field, choose **Select manually**.

14. In the **VLAN range for manual input**, specify the range.



NOTE: When the range of VLAN IDs that are automatically assigned by the system (with the auto-pick option enabled during the creation of a service definition) is less than or greater than the range of VLAN IDs that are manually specified (with the manual selection option enabled during the creation of a service definition), the following conditions apply during the creation of a service order with the Editable in Service Order check box selected during service definition creation:

- If you create a service order with the auto-pick option enabled, the VLAN ID is selected from the auto-pick range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range.
- If you create a service order with the auto-pick option disabled, the VLAN ID is selected from the manually configured range, and the value is displayed in the VLAN range for manual input field. If you attempt to change the VLAN ID manually, the value is restricted to the manually configured range.

15. In the **Outer Tag protocol ID**, select **0x8100**
16. In the **PE-CE Interface Rate Limiting Settings** panel, select the **Enable Interface Rate Limiting** check box.
17. In the **Rate Limit (Mbps)** field, enter **10**, for a default bandwidth of 10 Mbps.
18. To the right of the value you just entered, select the **Editable in service order** check box.

The **Rate Limit Range for manual-config (Min in Kbps, Max in Mbps)** and **Increment (Kbps)** fields become active.
19. In the **Rate Limit Range for manual-config (Min in Kbps, Max in Mbps)** fields, enter **10** and **64** respectively.
20. In the **Increment** field, enter **64**.
21. Click **Next** to proceed to the Review page of the wizard.
22. To save and complete the service definition, click **Done**.

The **Manage Service Definitions** page includes the new service definition.

You have created a customized Service Definition, but it has not yet been published. Before a service definition can be used in provisioning, it must be published.

23. To publish the service definition, in the **Manage Service Definitions** page, select the `vpls-dot1q-sd-1` service definition, and click the **Publish** button.

The **Information** window appears.

24. To confirm that you want to publish this service definition, click **Yes**.

In the **Manage Service Definitions** page, the **State** column changes to Published.

The service definition is now ready for use in provisioning.

- See Also**
- *Predefined Service Definitions*
 - *Creating a Multipoint-to-Multipoint VPLS Service Definition*
 - *Publishing a Custom Service Definition*

Creating a Customer

Before you can provision the service, customer details must be present in the Junos Space data base. To add a customer:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. In the **Service View** task pane, select **Customers**.
4. In the **Tasks** task pane, select **Customer > Manage Customers**.
5. In the **View Customers** task pane, select **Add (+)**.
6. In the **Name** field, enter **Best Customer**.
7. In the **Account number** field, enter **1234**.
8. Click **Create**.

The **Manage Customers** page shows the new customer.

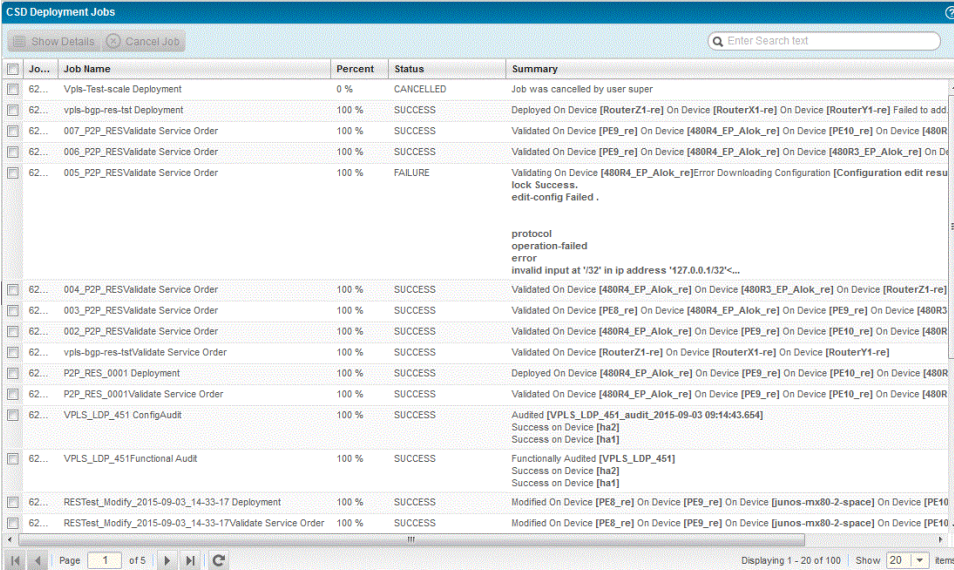
- See Also**
- *Adding a New Customer*

Creating and Deploying a Multipoint-to-Multipoint Service Order

Now that you have prestaged your devices, created a suitable service definition, and added the customer information to the database, you are ready to create and deploy a service order.

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services > VPLS Services to expand the tree and display the different service types that you can configure.
4. Select **Manage Services** from the task pane. The right pane displays two pages. The Manage Network Services page is displayed in the upper half of the right pane. Selecting a service from this page causes the associated service orders for the selected service to be displayed in the Manage Service Orders page in the lower half of the right pane.
5. Click the **New** icon at the top of the upper half of the page that displays previously created service orders.
6. In the Name field of the **Service Settings** window, in the **Name** field, enter **vpls_so_1**.
7. In the **Customer** field, select the customer for which you are creating the service order.
8. In the **Service Definition** field, select the service definition named **vpls-dot1q-sd-1**.
This service definition is the customized service definition you created earlier.
9. Click **Next**.
10. In the Node Settings page, add the **BLR**, **SFO**, and **SJC** devices or endpoints, and configure the roles of the devices.
11. Click **Next**.
12. In the Site Settings page, in the **Rate Limit** field, select **25**.
13. Clear the **Autopick VLAN ID** check box.

14. In the **VLAN ID** field, enter **600**.
15. Click **Next** to proceed to the Review page, which is the final step of the wizard.
16. Click **Done**. The VPLS service order is created.
17. Select the created VPLS service order in the Manage Service Orders page. You can save the service order for later deployment, schedule the service order for later deployment, or deploy the service order now. Click **Deploy now**.
18. Click **OK** to start the deployment.
19. To monitor the progress and status of the deployment, in the Manage Service Orders page, click the job ID under the Latest Job field. The **Job Management** page shows the status of the job.



Job ID	Job Name	Percent	Status	Summary
62...	Vpls-Test-scale Deployment	0 %	CANCELLED	Job was cancelled by user super
62...	vpls-bgp-res-lst Deployment	100 %	SUCCESS	Deployed On Device [RouterZ1-re] On Device [RouterX1-re] On Device [RouterY1-re] Failed to add...
62...	007_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE9_re] On Device [480R4_EP_Alok_re] On Device [PE10_re] On Device [480R3...
62...	006_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE9_re] On Device [480R4_EP_Alok_re] On Device [480R3_EP_Alok_re] On Device [480R...
62...	005_P2P_RESValidate Service Order	100 %	FAILURE	Validating On Device [480R4_EP_Alok_re]Error Downloading Configuration [Configuration edit resu lock Success. edit-config Failed . protocol operation-failed error Invalid input at '132' in ip address '127.0.0.1/32'<...
62...	004_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [480R3_EP_Alok_re] On Device [RouterZ1-re]
62...	003_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE8_re] On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [480R3...
62...	002_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R...
62...	vpls-bgp-res-lstValidate Service Order	100 %	SUCCESS	Validated On Device [RouterZ1-re] On Device [RouterX1-re] On Device [RouterY1-re]
62...	P2P_RES_0001 Deployment	100 %	SUCCESS	Deployed On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R...
62...	P2P_RES_0001Validate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R...
62...	VPLS_LDP_451 ConfigAudit	100 %	SUCCESS	Audited [VPLS_LDP_451_audit_2015-09-03 09:14:43.654] Success on Device [ha2] Success on Device [ha1]
62...	VPLS_LDP_451Functional Audit	100 %	SUCCESS	Functionally Audited [VPLS_LDP_451] Success on Device [ha2] Success on Device [ha1]
62...	RESTTest_Modify_2015-09-03_14-33-17 Deployment	100 %	SUCCESS	Modified On Device [PE8_re] On Device [PE9_re] On Device [junos-mx80-2-space] On Device [PE10...
62...	RESTTest_Modify_2015-09-03_14-33-17Validate Service Order	100 %	SUCCESS	Modified On Device [PE8_re] On Device [PE9_re] On Device [junos-mx80-2-space] On Device [PE10...

20. When you see in the **Job Management** window that the deployment is successful, in the Network Services task pane, select the **Service Provisioning** workspace again.
21. In the task pane, select **Deploy Services**.

The **Manage Network Services** page, which is displayed in the top half of the right pane, shows the new service.

- See Also**
- *Creating a Multipoint-to-Multipoint VPLS Service Order*
 - *Deploying a Service Order*

Performing a Functional Audit and a Configuration Audit

Now that your new service is deployed, we recommend that you validate its configuration and functional integrity. A functional audit runs operational commands on the device to verify that the service is up or down. A configuration audit verifies whether the configuration that was pushed to the device during deployment is actually on the device.

To perform a configuration audit and a functional audit of the service:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services > VPLS Services to expand the tree and display the different service types that you can configure.
4. Select **Manage Services** from the task pane. The right pane displays two pages. The Manage Network Services page is displayed in the upper half of the right pane. Selecting a service from this page causes the associated service orders for the selected service to be displayed in the Manage Service Orders page in the lower half of the right pane.
5. In the **Manage Network Services** page, select the service instance you just deployed.
6. Select the service instance, click the **Audit** menu and select **Functional Audit > Run Functional Audit**.
7. In the **Schedule Functional Audit** window, you can choose to perform the audit now or schedule it for later. Select **Audit now**, then click **OK**.
8. In the **Order Information** screen, click **OK**.
9. Select the service instance, click the **Audit** menu and select **Configuration Audit > Run Configuration Audit**.
10. In the **Schedule Configuration Audit** window, you can choose to perform the audit now or schedule it for later. Select **Audit now**, and then click **OK**.
11. In the **Order Information** window, click **OK**.

When the audit jobs have finished, success is indicated by an up arrow in the top right corner of the service.

12. To view the functional audit results, select the service instance and click **Audit > Functional Audit > View Results**.

In the **Functional Audit Results** window, select each device to view the results.

13. To view the results of the configuration audit, select the service instance and click **Audit > Configuration Audit > View Results**.

In the **Configuration Audit Results** window, select each device in turn and review the results. This report indicates any part of the service configuration that is missing on the device, or is inconsistent with the Junos Space database.

Following a successful audit, the service is deployed and ready to be used.

- Related Documentation**
- *Device Discovery Overview* in the *Junos Space Network Application Platform User Guide*
 - *Discovering Devices* in the *Junos Space Network Application Platform User Guide*

Example: Configuring and Deploying a Layer 3 VPN Full-Mesh Service

This example shows how to set up a simple full-mesh service provider VPN configuration, as shown in [Figure 63 on page 1319](#).

Figure 63: Simple Layer 3 VPN Full-Mesh Service

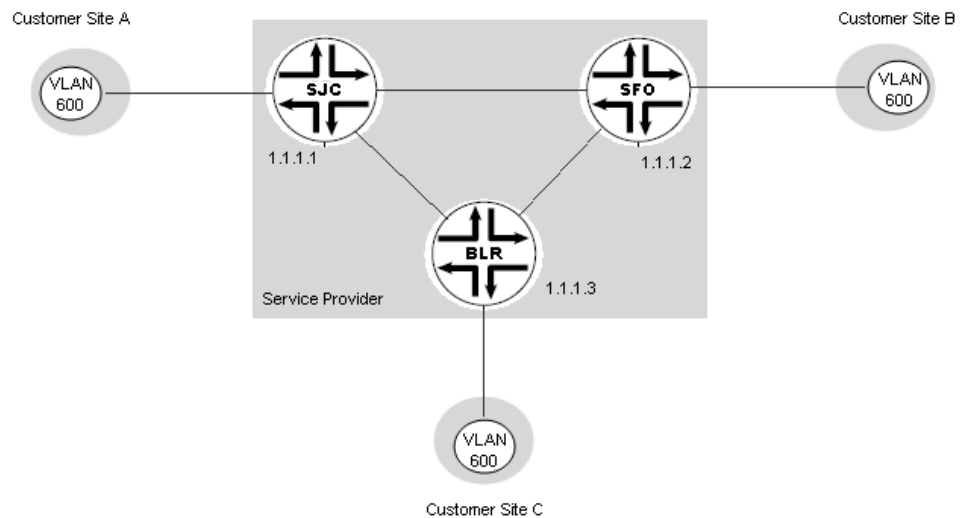
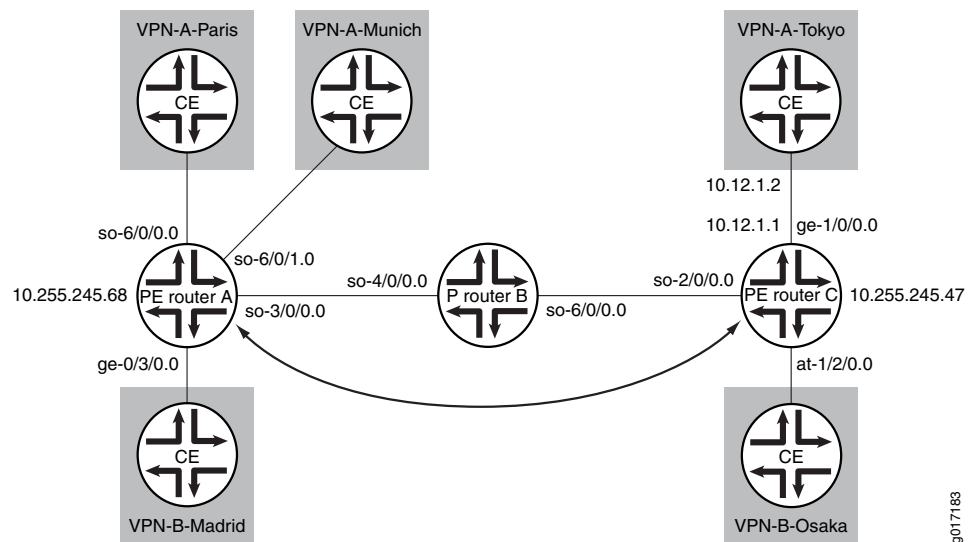


Figure 64: Example of a Simple VPN Topology



This service provides connectivity for one VLAN, (VLAN ID = 600). Customer site A connects to the network through an N-PE device named SJC (IP address 1.1.1.1). Customer site B connects to the network through an N-PE device named SFO (IP address 1.1.1.2). Customer site C connects to the network through an N-PE device named BLR (IP address 1.1.1.3).

- [Preparing Devices for Discovery on page 1320](#)
- [Discovering Devices on page 1321](#)
- [Preparing Devices for Prestaging on page 1322](#)
- [Discovering and Assigning N-PE Roles on page 1323](#)
- [Choosing or Creating a Service Definition on page 1324](#)
- [Creating a Customer on page 1326](#)
- [Creating and Deploying a Layer 3 VPN Service Order on page 1327](#)
- [Performing a Functional Audit and a Configuration Audit on page 1329](#)

Preparing Devices for Discovery

Before you can add a device using device discovery, the following conditions must be met:

- SSH v2 is enabled on the device. To enable SSH v2 on a device, issue the following CLI command:

```
set system services ssh protocol-version v2
```

- The NETCONF protocol over SSH is enabled on the device. To enable the NETCONF protocol over SSH on a device, issue the following CLI command:

```
set system services netconf ssh
```


- The device is configured with a static management IP address that is reachable from the Junos Space server. The IP address can be in-band or out-of-band.
- A user with full administrative privileges is created on the device for the Junos Space administrator.
- If you plan to use SNMP to probe devices as part of device discovery, ensure that SNMP is enabled on the device with appropriate read-only V1/V2C/V3 credentials.

Discovering Devices

Device discovery is a process that Junos Space uses to bring network devices under its control. This example brings two MX Series routers under Junos Space management.



NOTE: Alternatively, you can import devices using the Connectivity Services Director GUI. See [“Discovering Devices in a Physical Network” on page 177](#) for instructions on discovering devices from Build mode of Connectivity Services Director.

1. Log in to Junos Space using your credentials.
2. From the Junos Space Network management Platform user interface, select **Devices** > **Discover Devices** > **Discover Targets**.
3. In the **Discover Targets** window, click **+**.
The **Add Device Target** window appears.
4. Select **IP range**.
5. Enter the IP address information. This example uses a range of three addresses.

6. Click **Add**, and then click **Next**.
7. In the **Devices: Specify Probes** window, select both **Ping** and **SNMP** as probes.
8. Click **Next**.

9. In the Devices: **Specify Credentials** window, click **+** and enter the device login credentials.

10. Click **Finish**.

Device discovery begins. It displays a graph showing the status of the discovery operation. Initially, three devices are discovered. When the Junos Space software has accessed all three devices and brought them under its management, all three devices move from the Discovered column of the graph to the Managed column.

11. To check the results of the device discovery operation, select the **Devices** workspace again, then select **Device Management**. The **Manage Devices** page shows the added devices.

See Also

- *Device Discovery Overview* in the *Junos Space Network Application Platform User Guide*
- *Discovering Devices* in the *Junos Space Network Application Platform User Guide*

Preparing Devices for Prestaging

Before prestaging devices for multipoint-to-multipoint services, the following entities must be configured:

- MPLS must run on each N-PE device.
- MPBGP must run on each N-PE device that you want to participate in a Layer 3 full mesh service.

To satisfy the preceding criteria, ensure that the following configuration exists on each N-PE device:

```
interfaces {
  ge-0/0/0 {
    unit 0 {
      family inet {
        address 10.1.22.2/30;
      }
      family mpls;
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 192.168.1.30/32;
      }
    }
  }
}
routing-options {
  autonomous-system 65410;
```

```

}
protocols {
  mpls {
    interface ge-0/0/0.0;
    interface lo0.0;
  }
  bgp {
    group IBGP {
      type internal;
      local-address 192.168.10.1;
      family inet-vpn {
        unicast;
      }
      peer-as 65410;
      neighbor 192.168.10.4;
    }
  }
  ospf {
    traffic-engineering;
    area 0.0.0.0 {
      interface lo0.0 {
        passive;
      }
      interface ge-0/0/0.0;
    }
  }
  ldp {
    interface ge-0/0/0.0;
    interface lo0.0;
  }
}

```

Discovering and Assigning N-PE Roles

Before you can provision services, you must prestage the devices. prestaging includes assigning device roles and designating interfaces on those devices as UNIs. This example provides the steps to accept the recommendations of the Network Services application for N-PE devices and UNIs.

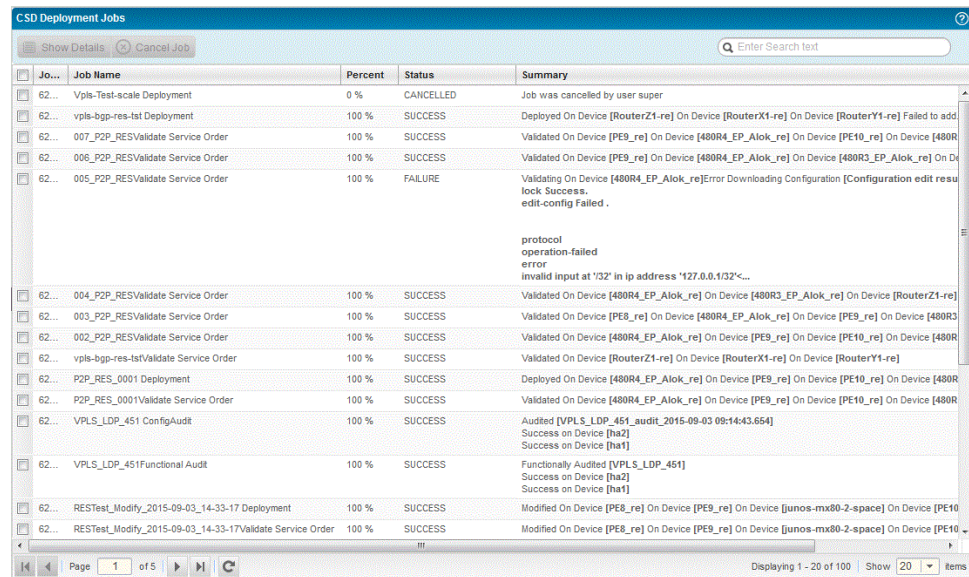
1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. In the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**.

View the values displayed under the Roles column of the discovered devices.

This action launches the role discovery process in which the Network Services application examines the devices under Junos Space management looking for devices that match predefined rules that identify N-PE devices. In this example, the Role Discovery Status graph shows that the Network Services application has discovered two such devices.

- Click **Manage Device Roles** and from the drop-down list, select **Discover Roles** to retrieve the roles of the devices. A dialog box is displayed with the job ID of the discovery job that is created to obtain the latest roles of the devices.
- To view the assignment status, in the **CSD Deployment Jobs** window that you can access from Deploy mode of Service View by selecting **View Deployment Jobs** from the task pane, click the job ID of the assignment job.

The **Job Management** page shows the progress and status of the role assignment job.



Job ID	Job Name	Percent	Status	Summary
62...	Vpls-Test-scale Deployment	0 %	CANCELLED	Job was cancelled by user super
62...	vpls-bgp-res-tst Deployment	100 %	SUCCESS	Deployed On Device [RouterZ1-re] On Device [RouterX1-re] On Device [RouterY1-re] Failed to add...
62...	007_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE9_re] On Device [480R4_EP_Alok_re] On Device [PE10_re] On Device [480R...
62...	006_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE9_re] On Device [480R4_EP_Alok_re] On Device [480R3_EP_Alok_re] On Dk...
62...	005_P2P_RESValidate Service Order	100 %	FAILURE	Validating On Device [480R4_EP_Alok_re]Error Downloading Configuration [Configuration edit resu edit-config Failed . protocol operation-failed error invalid input at '32' in ip address '127.0.0.1/32'<...
62...	004_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [480R3_EP_Alok_re] On Device [RouterZ1-re]
62...	003_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE8_re] On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [480R3]
62...	002_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R...
62...	vpls-bgp-res-tstValidate Service Order	100 %	SUCCESS	Validated On Device [RouterZ1-re] On Device [RouterX1-re] On Device [RouterY1-re]
62...	P2P_RES_0001 Deployment	100 %	SUCCESS	Deployed On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R...
62...	P2P_RES_0001Validate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R...
62...	VPLS_LDP_451 ConfigAudit	100 %	SUCCESS	Audited [VPLS_LDP_451_audit_2015-09-03 09:14:43.654] Success on Device [ha2] Success on Device [ha1]
62...	VPLS_LDP_451Functional Audit	100 %	SUCCESS	Functionally Audited [VPLS_LDP_451] Success on Device [ha2] Success on Device [ha1]
62...	REStest_Modify_2015-09-03_14-33-17 Deployment	100 %	SUCCESS	Modified On Device [PE8_re] On Device [PE9_re] On Device [junos-mx80-2-space] On Device [PE10...
62...	REStest_Modify_2015-09-03_14-33-17Validate Service Order	100 %	SUCCESS	Modified On Device [PE8_re] On Device [PE9_re] On Device [junos-mx80-2-space] On Device [PE10...

- To verify the result, in Build mode, select **Prestage Devices > Manage Device Roles** from the tasks pane.

The **Manage Device Roles** window shows two devices that can be used for provisioning.

- To unassign a device from N-PE role assignment, click **Manage Device Roles** and from the drop-down list, select **Unassign Role** to remove the role capability of a network element. You are prompted to confirm the operation. If you click **OK**, a request is submitted to remove the latest role of the network element or device.

- See Also**
- *Prestaging Devices Overview*
 - *Discovering and Assigning All N-PE Devices*
 - *Discovering and Assigning N-PE Devices with Exceptions*

Choosing or Creating a Service Definition

A service definition provides a template upon which services are built. It specifies service attributes that are not specific to a service instance. In this example, the service definition provides all service attributes except the N-PE devices, the UNIs, and bandwidth.

The Network Services application ships with standard service definitions. First, we check the standard service definitions to determine whether one already exists that will work.

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. In the **Network Services > Connectivity** task pane, select **Service Design > Manage Service Definitions**.

The **Manage Service Definitions** page lists all service definitions in the system. In a new system, the page lists only predefined service definitions.

This example requires a L3 VPN full mesh service definition with OSPF/Static routing to allow each PE router to distribute VPN-related routes to and from connected CE routers.

4. In the **Network Services > Connectivity** task pane, select **Service Design > Manage Service Definitions > New > L3VPN Service Definition**.

The General Settings window appears.

5. In the name field, enter the name “l3vpn-ospf-static-full-mesh-sd” for the service definition.
6. In the **Service type** field, select **L3 VPN (Full Mesh)**.



NOTE: This service definition does not include a service template definition for the service, so the **Service Template Definition** field is left blank.

7. In the **Connectivity Settings** box, select **Auto pick Route Distinguisher** to allow the Network Services application to automatically select the route distinguisher.
8. Click **Next** to save the General Settings step information.
Continue with “Site Settings” next.
9. In the VLAN ID selection field, select **Select manually** to have the service provisioner select a VLAN ID for the service.
10. To enable the service provisioner to override this setting in a service order, select the **Editable in service order** check box.

11. In the **VLAN range for manual input**, enter “500” and “700” for VLAN ID start and end values to restrict the range of VLANs to this pool.
12. In the PE-CE Settings box, select the **OSPF/Static Route** radio button for Allowed Routing Protocols to use OSPF/Static to allow each PE router to distribute VPN-related routes to and from connected CE routers.
13. Click **Review** to review and create the Layer 3 VPN service definition.

14. To save and complete the service definition, click **Finish**.

The **Manage Service Definitions** page includes the new service definition.

You have created a customized Service Definition, but it has not yet been published. Before a service definition can be used in provisioning, it must be published.

15. To publish the service definition, in the **Manage Service Definitions** page, select the vpls-dot1q-sd-1 service definition, and click the **Publish Service Definition** button.

The **Publish Service Definition** window appears.

16. To confirm that you want to publish this service definition, click **Publish**.

In the **Manage Service Definitions** page, the **State** column changes to Published.

The service definition is now ready for use in provisioning.

Creating a Customer

Before you can provision the service, customer details must be present in the Junos Space database. To add a customer:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. In the **Network Services > Connectivity** task pane, select **Service Provisioning > Manage Customers > Create Customer**.
4. In the **Name** field, enter **Best Customer**.
5. In the **Account number** field, enter **1234**.
6. Click **Create**

The **Manage Customers** window shows the new customer.

See Also • *Adding a New Customer*

Creating and Deploying a Layer 3 VPN Service Order

Now that you have prestaged your devices, created a suitable service definition, and added the customer information to the database, you are ready to create and deploy a service order.

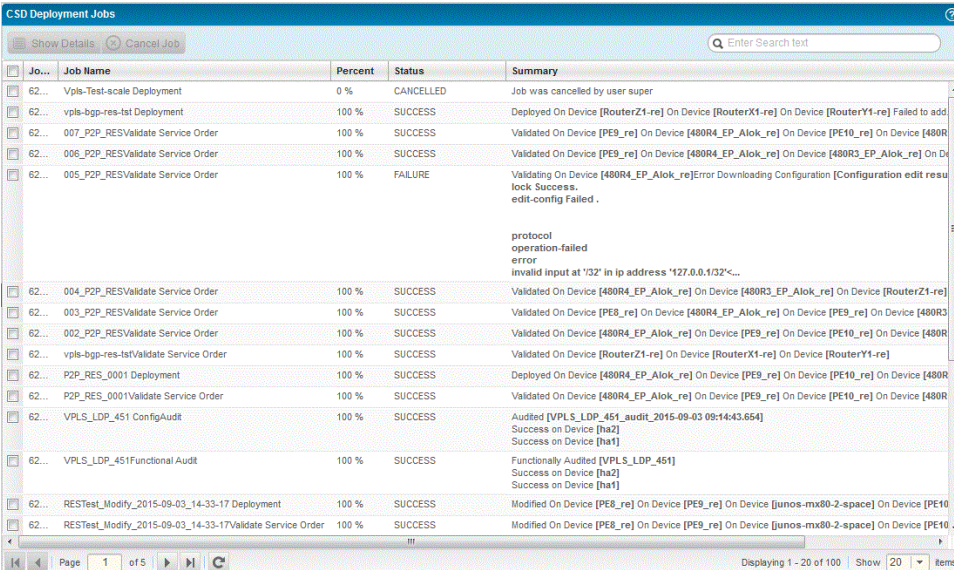
1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services > VPLS Services to expand the tree and display the different service types that you can configure.
4. Select **Deploy Services** from the task pane. The right pane displays two pages. The Manage Network Services page is displayed in the upper half of the right pane. Selecting a service from this page causes the associated service orders for the selected service to be displayed in the Manage Service Orders page in the lower half of the right pane.
5. Click the **New** icon at the top of the upper half of the page that displays previously created service orders. The Select Service Type dialog box appears.
6. Select **L3VPN** to create a Layer 3 VPN service order.

The General/Connectivity Settings panel appears initially in the right panel, as shown in the example.
7. In the **Create L3 VPN Service Order** window, select the service definition named **l3vpn-ospf-static-full-mesh-sd**.

This service definition is the customized service definition you created earlier.
8. In the **General Settings** box of the **Service Settings** window, in the **Name** field, enter **l3vpn_ospf_full_mesh_so**.
9. In the **Customer** field, select **Best Customer**.
10. In the PE-CE Settings box, enter "1.1.1.1" as the **OSPF domain ID**.

11. Click **Next**.
12. In the **Node Settings** window, select **BLR**, **SFO**, and **SJC** as the endpoint devices.
13. Click **Next**.
14. In the **Site Settings** window, clear the **Autopick VLAN ID** check box (the default setting).
15. In the VLAN ID field, enter "600".
16. In the **Interface IP** field, enter an IP address/subnet for the device, for example, 10.255.245.68/28.
17. In the **OSPF area ID** field, enter an IP address for the OSPF area.
18. Click **Save**.
19. Repeat Step 10 through Step 12, for each endpoint device that you want to include in the service.
20. Click **Next**. The Review page of the wizard is displayed.
21. Click **Done**. The service order is created and listed in the Manage Service Orders page.
22. You can schedule the deployment of the service order for a specific time, or deploy the service now. Select **Deploy now** and click **OK** to start the deployment.

23. To monitor the progress and status of the deployment, in the Order Information window, click the job ID. The **Job Management** page shows the status of the job.



Job ID	Job Name	Percent	Status	Summary
62...	Vpls-Test-scale Deployment	0 %	CANCELLED	Job was cancelled by user super
62...	vpls-bgp-res-1st Deployment	100 %	SUCCESS	Deployed On Device [RouterZ1-re] On Device [RouterX1-re] On Device [RouterY1-re] Failed to add...
62...	007_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE9_re] On Device [480R4_EP_Alok_re] On Device [PE10_re] On Device [480R...
62...	006_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE9_re] On Device [480R4_EP_Alok_re] On Device [480R3_EP_Alok_re] On D...
62...	005_P2P_RESValidate Service Order	100 %	FAILURE	Validating On Device [480R4_EP_Alok_re] Error Downloading Configuration [Configuration edit resu lock Success. edit-config Failed . protocol operation-failed error Invalid input at '132' in ip address '127.0.0.1/32'<...
62...	004_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [480R3_EP_Alok_re] On Device [RouterZ1-re]
62...	003_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE8_re] On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [480R3...
62...	002_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R...
62...	vpls-bgp-res-1stValidate Service Order	100 %	SUCCESS	Validated On Device [RouterZ1-re] On Device [RouterX1-re] On Device [RouterY1-re]
62...	P2P_RES_0001 Deployment	100 %	SUCCESS	Deployed On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R...
62...	P2P_RES_0001Validate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R...
62...	VPLS_LDP_451 ConfigAudit	100 %	SUCCESS	Audited [VPLS_LDP_451_audit_2015-09-03 09:14:43.654] Success on Device [ha2] Success on Device [ha1]
62...	VPLS_LDP_451Functional Audit	100 %	SUCCESS	Functionally Audited [VPLS_LDP_451] Success on Device [ha2] Success on Device [ha1]
62...	REStest_Modify_2015-09-03_14-33-17 Deployment	100 %	SUCCESS	Modified On Device [PE8_re] On Device [PE9_re] On Device [junos-mx80-2-space] On Device [PE10...
62...	REStest_Modify_2015-09-03_14-33-17Validate Service Order	100 %	SUCCESS	Modified On Device [PE8_re] On Device [PE9_re] On Device [junos-mx80-2-space] On Device [PE10...

24. When you see in the **Job Management** page that the deployment is successful, in the **Network Services** task pane, select the **Service Provisioning > Manage Deploy Services**.
The **Manage Network Services** page shows the new Layer 3 VPN full mesh service.

Performing a Functional Audit and a Configuration Audit

Now that your new service is deployed, we recommend that you validate its configuration and functional integrity. A functional audit runs operational commands on the device to verify that the service is up or down. A configuration audit verifies whether the configuration that was pushed to the device during deployment is actually on the device.

To perform a configuration audit and a functional audit of the service:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services > P2P Services to expand the tree and display the different service types that you can configure.
4. Select **Deploy Services** from the task pane. The right pane displays two pages. The Manage Network Services page is displayed in the upper half of the right pane. Selecting a service from this page causes the associated service orders for the selected

service to be displayed in the Manage Service Orders page in the lower half of the right pane.

5. In the **Manage Network Services** page, select the service instance you just deployed.
6. Select the service instance, and open the **Actions** menu and select **Run Functional Audit**.
7. In the **Schedule Functional Audit** window, you can choose to perform the audit now or schedule it for later. Select **Audit now**, then click **OK**.
8. In the **Order Information** screen, click **OK**.
9. Select the service instance, and open the **Audit** menu and select **Run Configuration Audit**.
10. In the **Schedule Configuration Audit** window, you can choose to perform the audit now or schedule it for later. Select **Audit now**, and then click **OK**.
11. In the **Order Information** window, click **OK**.

When the audit jobs have finished, success is indicated by an up arrow in the top right corner of the service.
12. To view the functional audit results:
 - a. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
 - b. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
 - c. From the **Network Services > Connectivity > L3VPN Services** View pane, select the **l3vpn_ospf_full_mesh_so** service instance.

- d. In the tasks pane, select **Audit/Results > Functional Audit**.
 - e. In the **Functional Audit Results** window, select each device to view the results.
13. To view the results of the configuration audit:
- a. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
 - b. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
 - c. From the **Network Services > Connectivity > L3VPN Services** View pane, select the **l3vpn_ospf_full_mesh_so** service instance.
 - d. In the tasks pane, select **Audit/Results > Configuration Audit**.
 - e. In the **Configuration Audit Results** window, select each device in turn and review the results. This report indicates any part of the service configuration that is missing on the device, or is inconsistent with the Junos Space database.

Following a successful audit, the service is deployed and ready to be used.

PART 16

Working with Chassis View

- [Working with Devices on page 1335](#)
- [Managing CLI Configlets on page 1349](#)

Working with Devices

- [About Chassis View on page 1335](#)
- [Accessing the Chassis View from the Physical Inventory Page on page 1337](#)
- [Viewing a Graphical Image of the Chassis and Components on page 1338](#)
- [Deleting Devices from Chassis View on page 1345](#)
- [Rebooting Devices After Examining the Status in Chassis View on page 1346](#)

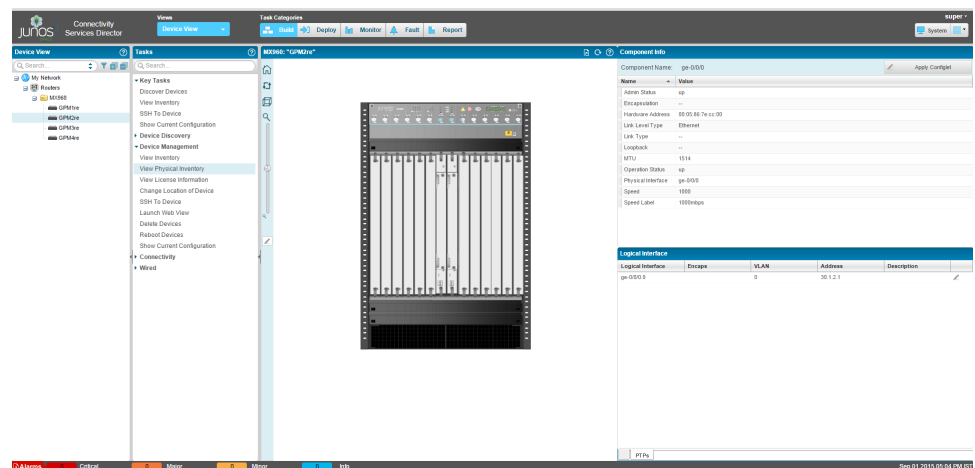
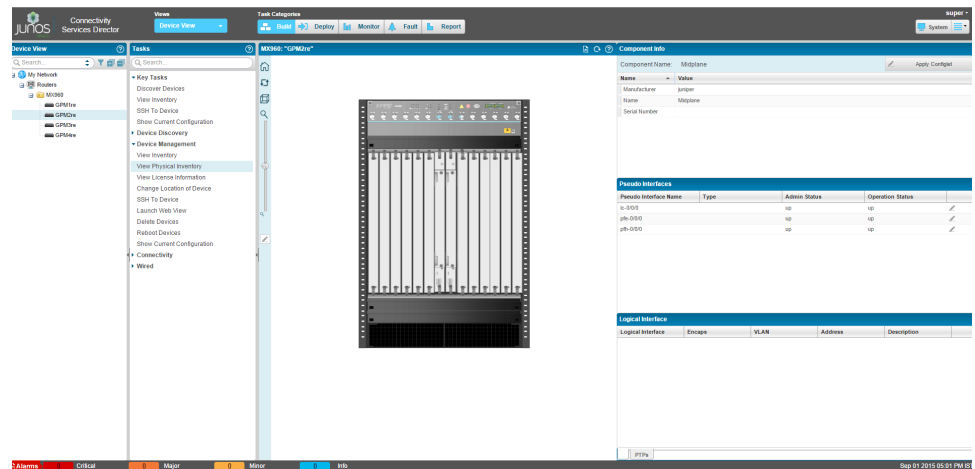
About Chassis View

You can view a high-level, graphical representation of the chassis. It indicates the state of the interfaces. When the administrative and operational status of the interface is up, it is displayed in green. If the administrative status is down, the interface is displayed in grey. And, if the administrative status is up and operational status is down, the interface is displayed in red. The image is a replica of the device. If you are connected to a virtual chassis, the image includes all the member switches of the virtual chassis. The chassis view also displays a count of alarms generated in the system; major alarms are displayed in red, and minor alarms in orange.

The purpose of the view is to try and provide a comprehensive monitoring view of the health and status of deployed devices across the network. In this view all the managed devices are shown with their appropriate status and health based on the services and device settings applied. This view helps the operator to know the health and status across the network, it provides with the operator to quickly see the macro level information, which allows the operator to further analyze the information provided and quickly navigate to individual devices and take any further corrective measure required. It provides a cohesive tool for the operator to quickly see the micro-level information and take any further remediation action required.

To view a pictorial representation of a device chassis and the configured components, such as interfaces, line cards, and hardware elements, select a managed device listed in the My Network tree in Device View of Build mode of the Connectivity Services Director GUI, and select **Device Management > View Physical Inventory** from the tasks pane. The right pane displays the device image and the corresponding description of the view selected in a tabular manner. The chassis view is displayed. The hardware and line module details are displayed with a pictorial view of the slots of the devices and the modules installed in these slots. The device image can be rotated to view the front, rear, top, bottom, right and left planes of the device by clicking the respective arrow buttons on

the page. The View Front icon and the View Back icon are denoted by a square icon with downward and upward arrows in the square. The View Front and View Back icons are toggle buttons. The device image can be rotated in various orientation along 360 degree. You can use the navigation options for rotating devices to view different planes on the device and the components installed on each plane. The front view displays the components installed and the interfaces configured on the device. Click Refresh to update the contents of the page and be displayed.



Related Documentation

- [Deleting Devices from Chassis View on page 1345](#)
- [Rebooting Devices After Examining the Status in Chassis View on page 1346](#)
- [Accessing the Chassis View from the Physical Inventory Page on page 1337](#)

Accessing the Chassis View from the Physical Inventory Page

The Dashboard page is the landing page that is displayed when you login to the Connectivity Services Director application. You can view all the available devices that are managed by Connectivity Services Director from the Device Inventory page. The Device Inventory page is accessible in Device View of Build mode as the default landing page. Alternatively, select **View Inventory** in the task pane to open the Device Inventory page. Based on your selection of routers, the Device Inventory page displays device details.

The Device Inventory page varies based on your selection in the View pane. When you select a node in the View pane, the inventory of all devices that are included under that node is displayed.

For example:

- Device View and My Network is selected: Displays all the devices that are managed by Connectivity Services Director.

You can view the physical inventory of all the devices in your network in the Device Physical Inventory page. The Device Physical Inventory page displays information about the slots that are available for a device and provides information about power supplies, chassis cards, fans, part numbers, and so on. Connectivity Services Director displays hardware inventory by device name, based on data retrieved both from the device during discovery and resynchronizing operations, and from the data stored in the hardware catalog. For each managed device, the physical inventory page provides descriptions for field replaceable units (FRUs), part numbers, model numbers, and the pluggable locations from which empty slots are determined.

To view a pictorial representation of a device chassis and the configured components, such as interfaces, line cards, and hardware elements, select a managed device listed in the My Network tree in Device View of Build mode of the Connectivity Services Director GUI, and select **Device Management > View Physical Inventory** from the tasks pane.

The following are the different device types in the device families that are supported in Chassis view:

- MX Series routers—MX5, MX10, MX40, MX240, MX480, MX960, MX2010, MX2020, MX80, MX80-P, MX80-T, MX80-48-T
- ACX Series routers—ACX1000, ACX1100, ACX2000, ACX2100, ACX2200, ACX4000, ACX500-DC, ACX500-O, ACX500-O-POE, ACX5048, ACX5096
- PTX Series routers—PTX3000, PTX5000, PTX1000

Related Documentation

- [Deleting Devices from Chassis View on page 1345](#)
- [Rebooting Devices After Examining the Status in Chassis View on page 1346](#)
- [About Chassis View on page 1335](#)
- [Service Monitoring Capabilities in Connectivity Services Director on page 1192](#)

Viewing a Graphical Image of the Chassis and Components

The Chassis view provides a pictorial representation of the chassis or device, and the modules or components that are installed in it, such as the line cards, interfaces, and other hardware elements

To view a graphical image of the chassis and its associated components:

1. From the View selector, select **Device View**. The functionalities that you can configure in this view are displayed.
2. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and view the list of devices. Select the device for which you want to define the optical port settings.
3. From the Tasks pane, select **Device Management > View Physical Inventory**. A graphical view of the device is displayed on the right pane.
4. Click a particular module to display the associated details in the lower half of the page. The Rotate and Perspective buttons enable you to view the images in required orientation.
5. Click the Rotate (arrows in a square symbol) icon to cause the device image to continuously rotate along the x-axis.
6. Click the Perspective (cube symbol) icon to display the device image in three-dimensional format. It is a toggle button, which causes the device image to be shown in either three-dimensional or one-dimensional format.
7. Select the level of magnification of the image by clicking the Zoom (magnifying glass) icon. The image is expanded and displayed. Alternatively, use the slider control beneath the Zoom icon to change the level of magnification.
8. Click the home icon to return to the front view of the chassis. The selected interface is surrounded with a colored outline based on the operational status as suggested below. An interface that is operationally up is denoted in green and an interface that is operationally down is represented in red. The components are depicted as small colored icons at the top left corner of the front-view equipment image.

In the graphical image of the device displayed, you can mouse over the different parts of the device, such as the interfaces, line cards, and slots. When you mouse over the different modules, their corresponding details are displayed as tooltips. On clicking the device components, the corresponding description for the selected component is displayed by default under the Component Info pane and the Equipment tab with the following values.

- **Manufacturer**—Name of the company that built and shipped the device.
- **Part number**—Part number of the chassis component.
- **Serial number**—Serial number of the chassis component. The serial number of the backplane is also the serial number of the router or switch chassis. Use this serial number when you need to contact Juniper Networks Customer Support about the router or switch chassis.

When you select any physical interface configured on the DPCs or PICs or MICs provisioned, the following fields are displayed for the corresponding component for each interface. The interface is surrounded by a colored box to show the Operational Status.

The Component Info pane and the Active Alarms monitor are displayed in the lower half of the page.

The Active Alarms monitor shows any active alarm that has not yet been cleared. You can view the alarm name, the unique identifier assigned to the alarm, the person to which the alarm is assigned for corrective action, and the severity of the alarm. Click the **Launch Alarm Mgmt** icon (right upward-slanting arrow enclosed in a square) to navigate to the Fault mode and view the four standard alarm monitors available in Fault mode.

Active Alarms for the respective components are displayed when the component is clicked in the graphical image of the chassis displayed. The components for which the alarms are displayed are Flexible Port Concentrator (FPC), Dense Port Concentrator (DPC), Physical Interface Card (PIC), Modular Interface Card (MIC), Routing Engine, Control Boards, fan trays, Switch Interface Board (SIB), and power supply module (PSM).

The following fields are displayed in the Active Alarms pane:

Table 186: Active Alarms Monitor

Table Column	Description
Severity	<p>The severity of the alarm. Severity levels are:</p> <ul style="list-style-type: none"> • Critical—A critical condition exists; immediate action is necessary. • Major—A major error has occurred; escalate or notify as necessary. • Minor—A minor error has occurred; notify or monitor the condition. • Info—An informational message; no action is necessary.
Name	The alarm name.
Source	The IP address of the device or network element that generated the alarm. The SNMP agent is located at the source IP. In most cases, the source IP is the IP address of the switch or controller.
Last Updated	The date and time that the information for the alarm was last modified.

The following fields are displayed in the Component Info pane:

Table 187: Fields for Physical Interfaces in the Component Info Pane

Field	Description
Host Name	Hostname of the device.
Physical Interface Name	Name of the physical interface.
IP Address	IP address configured on the interface.
Encapsulation	Encapsulation configured on the logical interface.
Hardware Address	MAC address configured on the interface
Operation Status	Operational status of the physical interface: Up, Down.
Admin Status	Administrative state of the interface: Enabled or Disabled. If the interface is disabled, it can provide network connectivity, but it cannot provide power to connected devices.
Link Level Type	Encapsulation type configured on the interface.
Link Type	Data transmission type.
Speed	Speed at which the interface is running.
MTU	Maximum transmission unit size on the physical interface.
Loopback	Specifies whether the loopback status is enabled or disabled. If loopback is enabled, type of loopback: Local or Remote.
Description	Configured textual description of the interface.

A redundant Ethernet interface is a pseudointerface that includes at minimum one physical interface from each node of the cluster. A redundant Ethernet interface must contain, at minimum, a pair of Fast Ethernet interfaces or a pair of Gigabit Ethernet interfaces that are referred to as child interfaces of the redundant Ethernet interface (the redundant parent). If two or more child interfaces from each node are assigned to the redundant Ethernet interface, a redundant Ethernet interface link aggregation group must be formed.

A pseudowire subscriber logical interface terminates an MPLS pseudowire tunnel from an access node to the MX Series router that hosts subscriber management, and enables you to perform subscriber management services at the interface. Subscriber management supports the creation of subscriber interfaces over point-to-point MPLS pseudowires. The pseudowire subscriber interface capability enables service providers to extend an MPLS domain from the access-aggregation network to the service edge, where subscriber management is performed. Service providers can take advantage of MPLS capabilities such as failover, rerouting, and uniform MPLS label provisioning, while using a single pseudowire to service a large number of DHCP and PPPoE subscribers in the service network.



NOTE: The pseudowire is a tunnel that is either an MPLS-based Layer 2 VPN or Layer 2 circuit. The pseudowire tunnel transports Ethernet encapsulated traffic from an access node (for example, a DSLAM or other aggregation device) to the MX Series router that hosts the subscriber management services. The termination of the pseudowire tunnel on the MX Series router is similar to a physical Ethernet termination, and is the point at which subscriber management functions are performed. A service provider can configure multiple pseudowires on a per-DSLAM basis and then provision support for a large number of subscribers on a specific pseudowire. Figure 1 shows an MPLS network that provides subscriber management support.

The following table describes the fields displayed in the Pseudo Interfaces pane.

Table 188: Pseudo Interfaces Columns

Field	Description
Pseudo Interface Name	Name of the pseudowire subscriber logical interface.
Type	Signaling type for the pseudowire interface. You can use either Layer 2 circuit signaling or Layer 2 VPN signaling. The two signaling types are mutually exclusive for a given pseudowire.
Operation Status	Operational status of the physical interface: Up, Down.
Admin Status	Administrative state of the interface: Enabled or Disabled. If the interface is disabled, it can provide network connectivity, but it cannot provide power to connected devices.

The logical interfaces configured on each interface are also shown along with the physical interface description in a tabular format. The following table describes the details displayed for logical interfaces.

Table 189: Logical Interfaces Columns

Field	Description
Device Name	The device configuration name.
Interface Name	Standard information about the interface, in the format type-/fpc/pic/port/logical interface, where type is the media type that identifies the network device; for example, ge-0/0/6.135.
IP Address	The IP address for the logical interface.
Encapsulation	The encapsulation type used on the logical interface.
Vlan	The VLAN ID for the logical interface.

Table 189: Logical Interfaces Columns (continued)

Field	Description
Description	An optional description configured for the interface. It can be any text string of 512 or fewer characters. Any longer string is truncated. If there is no information, the column entry is blank.

From the chassis view window, click the **Details** icon (arrow enclosed in a square) at the top-right corner of the window to open the Chassis View Details page that lists the configured devices and their parameters in the form of a table.

The following fields are displayed on the right pane, depending on the component or element of the chassis you selected from the chassis image displayed.

Table 190: Fields in the Chassis View Details Page

Field	Description
Module	Name of the SDG and the platform type, such as MX240 or MX480. Click the plus sign (+) to expand the tree to display the components of the device, such as chassis, PIC, CPU, and PIC parameters. Information about the chassis, midplane, craft interface (FPM), power midplane (PMP), Power Supply Modules (PSMs), Power Distribution Modules (PDMs), Routing Engines, Control Boards (CBs) and Switch Processor Mezzanine Boards (SPMBs), Switch Fabric Boards (SFBs), Flexible PIC Concentrators (FPCs), PICs, adapter cards (ADCs) and fan trays is displayed.
Model Number	Model number of the FRU hardware component.
Model	Model of the FRU component.
Part Number	Part number of the chassis component.
Serial Number	Serial number of the chassis component. The serial number of the backplane is also the serial number of the router chassis. Use this serial number when you need to contact Juniper Networks Customer Support about the router or switch chassis.

Table 190: Fields in the Chassis View Details Page (continued)

Field	Description
Description	

Table 190: Fields in the Chassis View Details Page (continued)

Field	Description
	<p>Brief description of the hardware item:</p> <ul style="list-style-type: none"> Type of power supply. Type of PIC. If the PIC type is not supported on the current software release, the output states Hardware Not Supported. Type of FPC: FPC Type 1, FPC Type 2, FPC Type 3, FPC Type 4, or FPC Type OC192. On EX Series switches, a brief description of the FPC. On the J Series routers, the FPC type corresponds to the Physical Interface Module (PIM). The following list shows the PIM abbreviation in the output and the corresponding PIM name. <ul style="list-style-type: none"> 2x FE—Either two built-in Fast Ethernet interfaces (fixed PIM) or dual-port Fast Ethernet PIM 4x FE—4-port Fast Ethernet ePIM 1x GE Copper—Copper Gigabit Ethernet ePIM (one 10-Mbps, 100-Mbps, or 1000-Mbps port) 1x GE SFP—SFP Gigabit Ethernet ePIM (one fiber port) 4x GE Base PIC—Four built-in Gigabit Ethernet ports on a J4350 or J6350 chassis (fixed PIM) 2x Serial—Dual-port serial PIM 2x T1—Dual-port T1 PIM 2x E1—Dual-port E1 PIM 2x CTIE1—Dual-port channelized T1/E1 PIM 1x T3—T3 PIM (one port) 1x E3—E3 PIM (one port) 4x BRI S/T—4-port ISDN BRI S/T PIM 4x BRI U—4-port ISDN BRI U PIM 1x ADSL Annex A—ADSL 2/2+ Annex A PIM (one port, for POTS) 1x ADSL Annex B—ADSL 2/2+ Annex B PIM (one port, for ISDN) 2x SHDSL (ATM)—G SHDSL PIM (2-port two-wire module or 1-port four-wire module) 1x TGM550—TGM550 Telephony Gateway Module (Avaya VoIP gateway module with one console port, two analog LINE ports, and two analog TRUNK ports) 1x DS1 TIM510—TIM510 E1/T1 Telephony Interface Module (Avaya VoIP media module with one E1 or T1 trunk termination port and ISDN PRI backup) 4x FXS, 4x FXO, TIM514—TIM514 Analog Telephony Interface Module (Avaya VoIP media module with four analog LINE ports and four analog TRUNK ports) 4x BRI TIM521—TIM521 BRI Telephony Interface Module (Avaya VoIP media module with four ISDN BRI ports) Crypto Accelerator Module—For enhanced performance of cryptographic algorithms used in IP Security (IPsec) services MPC M 16x 10GE—16-port 10-Gigabit Module Port Concentrator that supports SFP+ optical transceivers. (Not on EX Series switches.) For hosts, the Routing Engine type. For small form-factor pluggable transceiver (SFP) modules, the type of fiber: LX, SX, LH, or T. LCD description for EX Series switches (except EX2200 switches).

Table 190: Fields in the Chassis View Details Page (continued)

Field	Description
	<ul style="list-style-type: none"> • MPC2—1-port MPC2 that supports two separate slots for MICs. • MPC3E—1-port MPC3E that supports two separate slots for MICs (MIC-3D-1X100GE-CFP and MIC-3D-20GE-SFP) on MX960, MX480, and MX240 routers. The MPC3E maps one MIC to one PIC (1 MIC, 1 PIC), which differs from the mapping of legacy MPCs. • 100GBASE-LR4, pluggable CFP optics • Supports the Enhanced MX Switch Control Board with fabric redundancy and existing SCBs without fabric redundancy. • Interoperates with existing MX Series line cards, including Flexible Port Concentrators (FPC), Dense Port Concentrators (DPCs), and Modular Port Concentrators (MPCs). • MPC4E—Fixed configuration MPC4E that is available in two flavors: MPC4E-3D-32XGE-SFP and MPC4E-3D-2CGE-8XGE on MX2020, MX960, MX480, and MX240 routers. • LCD description for MX Series routers

Related Documentation

- [Deleting Devices from Chassis View on page 1345](#)
- [Rebooting Devices After Examining the Status in Chassis View on page 1346](#)
- [About Chassis View on page 1335](#)

Deleting Devices from Chassis View

You can delete devices that are no longer used from Connectivity Services Director and for which you do not want to view a pictorial representation using the Chassis View functionality. Deleting a device removes all device configuration and device inventory information from the Junos Space database. Once a device is deleted from the database, all the profiles associations, device configurations, and inventory information of the deleted device are also deleted. However, the system maintains the audit logs and monitoring data for the device even after the device is deleted.

Use the Delete Devices page to delete devices from Connectivity Services Director. While in Build mode, click Delete Devices from the Tasks > Device Management menu. The Delete Devices page appears.

The Delete Devices page displays the devices contextually depending on your selection in the View pane. For example, if you select a site in Service View and click Delete Devices, Connectivity Services Director displays all the devices. If you select a particular switch family in Device View and click Delete Devices, only devices that belong to that switch family are displayed.

To delete devices, complete the following tasks:

1. From the View selector, select Service View. The functionalities that you can configure in this view are displayed.
2. Click the Build mode icon in the Service View of the Connectivity Services Director banner. The workspaces that are applicable to this mode are displayed.

Select the My Network scope in the View pane that contains the devices you want to delete.
3. Select Delete Devices from the Tasks pane.
4. Select the check box adjacent to the device that you want to delete. Click Done.
5. Connectivity Services Director prompts you to confirm the deletion. Click Yes to confirm the deletion or No to go back and make changes to the selection.

**Related
Documentation**

- [Rebooting Devices After Examining the Status in Chassis View on page 1346](#)
- [About Chassis View on page 1335](#)
- [Service Monitoring Capabilities in Connectivity Services Director on page 1192](#)

Rebooting Devices After Examining the Status in Chassis View

In certain situations, when you identify a certain discrepancy or malfunctioning of a component, such as a line card or an interface, by examining the status of the hardware module using the Chassis View, you might require the component to be rebooted. When a hard disk error occurs, a Routing Engine might enter a state in which it responds to local pings and interfaces remain up, but no other processes are responding. To recover from this situation, you can reboot a single Routing Engine when a hard disk error occurs. Similarly, you can restart the FPCs when a traffic black-hole condition is detected.

Use the Reboot Devices task to immediately reboot the selected device. This task is available in all scopes when in Build mode. To reboot one or more devices immediately:

1. For the My Network scope, you can customize what monitors appear on Summary tab, giving you the ability to view at a glance those aspects of network health and performance that are most important to you.
2. Click the Build mode icon in the Service View of the Connectivity Services Director banner. The workspaces that are applicable to this mode are displayed.
3. Select the My Network scope in the View pane that contains the devices you want to reboot.

4. Select Reboot Devices from the Tasks pane.
5. Expand the tree on the page as needed to locate the available devices.
6. Select the check box for one or more devices.
7. Click Done to start the reboot or click Cancel to return to the Device Inventory page.
The rebooting process triggers a Cold Start Alarm that can be seen in Fault mode.

**Related
Documentation**

- [Deleting Devices from Chassis View on page 1345](#)
- [Accessing the Chassis View from the Physical Inventory Page on page 1337](#)
- [About Chassis View on page 1335](#)
- [Service Monitoring Capabilities in Connectivity Services Director on page 1192](#)

CHAPTER 50

Managing CLI Configlets

- [CLI Configlets Overview on page 1349](#)
- [CLI Configlets Workflow on page 1352](#)
- [Configlet Context on page 1355](#)
- [Creating a CLI Configlet on page 1360](#)
- [Modifying a CLI Configlet on page 1363](#)
- [Deleting CLI Configlets on page 1363](#)
- [Viewing CLI Configlets on page 1364](#)
- [Creating a Parameter for a CLI Configlet on page 1366](#)
- [Applying a CLI Configlet to Devices on page 1368](#)
- [Deploying CLI Configlet Details on page 1372](#)

CLI Configlets Overview

CLI Configlets are configuration tools provided by Junos OS that enables you to apply a configuration to a device by reducing configuration complexity. CLI Configlets contain the Junos OS configuration as a formatted ASCII text. Junos Space uses the NETCONF protocol to load and commit the configuration on devices.

A CLI Configlet is a configuration template that is transformed into a CLI configuration string before being applied to a device. The dynamic elements (strings) in configuration templates are defined using template variables. These variables act as an input to the process of transformation to construct the CLI configuration string. These variables can contain the interface name, device name, description text, or any such dynamic values. The value of these variables are obtained from the user or the system or given by the context at the time of execution. Velocity templates (VTL) are used to define CLI Configlets.

You can access the CLI Configlets workspace by selecting CLI Configlets from the left pane. From the CLI Configlets workspace, you can perform the following tasks:

- Viewing the statistics of CLI Configlets in Junos Space Network Management Platform
- Creating, modifying, cloning, applying, or deleting a CLI Configlet
- Marking and unmarking CLI Configlets as favorites

You can also apply CLI Configlets to devices from the Devices workspace. It can be triggered from the actual elements for which the configuration has to be applied. The context of the element for which the CLI Configlet is being applied is called an execution context.



NOTE: CLI Configlets are not supported on SSG Series devices, NetScreen Series devices, TCA Series devices, BXOS Series devices, and Junos Content Encore devices.

- [Configlet Variables on page 1350](#)
- [Velocity Templates on page 1350](#)
- [Directives on page 1351](#)

Configlet Variables

Variables in CLI Configlets include a leading “\$”. CLI Configlets use three kinds of variables: default, user-defined, and predefined.

Default Variables

The value of these variables need not be input by the user; these values are derived from the current execution context. [Table 191 on page 1350](#) lists the default variables.

Table 191: Default Variables

Variable	Value
\$DEVICE	Name of the host on which the CLI Configlet is applied
\$INTERFACE	Name of the interface for which the CLI Configlet is applied
\$UNIT	Unit number of the logical interface for which the CLI Configlet is being applied
\$CONTEXT	Context of the element for which the CLI Configlet is applied

User-defined Variables

The values for these variables are entered by the user at execution time. Text fields or selection fields are used to obtain data from the user.

Predefined Variables

These are the variables for which the values are predefined when you create the CLI Configlet. These variables are also called invisible parameters because they cannot be modified by the user.

Velocity Templates

Junos Space Network Management Platform enables you to define the device configuration in the form of velocity templates (VTL). These templates are called CLI Configlets. The VTL variable is a reference type, which includes the leading “\$” character,

followed by a VTL Identifier. CLI Configlets are transformed into a CLI configuration string before they are applied to the device. This transformation is directed by references and directives of VTL.

References are used to embed dynamic contents in the configuration text. Directives allow dynamic manipulation of the contents.

Refer to <http://velocity.apache.org/engine/releases/velocity-1.4/user-guide.html> for detailed information about VTL.

Directives

Directives include an included CLI Configlet's contents and parameters in the base CLI Configlet and import the metadata information related to the parameters of the included CLI Configlet. You can include CLI Configlets in Junos Space Platform by using two directives: `#include_configlet` and `#mixin` directives.

#include_configlet – This directive includes an included CLI Configlet's contents and parameters in the base CLI Configlet and imports the metadata information related to the parameters of the included CLI Configlet. If you define a new parameter in the base CLI Configlet by using the `#include_configlet` directive, the metadata information is fetched and used from the included CLI Configlets. The parameter values updated in the included CLI Configlet after their inclusion into the base CLI Configlet are not updated and available for the base CLI Configlet. If both the base CLI Configlet and included CLI Configlet contain parameters with a common name, the metadata information related to the parameters is ignored.

#mixin – This directive differentiates the parameters of the base CLI Configlet from the parameters of the included CLI Configlet on the Junos Space user interface. The parameter values for the included CLI Configlets can be modified even when you apply the CLI Configlet to the device. You cannot include CLI Configlets that have a period (.) or space in its name.

You include these directives in the base CLI Configlet in the following format:

- `#include_configlet("<name of the included configlet>")`
- `#mixin("<name of the included configlet>")`

Related Documentation

- [CLI Configlets Workflow on page 1352](#)
- [Configlet Context on page 1355](#)
- [Creating a CLI Configlet on page 1360](#)
- [Modifying a CLI Configlet on page 1363](#)
- [Deleting CLI Configlets on page 1363](#)
- [Viewing CLI Configlets on page 1364](#)
- [Creating a Parameter for a CLI Configlet on page 1366](#)
- [Applying a CLI Configlet to Devices on page 1368](#)

CLI Configlets Workflow

A CLI Configlet can be defined from the CLI Configlets workspace. [Table 192 on page 1352](#) lists the parameters to be defined for a CLI Configlet.

Table 192: Parameters for a CLI Configlet

Parameter	Description
Name	Name of the CLI Configlet. The name cannot exceed 255 characters. Allowable characters include the hyphen (-), underscore (_), letters, and numbers and the period (.). You cannot have two configlets with the same name.
Category	Category of the CLI Configlet. The category cannot exceed 255 characters. Allowable characters include the hyphen (-), underscore (_), letters, and numbers and the period (.).
Device Family Series	Device family series for which the CLI Configlet is applicable.
Context	Context for which the CLI Configlet is applicable. This is an optional field.
Description	Description of the CLI Configlet. The description cannot exceed 2500 characters. This is an optional field.
Preview options	Selecting the Show Parameters option displays the parameters that are present in the CLI Configlet. The Show Configuration option displays the consolidated configuration before the CLI Configlet is applied.
Post-view options	Selecting the Show Parameters option displays the parameters that are present in the CLI Configlet. The Show Configuration option displays the consolidated configuration after the CLI Configlet is applied.
Configlet Content	The actual CLI Configlet is defined here. The CLI Configlet can contain multiple pages and follows a tablike structure. The configuration being applied onto the device can be split among multiple pages. When the configuration is applied, all the pages are combined in order of the page numbers and applied onto the device in a single commit operation. You must always validate the CLI Configlet before moving to the next page.
Reference Number	The range of values are from 1 to 2 ¹⁶ .



NOTE: You cannot move to the next page if the contents of the CLI Configlet are invalid. Validation includes bracket matching.

Parameters are variables defined in the CLI Configlet whose values are either retrieved from the environment or entered by the user during execution. When the user applies CLI Configlets, the user is asked to input values for all variables defined in the CLI Configlet.

To configure a parameter, click the modify icon on the toolbar. The Edit Configlet Parameter page is displayed. Use this page to set the attributes of a parameter.

To add an additional parameter, click the add icon on the toolbar. The Add Configlet Parameter page is displayed. The attributes of a parameter are set from this page.

To delete a parameter, click the delete icon on the toolbar. By default, all variables present in the CLI Configlet are listed on the Parameters page. Local variables must be deleted manually or set to the “Invisible” type.

Table 193 on page 1353 lists the attributes of the CLI Configlet parameters.

Table 193: Attributes of CLI Configlet Parameters

CLI Configlet Parameter Attributes	Description
Parameter	<p>Name of the parameter</p> <p>If displayed with a name space in the <code><configlet name>.<parameter.name></code> format, this parameter belongs to the included CLI Configlet.</p>
Display Name	Display name of the parameter
Description	Description of the parameter
Types	<p>The types of parameters supported are:</p> <ul style="list-style-type: none"> • Text field – You can provide a custom value when executing the CLI Configlet. The default value for this field can be configured with an XPath in the Configured Value Xpath field or with a plain string in the Default Value field. This returns a single value. • Selection field – You can select a value from a set of options when executing this CLI Configlet. The default value for this field can be configured with an XPath in the Configured Value Xpath field or with a plain string in the Default Value field. The options can be configured by an XPath in the Selection Values Xpath field, or by using a CSV string in the Selection Values field. This returns a single value. <p>NOTE: Though this returns a single value, the return value is of the array type and the selected value can be taken from index 0.</p> <ul style="list-style-type: none"> • Invisible field – You cannot edit this field. This parameter refers to values defined explicitly as a CSV string in the Default Value field or by an XPath in the Configured Value Xpath field. This field returns an array of values. • Password field – You need to enter a value when you apply a CLI Configlet containing the parameter. This hides sensitive information in the Apply CLI Configlet job results. • Password Confirm field – You need to enter a value twice when you apply a CLI Configlet containing the parameter. This hides sensitive information in the Apply CLI Configlet job results.

Table 193: Attributes of CLI Configlet Parameters (continued)

CLI Configlet Parameter Attributes	Description
Configured Value XPath	<p>This field is used to give the XPath of the configured values. The behavior of this field depends on the type of parameter. When the parameter type is a text field or selection field, the corresponding value present in the XPath is taken as the default value. This value can be modified. If the XPath returns multiple values, the first value returned is considered. When the parameter type is an invisible field, the list of values returned by the XPath is taken as the value of the parameter.</p> <p>Invisible field has configured value XPath and selection value XPath only when the parameter scope is either device specific or entity specific. This is disabled if the scope is global.</p> <p>NOTE: When using \$INTERFACE, \$UNIT, Configured Value Xpath field, Invisible field, and Selection field, the variable definition in the Configlet Editor should contain <code>.get(0)</code> in order to fetch the value from the array. For example, <code>\$INTERFACE.get(0)</code>.</p>
Default Value	Displays the same behavior as the Configured Value Xpath field except that the value is given explicitly. This field is considered only when configured value XPath is not specified or if the XPath does not return any value.
Selection Values XPath	This field is enabled only if the parameter type is a Selection field. This field contains the XPath (with reference to the device XML) to fetch the set of values for the Selection field.
Selection Values	<p>This field is the same as the Selection Values XPath field except that the value is given explicitly. This field is considered only when selection values XPath is not specified or if the XPath does not return any value.</p> <p>NOTE: Comma-separated values can be used to provide an array of values in the Default Value and Selection Values fields.</p> <p>NOTE: While defining the XPath, you must directly access the text node with the <code>text ()</code> function. Otherwise the complete XML path of the node is returned. For example, <code>/device/interface-information/physical-interface/name/text()</code> to fetch the names of all interfaces.</p>
Order	Order of the parameter. This is the relative order in which the field must be displayed for user input at the time of execution.
Regex Value	This field contains regular expression for the parameter that is used to validate the parameter value while you apply the CLI Configlet to the device.
Read-only	<p>Whether the parameter belongs to the base configlet or the included configlet:</p> <ul style="list-style-type: none"> false – This parameter belongs to the base configlet. true – This parameter belongs to the included configlet. The parameter cannot be modified or deleted from this configlet.

- Related Documentation**
- [CLI Configlets Overview on page 1349](#)
 - [CLI Configlets Workflow on page 1352](#)
 - [Configlet Context on page 1355](#)
 - [Creating a CLI Configlet on page 1360](#)
 - [Modifying a CLI Configlet on page 1363](#)
 - [Deleting CLI Configlets on page 1363](#)
 - [Viewing CLI Configlets on page 1364](#)
 - [Creating a Parameter for a CLI Configlet on page 1366](#)
 - [Applying a CLI Configlet to Devices on page 1368](#)

Configlet Context

Execution of scripts and CLI configlets may be required in some case. For example, one might need to restrict the scope of execution of 'disable interface' script to just the interfaces that are enabled. Having a context associated to the script or configlet solves this problem of restricting the scope. Context of an element is basically a unique path which leads to its XML counterpart in the device XML.

For all context related computations, we consolidate the XMLs fetched from the device under one node called device. This includes configuration XML, interface-information XML, chassis-inventory XML, and system-information XML.

An example of a device XML is as follows:

```
<device>
  <interface-information>....</interface-information>
  <system-information>....</system-information>
  <chassis-inventory>....</chassis-inventory>
  <configuration>....</configuration>
  ....
</device>
```

[Table 194 on page 1355](#) shows the commands to view the XML from the CLI of the device.

Table 194: Commands to View XML from the CLI

XML type	Command
Chassis Inventory	> show chassis hardware display xml
Interface Information	> show interfaces display xml
Configuration	> show configuration display xml
System Information	-



NOTE: The command for system information XML is not available. An instance of the system information XML is as follows:

```
<system-information>
<hardware-model>ex4200-24t</hardware-model>
<os-name>junos-ex</os-name>
<os-version>11.3R2.4</os-version>
<serial-number>BM0210293858</serial-number>
<host-name>EX4200-200</host-name>
<virtual-chassis/>
</system-information>
```

Context of an Element

There is a need to have the ability to restrict a script or configlet execution to certain elements of interest. For example, one might need to restrict the scope of execution of 'disable interface' script only to the interfaces that are enabled. Having a context associated with the script or configlet solves this scoping problem.

The context of an element is the XPath that maps to the XML node that represents the element in the device XML. [Table 195 on page 1356](#) lists the type of element, XML referred, and the content path.

Table 195: Context Path and XML node referred for different element types

Element Type	XML Referred	Context Path
Device	N/A	/device
Physical Inventory element	Chassis Inventory	/device/chassis-inventory/*
Physical Interface	Interface Information	/device/interface-information/*
Logical Interface	Configuration	/device/configuration/*

[Table 196 on page 1356](#) lists some examples for XPaths for different elements.

Table 196: XPaths for different elements

Element	Context	Description
Device	/device	The context of a device
Chassis	/device/chassis-inventory/chassis[name='Chassis']	Context of a chassis
Routing Engine	/device/chassis-inventory/chassis[name='Chassis']/chassis-module[name='Routing Engine 0']	The context of a routing engine
FPC	/device/chassis-inventory/chassis[name='Chassis']/chassis-module[name='FPC 1']	The context of an FPC in slot 1

Table 196: XPathS for different elements (continued)

Element	Context	Description
PIC	/device/chassis-inventory/chassis[name='Chassis']/chassis-module[name='FPC 1']/chassis-sub-module[name='PIC 4']	The context of a PIC in slot 4 under FPC in slot 1
Logical Interfaces	device/configuration/interfaces/interface[name='ge-0/0/1']/unit[name='0']	The context of logical interface ge-0/0/1.0
Physical Interfaces	/device/interface-information/physical-interface[name='ge-0/1/1']	The context of a physical interface ge-0/1/1

Context filtering

The context attribute of the script or configlet dictates which elements (inventory component or logical interface or physical interface) it is applicable to.

The rule to check whether the script or configlet is applicable to an element is as follows:

- Evaluate the context XPath associated to a script or configlet on the device XML. This results in a set of XML nodes.
- If the resultant XML node list contains the XML node representing the subject element, then the script/template entity is considered a match.

Given below are few examples of script or configlet contexts with their descriptions:

- /device/chassis-inventory/chassis[name='Chassis']/chassis-module[starts-with(name,'Routing Engine')] - Applicable to all routing engines
- /device/chassis-inventory/chassis[name='Chassis']/chassis-module[starts-with(name,'FPC')] - Applicable to all FPCs
- /device[starts-with(system-information/os-version,'11')]/interface-information/physical-interface[starts-with(name,'ge')] - Applicable to all interfaces of type 'ge' which has system os-version as 11
- /device/interface-information/physical-interface[admin-status="up"] - Applicable to all physical interfaces with admin status in up state.
- /device/chassis-inventory/chassis[name='Chassis']/chassis-module[starts-with(name,'FPC')]/chassis-sub-module[starts-with(name,'PIC')] | /device/chassis-inventory/chassis[name='Chassis']/chassis-module[starts-with(name,'FPC')]/chassis-sub-module[starts-with(name,'PIC')] - Applicable to all PICs



NOTE: If we intend to specify the scope of a script as PICs, then we would have to consider two different XPathS the PIC can take (One with MIC in-between and one without). We have to give an OR combination of both the XPathS.



NOTE: If no context is associated to a script or configlet, then the context of the script is taken as “/device”. These scripts or configlets would be listed for execution in devices.

Physical Interface Example

Consider the following device XML

```
<device>
  <interface-information>
    <physical-interface>
      <name>ge-0/0/0</name>
      <admin-status>up</admin-status>
      ....
    </physical-interface>
    <physical-interface>
      <name>ge-0/0/1</name>
      <admin-status>down</admin-status>
      ....
    </physical-interface>
    .....
  </interface-information>
  ....
  <!-- ALL THE OTHER NODES -->
  ....
</device>
```

Context of an element

Context of physical-interface ge-0/0/0 is
/device/interface-information/physical-interface[name='ge-0/0/0']

This XPath maps to the node below. This is the XML counterpart of the interface ge-0/0/0

```
<physical-interface>
  <name>ge-0/0/0</name>
  <admin-status>up</admin-status>
  ....
</physical-interface>
```

Physical Interface in “up” state:

If the user wants to write a configlet to set the admin status of an interface down if its up, the context of the script can be set as
/device/interface-information/physical-interface[admin-status='up']

This configlet will be enabled only for interfaces with admin status up. Since in our example, ge-0/0/0 satisfies the above condition, this configlet can be executed on it.

To view the contexts for writing CLI configlet scripts for different service types, refer [Table 135 on page 1089](#).

Table 197: CLI Configlets Contexts for Different Service Types

Service Type	Context
P2P	@CONTEXT = "/device/configuration/protocols/l2circuit/neighbor/interface" Example : /device[name="MX80-NGCE-1"]/configuration/protocols/l2circuit/neighbor[name="30128"]/interface[name="ge-0/1/5784"]
L3VPN	/*@CONTEXT = "/device/configuration/routing-instances/instance/interface" */ Example : /device[name="kochin"]/configuration/routing-instances/instance[name="SO62441630" and instance-type="vrf"]/interface[name="ge-0/1/3.934"]
VPLS	/* @CONTEXT = "/device/configuration/routing-instances/instance/interface" */ Example : /device[name="kochin"]/configuration/routing-instances/instance[name="SO62441630" and instance-type="vpls"]/interface[name="ge-0/1/3.945"]
P2P or L3VPN with L2E	/* @CONTEXT = "/device/configuration/protocols/connections/interface-switch/interface" */ Example: /device[name="MX80-1"]/configuration/protocols/connections/interface-switch/interface[name="ge-1/0/0.1801"]
P2P (Local switching)	/* @CONTEXT = "/device/configuration/protocols/l2circuit/local-switching/interface/end-interface" */ Example /device[name="MX80-1"]/configuration/protocols/l2circuit/local-switching/interface[name="ge-1/0/0.1801"]/end-interface[name="ge-1/2/2881"]
NPS (Network peering)	/* @CONTEXT = "/device/configuration/protocols/bgp/group" */ Example /device[name="MX80-1"]/configuration/protocols/bgp/group[type="external"]

Related Documentation

- [CLI Configlets Workflow on page 1352](#)
- [Creating a CLI Configlet on page 1360](#)
- [Modifying a CLI Configlet on page 1363](#)
- [Deleting CLI Configlets on page 1363](#)
- [Viewing CLI Configlets on page 1364](#)
- [Creating a Parameter for a CLI Configlet on page 1366](#)
- [Applying a CLI Configlet to Devices on page 1368](#)

Creating a CLI Configlet

You create a CLI Configlet to push a configuration to devices. You can also add parameters to a CLI Configlet. Parameters are the variables defined in the CLI Configlet whose values are either obtained from the environment or given by the user during execution.

You must create Configlets and the parameters for a CLI Configlet using the Configlets workspace of the Junos Space Network Management Platform GUI, before you can apply the created Configlets to devices and deploy Configlets using the Connectivity Services Director GUI.

To create a CLI Configlet:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configlets**.

The Configlets page is displayed.

2. Click the Create CLI Configlet icon on the toolbar.

The Create CLI Configlet page is displayed.

3. In the **Name** field, enter a name for the CLI Configlet.

The name cannot exceed 255 characters. Allowable characters include the hyphen (-), underscore (_), letters, numbers, and the period (.). You cannot have two CLI Configlets with the same name.

4. In the **Category** field, enter a name for the category of the CLI Configlet.

The name of the category cannot exceed 255 characters. Allowable characters include the hyphen (-), underscore (_), letters, numbers, and the period (.).

5. From the **Device Family Series** drop-down list, select the device family for the CLI Configlet.

6. (Optional) From the **Context** drop-down list, select the appropriate context for the CLI Configlet.

7. In the **Reference Number** field, enter a reference number for the CLI Configlet.

The default value is 1. The maximum value is 2^{16} .

8. (Optional) In the **Description** field, enter a description.

The description cannot exceed 2500 characters.

9. For Execution Type, select the type of execution. The option buttons available are **Single Execution** and **Grouped Execution**.

By default, the **Single Execution** option button is selected.

- If you select **Single Execution**, you can apply the CLI Configlet only to one device at a time.
 - If you select **Grouped Execution**, you can apply the CLI Configlet to multiple devices at a time.
10. For Preview options, clear the check boxes if you do not want to view the parameters and the configuration in the CLI Configlet after downloading it.

The check boxes available are **Show Parameters** and **Show Configuration**. By default, both check boxes are selected.

11. For Postview options, clear the check boxes if you do not want to view the parameters and the configuration in the CLI Configlet before creating it.

The check boxes available are **Show Parameters** and **Show Configuration**. By default, both check boxes are selected.

12. In the Configlet Editor area, enter the configuration for the CLI Configlet. You can type or manually paste the configuration in the Configlet Editor.



NOTE: You cannot create a CLI Configlet if you do not enter the configuration in the Configlet Editor.



NOTE: You can also create a CLI Configlet to erase specific configuration from the devices. To do so, include the `delete:` statement above the hierarchy level that should be deleted from the devices. When you apply the CLI Configlet to a device, the physical interface of a device, the logical interface of a device, or the physical inventory element of a device, the configuration in the hierarchy level is erased on the device.

For more information about the protocol and syntax used for creating, modifying, and deleting the configuration by using CLI Configlets, see the [Junos XML Management Protocol Guide](#).



NOTE: When you define a configuration of the CLI Configlet, you should specify variables that accept special characters as input within double quotation marks.

13. Click **Next**.

You can add the parameters for the CLI Configlet on this page.

14. To add a parameter to the CLI Configlet:

- a. Click the Add Parameter icon.

The Add Configlet Parameter pop-up window is displayed.

- b. In the **Parameter** field, enter the name of the parameter.

The name of the parameter cannot exceed 255 characters. Allowable characters include the hyphen (-), underscore (_), letters, numbers, and the period (.).

- c. In the **Display Name** field, enter a display name for the parameter.

The display name cannot exceed 255 characters. Allowable characters include the hyphen (-), underscore (_), letters, numbers, and the period (.).

- d. In the **Description** field, enter a description for the parameter.

- e. From the **Parameter Scope** drop-down list, select an appropriate scope for the parameter.

The options available are Global, Device Specific, and Entity Specific.

- f. From the **Parameter Type** drop-down list, select an appropriate type of parameter. The options available are:

- Text Field – You can enter any value.
- Selection Field – You can select a value from a set of options.
- Invisible Field – The field displays a value that is explicitly defined by the user or an XPath.
- Password Field – Enter a password to apply the CLI Configlet.
- Password Confirm Field – Enter the password again to confirm the password.

- g. From the **Regex Value** drop-down list, select an appropriate regular expression value.

This field is enabled if you choose the type of parameter as Text Field, Password Field, or Confirm Password Field.

- h. From the **Configured Value Xpath** drop-down list, select an appropriate XPath value.

This field is enabled if you choose the type of parameter as Text Field, Selection Field, or Invisible Field. This is the XPath (with reference to the device XML) to fetch the set of values.

- i. In the **Default Value** field, enter a default value.

This field is enabled if you choose the type of parameter as Text Field, Selection Field, or Invisible Field. This field is considered only when the XPath is not specified.

- j. From the **Selection Values Xpath** drop-down list, select an appropriate XPath value.

This field is enabled if you choose the type of parameter as Selection Field. This is the XPath (with reference to the device XML) to fetch the set of values.

- k. In the **Selection Values** field, enter an appropriate selection value.

This field is enabled if you choose the type of parameter as Selection Field.

- l. In the **Order** field, enter the order in which the parameters should be listed while applying the CLI Configlet.
 - m. Click **Add**.
15. (Optional) Add multiple parameters.
16. (Optional) To go back to the previous page, click **Back**.

You are redirected to the previous page.
17. Click **Create**.

The CLI Configlet is created. You are redirected to the Configlets page.

Related Documentation

Modifying a CLI Configlet

You modify a CLI configlet when you want to change the properties of the CLI configlet.

To modify a CLI configlet:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configlets**.

The Configlets page is displayed.
2. Select the CLI configlet you want to modify and click the **Modify** button.

The Modify CLI configlet page is displayed.
3. Modify the CLI configlet properties and click **Update**.

The CLI configlet is modified.

Related Documentation

- *CLI Configlets Overview*
- *Creating a CLI Configlet*
- *Exporting CLI Configlets*
- *Importing CLI Configlets*

Deleting CLI Configlets

You delete CLI configlets when you no longer want to use them to apply configuration to devices.

You must create Configlets and the parameters for a CLI Configlet using the Configlets workspace of the Junos Space Network Management Platform GUI, before you can apply the created Configlets to devices and deploy Configlets using the Connectivity Services Director GUI.

To delete CLI configlets:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configlets**.

The Configlets page is displayed.

2. Select the CLI configlets you want to delete and select the Delete CLI Configlets icon from the Actions menu.

The Delete CLI Configlet pop-up window is displayed.

3. Click **Confirm**.

The CLI configlets are deleted.

Related Documentation

Viewing CLI Configlets

You create a CLI Configlet to push a configuration to devices. You can also add parameters to a CLI Configlet. Parameters are the variables defined in the CLI Configlet whose values are either obtained from the environment or given by the user during execution.

To view CLI Configlets:

1. From the View selector, select **Device View**. The workspaces that you can configure in this view are displayed.
2. Click the **Build** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed.
3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and view the list of devices.
4. Select the device for which you want to apply CLI configlets. A graphical view of the device is displayed on the right pane.
5. From the tasks pane, select **Configuration Deployment > View Applied Configlets**.

The Manage CLI-Applied Configlets page is displayed.

6. Select the device for which you want to view the applied CLI configlets. A graphical view of the device is displayed on the right pane.

The following fields are displayed on this page:

Table 198: Columns on the Manage CLI-Applied Configlets Page

Field	Description
Name	Name of the configuration view
Domain Name	Domain to which the configuration view is associated
Category	The Category of the configlet. The Category cannot exceed 255 characters. Allowable characters include the dash (-), underscore (_), letters, and numbers and the period (.).
Description	Description of the configlet. The description cannot exceed 2500 characters. This is an optional field.
Applied To	Name of the interface or the device to which the Configlet is being deployed.
Version	Version of the Configlet template used to create the Configlet.
Validation State	State of the Configlet such as an invalid Configlet or a validated Configlet.
Deployed State	Status of deployment of the Configlet.
Deployed Time	Date and time when the Configlet was deployed.
Deploy Now	Click this button to deploy and propagate the selected Configlet immediately to the device.
Schedule Deploy	Click this button to schedule the deploy of the selected Configlet for a later time.
Discard Deploy	Click this button to delete the selected Configlet.
Creation Time	Date and time when the Configlet was created.
Last Updated Time	Latest time when the Configlet was last updated.

Related Documentation

- [CLI Configlets Workflow on page 1352](#)
- [Configlet Context on page 1355](#)
- [Creating a CLI Configlet on page 1360](#)
- [Modifying a CLI Configlet on page 1363](#)
- [Deleting CLI Configlets on page 1363](#)
- [Creating a Parameter for a CLI Configlet on page 1366](#)

- [Applying a CLI Configlet to Devices on page 1368](#)

Creating a Parameter for a CLI Configlet

From the Manage Configlets page, you can also add parameters to a CLI Configlet. Parameters are the variables defined in the CLI Configlet whose values are either obtained from the environment or given by the user during execution. The following fields are displayed on this page:

Table 199: Attributes of a parameter

Parameter	Name of the parameter.
Display Name	Display name of the parameter.
Configured Value XPATH	<p>This field is used to give the XPath of the configured values. The behavior of this field depends on the type of view. When the view type is form, the corresponding value present in the XPath is taken as the field value. In case XPath returns multiple values, first value returned is considered. In case the XPath returns multiple values, the first value returned is considered. When the view type is grid, the following behavior is followed. If more than one parameters defined then following rules should be met.</p> <ul style="list-style-type: none"> • For independent index parameters, a join would be performed between the values returned by the XPath and the existing set of rows. • For dependent index parameters, join would be performed between the values returned by the XPath and the correspondent row. <p>For non index parameters, if list of values returned then they are aggregated into comma separated values.</p>
Description	Description of the parameter.
Scope	Scope of the parameter, such as device/entity specific or global.
Default Value	Default value of the parameter. The behavior is same as that of Configured value XPath except that the value is given explicitly. This field is considered only when Configured Value XPATH is not specified or if the XPath doesn't return any value.

From the Manage Configlets page, if you click the **Add Parameter** button, you are navigated to the Manage Arguments page. The Manage Arguments panel displays a list of arguments for the adding script and a form to manage the properties for them. When you select an argument from the grid, the lower part of the page displays the properties applicable to the selected argument.

To add a parameter to the CLI Configlet:

1. From the Manage Configlets page, click the **Add Parameter** button.

The Add Configlet Parameter pop-up window is displayed.

2. In the **Parameter** field, enter the name of the parameter.

The name of the parameter cannot exceed 255 characters. Allowable characters include the hyphen (-), underscore (_), letters, numbers, and the period (.).

3. In the **Display Name** field, enter a display name for the parameter.

The display name cannot exceed 255 characters. Allowable characters include the hyphen (-), underscore (_), letters, numbers, and the period (.).

4. In the **Description** field, enter a description for the parameter.
5. From the **Parameter Scope** drop-down list, select an appropriate scope for the parameter.

The options available are Global, Device Specific, and Entity Specific.

6. From the **Parameter Type** drop-down list, select an appropriate type of parameter. The options available are:

- Text Field – You can enter any value.
- Selection Field – You can select a value from a set of options.
- Invisible Field – The field displays a value that is explicitly defined by the user or an XPath.
- Password Field – Enter a password to apply the CLI Configlet.
- Password Confirm Field – Enter the password again to confirm the password.

7. From the **Regex Value** drop-down list, select an appropriate regular expression value.

This field is enabled if you choose the type of parameter as Text Field, Password Field, or Confirm Password Field.

8. From the **Configured Value Xpath** drop-down list, select an appropriate XPath value.

This field is enabled if you choose the type of parameter as Text Field, Selection Field, or Invisible Field. This is the XPath (with reference to the device XML) to fetch the set of values.

9. In the **Default Value** field, enter a default value.

This field is enabled if you choose the type of parameter as Text Field, Selection Field, or Invisible Field. This field is considered only when the XPath is not specified.

10. From the **Selection Values Xpath** drop-down list, select an appropriate XPath value.

This field is enabled if you choose the type of parameter as Selection Field. This is the XPath (with reference to the device XML) to fetch the set of values.

11. In the **Selection Values** field, enter an appropriate selection value.

This field is enabled if you choose the type of parameter as Selection Field.

12. In the **Order** field, enter the order in which the parameters should be listed while applying the CLI Configlet.

13. Click **Add**.

14. (Optional) Add multiple parameters.

15. (Optional) To discard the changes and go back to the previous page, click **Cancel**.

You are redirected to the previous page.

16. Click **Save**.

The CLI Configlet is created. You are redirected to the Configlets page.

**Related
Documentation**

- [CLI Configlets Workflow on page 1352](#)
- [Configlet Context on page 1355](#)
- [Modifying a CLI Configlet on page 1363](#)
- [Deleting CLI Configlets on page 1363](#)
- [Viewing CLI Configlets on page 1364](#)
- [Creating a Parameter for a CLI Configlet on page 1366](#)
- [Applying a CLI Configlet to Devices on page 1368](#)

Applying a CLI Configlet to Devices

You apply a CLI Configlet to devices when you want to push a configuration from the CLI Configlet to the devices.



NOTE:

At the time of creating the CLI Configlet:

- If you selected the Single execution type, the CLI Configlet can be applied to only one device.
- If you selected the Grouped execution type, the CLI Configlet can be applied to multiple devices simultaneously.

To apply a CLI Configlet to a device:

1. From the View selector, select **Chassis View**. The workspaces that you can configure in this view are displayed.
2. Click the **Build** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed.
3. From the Chassis View pane, click the plus sign (+) next to the My Network tree to expand the tree and view the list of devices.
4. Select the device for which you want to apply CLI configlets. A graphical view of the device is displayed on the right pane.
5. You can right-click each selectable component such as chassis or physical interfaces in the chassis view. The shortcut menu that is displayed indicates the name of the

selected component, state of the component, context path of the component, and the Manage Configlets option. Select **Manage Configlets** from the shortcut menu. The Select Configlets window is displayed, listing all of the available configlet templates that are applicable to the selected component.

6. To select a configlet to be applied to a device, do one of the following:
 - Double-click the chassis component, such as physical or logical interfaces, in the chassis view. The selected area is used as the context to list the templates in the Configlet selection window.
 - Click the Apply Configlet icon and use the links shown on the components in chassis view to select the context and apply configlets.
7. The Apply Configlet menu is displayed, depending on the component or context selected:

If you selected the chassis, the device configuration context is applicable. Click the Edit (pencil) icon beside the Zoom menu in the chassis image view. You can select the Configlets that can be applied to the device and the device context is listed for configuration.

If you selected a physical interface, select Apply Configlets from the Actions menu on the rightmost pane that displays component details. You can select the configlets from the list for the selected physical interface on the device.

If you selected a pseudo-interface and a logical Interface, click the pencil icon displayed in the the pseudo and logical interfaces grid. When you click the icon, the chassis element on the respective row is used as the context element and the list of Configlets that can be applied are displayed.

8. Select the CLI Configlet that you want to apply to the devices and select **Apply CLI Configlet** from the Actions menu.

The Apply CLI Configlet page is displayed.

When you select a Configlet Template from the Select Configlets table, the parameters panel is updated with the applicable parameters for the selected Configlet Template. The field components are based on the Parameter Type.

9. Select the devices on which you want to apply the CLI Configlet and select **Apply CLI Configlet** from the Actions menu.

The Apply CLI Configlet page displays the parameters. Only text field and selection field type parameters are displayed.

To view the description of the parameter, mouse over the entry in the Parameter column.



NOTE: You cannot select more than 25 devices. If the device selection using the search criteria or tags lists more than 25 devices,

10. Double-click the **Value** column for each parameter and enter a value.

All values are accepted for the text field type parameter. For a selection field type parameter, you should select from one of the values you provided for the parameter. The set of values present and the default value selected were defined when the template was created.

11. Click **Next**.

The parameter value is validated against the regular expression (if given). If the parameter value violates the regular expression, then a validation error is displayed.

The Preview area of the Apply CLI Configlet page displays the preview of the CLI Configlet. If you selected to view the parameters and the configuration when previewing the CLI Configlet, the parameters and the configuration are displayed.



NOTE: Contents of the Preview area depend on the preview options in the CLI Configlet.

12. (Optional) Click **Validate** to validate the configuration.

The Validate Results page is displayed.

A job is triggered. The Progress column displays the progress against each device. When the validation is complete, the results of the validation are displayed. The Status column indicates the results of the validation.



NOTE: You can also view the validation results from the Job Management page. To view the validation results, double-click the job ID and click the **View Results** link corresponding to the device.

Job ID	Job Name	Percent	Status	Summary
62...	Vpls-Test-scale Deployment	0 %	CANCELLED	Job was cancelled by user super
62...	vpls-bgp-res-tst Deployment	100 %	SUCCESS	Deployed On Device [RouterX1-re] On Device [RouterX1-re] On Device [RouterY1-re] Failed to add
62...	007_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE9_re] On Device [480R4_EP_Alok_re] On Device [PE10_re] On Device [480R3_EP_Alok_re]
62...	006_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE9_re] On Device [480R4_EP_Alok_re] On Device [480R3_EP_Alok_re] On Device [480R2_EP_Alok_re]
62...	005_P2P_RESValidate Service Order	100 %	FAILURE	Validating On Device [480R4_EP_Alok_re]Error Downloading Configuration [Configuration edit resu lock Success. edit-config Failed .
62...	004_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [480R3_EP_Alok_re] On Device [RouterZ1-re]
62...	003_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE8_re] On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [480R3_EP_Alok_re]
62...	002_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R3_EP_Alok_re]
62...	vpls-bgp-res-tst/Validate Service Order	100 %	SUCCESS	Validated On Device [RouterZ1-re] On Device [RouterX1-re] On Device [RouterY1-re]
62...	P2P_RES_0001 Deployment	100 %	SUCCESS	Deployed On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R3_EP_Alok_re]
62...	P2P_RES_0001/Validate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R3_EP_Alok_re]
62...	VPLS_LDP_451 ConfigAudit	100 %	SUCCESS	Audited [VPLS_LDP_451_audit_2015-09-03 09:14:43.654] Success on Device [ha2] Success on Device [ha1]
62...	VPLS_LDP_451/Functional Audit	100 %	SUCCESS	Functionally Audited [VPLS_LDP_451] Success on Device [ha2] Success on Device [ha1]
62...	RESTTest_Modify_2015-09-03_14-33-17 Deployment	100 %	SUCCESS	Modified On Device [PE8_re] On Device [PE9_re] On Device [junos-mx80-2-space] On Device [PE10_re]
62...	RESTTest_Modify_2015-09-03_14-33-17/Validate Service Order	100 %	SUCCESS	Modified On Device [PE8_re] On Device [PE9_re] On Device [junos-mx80-2-space] On Device [PE10_re]

13. Click **Close**.

You are redirected to the Apply CLI Configlet page.

14. Select whether to apply the CLI Configlet now or later.

- To apply the CLI Configlet now:

- Click **Apply**.

The Configlets Results page is displayed. This page shows the job results.

- Click **Close** to return to the Configlets page.

- To apply the CLI Configlet later:

- a. Click **Back**.

You are redirected to the previous page.

- b. Select **Schedule at a later time**.

- c. Enter the date in the **Date** field in the DD/MM/YYYY format.

- d. Enter the time in the **Time** field in the hh:mm format.

- e. Click **Apply**.

The Job Information dialog box is displayed.

- f. Click **OK**.

Click **Cancel** to return to the Device Management CLI Configlets page.

**Related
Documentation**

- [CLI Configlets Workflow on page 1352](#)
- [Configlet Context on page 1355](#)
- [Creating a CLI Configlet on page 1360](#)
- [Modifying a CLI Configlet on page 1363](#)
- [Deleting CLI Configlets on page 1363](#)
- [Viewing CLI Configlets on page 1364](#)
- [Creating a Parameter for a CLI Configlet on page 1366](#)

Deploying CLI Configlet Details

You apply a CLI Configlet to devices when you want to push the configuration to devices. The CLI Configlet can be deployed to only one device, or the CLI Configlet can be deployed to multiple devices simultaneously. The saved configlets that are being propagated to devices can be viewed by selecting the Deployment option in the task pane. You can select a particular Configlet and view the parameters contained in it in the form of configuration stanzas and hierarchy levels. Each level in the hierarchy is indented to indicate each statement's relative position in the hierarchy. Each level is generally set off with braces, with an open brace ({) at the beginning of each hierarchy level and a closing brace (}) at the end.

To select whether to apply the CLI Configlet now or later:

1. From the View selector, select **Device View**. The workspaces that you can configure in this view are displayed.
2. Click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed.
3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and view the list of devices.
4. Select the device for which you want to view the applied CLI configlets. A graphical view of the device is displayed on the right pane.
5. From the tasks pane, select **Configuration Deployment > View Applied Configlets**.
The Manage CLI-Applied Configlets page is displayed.
6. Select a Configlet from the table of displayed Configlets that you want to deploy.
7.
 - To apply the CLI Configlet now:
 - Click **Deploy Now**.
Use the CSD Deployment Jobs page in Deploy mode of Service View (by selecting Service Provisioning > View Deployment Jobs) to view the status of the deployment job created to provision the configlet to the device.
 - Click **Close** to return to the Configlets page.
 - To apply the CLI Configlet later:
 - a. Select **Schedule Deploy**.
 - b. Enter the date in the **Date** field in the DD/MM/YYYY format.
 - c. Enter the time in the **Time** field in the hh:mm format.

- d. Click **Apply**.
- e. Use the CSD Deployment Jobs page in Deploy mode of Service View (by selecting Service Provisioning > View Deployment Jobs) to view the status of the deployment job created to provision the configlet to the device.

To view a deployed CLI Configlet details:

1. From the View selector, select **Device View**. The workspaces that you can configure in this view are displayed.
2. Click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed.
3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and view the list of devices.
4. From the tasks pane, select **Configuration Deployment > View Applied Configlets**.

The Manage CLI-Applied Configlets page is displayed.

5. Select the device for which you want to view the applied CLI configlets. A graphical view of the device is displayed on the right pane.

The following fields are displayed on this page:

Table 200: Columns on the Manage CLI-Applied Configlets Page

Field	Description
Name	Name of the configuration view
Domain Name	Domain to which the configuration view is associated
Category	The Category of the configlet. The Category cannot exceed 255 characters. Allowable characters include the dash (-), underscore (_), letters, and numbers and the period (.).
Description	Description of the configlet. The description cannot exceed 2500 characters. This is an optional field.
Applied To	Name of the interface or the device to which the Configlet is being deployed.
Version	Version of the Configlet template used to create the Configlet.
Validation State	State of the Configlet such as an invalid Configlet or a validated Configlet.
Deployed State	Status of deployment of the Configlet.
Deployed Time	Date and time when the Configlet was deployed.

Table 200: Columns on the Manage CLI-Applied Configlets Page (continued)

Field	Description
Deploy Now	Click this button to deploy and propagate the selected Configlet immediately to the device.
Schedule Deploy	Click this button to schedule the deploy of the selected Configlet for a later time.
Discard Deploy	Click this button to delete the selected Configlet.
Creation Time	Date and time when the Configlet was created.
Last Updated Time	Latest time when the Configlet was last updated.

6. Select a Configlet from the table of displayed Configlets for which you want to view the configuration details. A dialog box is displayed with the configuration attributes and parameters defined for the Configlet being deployed.
7. Click **Close** after you finish viewing the Configlet information. You are returned to the page listing all of the deployed Configlets.

**Related
Documentation**

- [CLI Configlets Workflow on page 1352](#)
- [Configlet Context on page 1355](#)
- [Creating a CLI Configlet on page 1360](#)
- [Modifying a CLI Configlet on page 1363](#)
- [Deleting CLI Configlets on page 1363](#)
- [Creating a Parameter for a CLI Configlet on page 1366](#)
- [Applying a CLI Configlet to Devices on page 1368](#)

PART 17

Managing Optical Interfaces, OTUs, ODUs, ILAs, and IPLCs on MX Series and PTX Series Routers

- [Overview of Optical Interfaces, OTUs, and ODUs on page 1377](#)
- [Overview of Optical ILAs and IPLCs on page 1445](#)
- [Configuring and Monitoring Optical Interfaces, OTUs, and ODUs on page 1487](#)
- [Configuring and Monitoring Optical Inline Amplifiers on page 1579](#)
- [Configuring and Monitoring Optical Integrated Photonic Line Cards on page 1605](#)

CHAPTER 51

Overview of Optical Interfaces, OTUs, and ODUs

- [Optical Interfaces Management and Monitoring on MX Series and PTX Series Routers Overview on page 1378](#)
- [Ethernet DWDM Interface Wavelength Overview on page 1380](#)
- [Attenuation and Dispersion in a Fiber-Optic Cable on PTX Series Routers Overview on page 1380](#)
- [Understanding Pre-FEC BER Monitoring and BER Thresholds on page 1381](#)
- [DWDM Controllers Overview on page 1384](#)
- [PTX5000 PIC Description on page 1385](#)
- [PTX3000 PIC Description on page 1386](#)
- [100-Gigabit Ethernet OTN Optical Interface Specifications on page 1389](#)
- [100-Gigabit DWDM OTN PIC Optical Interface Specifications on page 1390](#)
- [100-Gigabit DWDM OTN PIC \(PTX Series\) on page 1394](#)
- [100-Gigabit Ethernet OTN PIC with CFP2 \(PTX Series\) on page 1402](#)
- [100-Gigabit Ethernet PIC with CFP2 \(PTX Series\) on page 1405](#)
- [100-Gigabit Ethernet PIC with CFP \(PTX Series\) on page 1408](#)
- [100GbE PICs for PTX Series Routers on page 1414](#)
- [P2-10G-40G-QSFPP PIC Overview on page 1415](#)
- [Understanding the P2-100GE-OTN PIC on page 1419](#)
- [100-Gigabit DWDM OTN PIC with CFP2 \(PTX Series\) on page 1423](#)
- [100-Gigabit DWDM OTN MIC with CFP2 on page 1432](#)
- [100-Gigabit Ethernet OTN Options Configuration Overview on page 1440](#)
- [Configuring the 10-Gigabit or 100-Gigabit Ethernet DWDM Interface Wavelength on page 1442](#)

Optical Interfaces Management and Monitoring on MX Series and PTX Series Routers Overview

Packet optical networking is useful in any network with a converged supercore that needs to transport traffic in as efficient and effective a manner as possible. Packet optical devices, such as Juniper Networks MX Series routers and PTX Series Packet Transport Routers properly equipped with suitable line cards, are capable of placing packets directly onto optical transports and receiving packets the same way. In a packet optical network, the packets leave the router in an optical transport envelope at the correct wavelength and arrive the same way, bypassing much of the other external networking equipment needed to groom or otherwise process electrical or optical signals originating on the router.

Connectivity Services Director is the network management application implemented on the Junos Space Network Management application and enables service providers achieve faster IP service rollouts for business needs and reduce overall OpEx for managing the service life cycle. A unified network device management interface is essential to efficiently deploy a large number of devices that contain optic PICs. Considering that these devices are hosted in remote locations, it is essential to ensure that the device management interface (DMI) provides the right level of automation to reduce the time required to set up and configure each device without requiring additional manual intervention at the site after deployment. Centralized configuration management, rapid deployment, polling, statistics capture, and reporting are some of the essential components of a robust DMI.

Connectivity Services Director enables you to manage the packet optical functionality provided by 100-Gigabit Ethernet Optical Transport Network (OTN) and dense wavelength-division multiplexing (DWDM) PICs that can be installed on PTX Series devices. In addition, you can manage the packet optical functionality provided by the 100-Gigabit Ethernet and DWDM MICs that can be installed on MX Series routers. Connectivity Services Director presents a topological network view and a site view. The topological network view offers a pictorial representation of optical sites, links, and services. The site view provides information about the status, configuration, alarms or faults, and the performance of the optical interfaces. FCAPS (fault, configuration, accounting, performance, and security) is an explicit model that is used to achieve the operational objectives of network management. Connectivity Services Director offers an effective management system for a complete FCAPS functionality.

An important aspect of any network management system is to monitor, control, and plan the network infrastructure that comprises a large number of devices and extensive configuration parameters in a streamlined, easy, and cohesive way. The bulk, single-step propagation of settings on large sets of devices without impacting the working efficiency and traffic-handling capacity of the network is a salient objective.

You can configure, manage, and monitor the following components on PTX3000 and PTX5000 routers:

- 100-Gigabit DWDM OTN PIC (P1-PTX-2-100G-WDM)
- 100-Gigabit Ethernet OTN PIC with CFP (P1-PTX-2-100GE-CFP)

- 100-Gigabit Ethernet OTN PIC with CFP2 (P2-100GE-OTN)
- 100-Gigabit DWDM OTN PIC with CFP2 (PTX-5-100G-WDM)
- P2-100GE-CFP2 (4x100G CFP2 PIC)
- P1-PTX-24-10GE-SFPP (24x10G LAN PIC)
- P1-PTX-24-10G-W-SFPP (24x10G LAN/WAN PIC)
- P1-PTX-2-100G-C-WDM-C (2x100G LH DWDM PIC)
- P1-PTX-2-40GE-CFP (2x40-Gigabit Ethernet PIC with CFP)
- P1-PTX-2-100GE-CFP (2x100-Gigabit Ethernet PIC with CFP)
- P1-PTX-2-100G-WDM—Designed for metro, regional, or long-haul applications.
- 4-port 100-Gigabit Ethernet PIC (PTX5000)

The PIC supports 100GBASE-LR4 and 100GBASE-SR10 transceivers. The CFP2-100G-SR10-D transceiver is not dual-rate, it supports Ethernet only. The CFP2-100G-SR10-D2 transceiver is dual-rate, but only when used in a PIC that supports OTN, such as P2-100GE-OTN.

- P2-10G-40G-QSFPP PIC on the FPC2-PTX-P1A FPC (PTX5000)

You can configure the P2-10G-40G-QSFPP PIC to operate either in 10-Gigabit Ethernet mode or in 40-Gigabit Ethernet mode.

The Chassis View provides a pictorial representation of the chassis or device, and the modules or components that are installed in it, such as the line cards, interfaces, and other hardware elements. To view a pictorial representation of a device chassis and the configured components, such as interfaces, line cards, and hardware elements, select a managed device listed on the My Network tree in Device View of Connectivity Services Director, and select **Device Management > View Physical Inventory** from the tasks pane. The right pane displays the device image and the corresponding description of the view selected in a table. The Chassis View is displayed. The hardware and line module details are displayed with a pictorial view of the slots of the devices and the modules installed in these slots. Use the arrow buttons on the page to rotate the device image to view all planes of the device and the components installed on each plane.

Click the right and left arrow buttons to view the right and left planes of the device. To view the front and the back planes of the devices, click the double-left and double-right arrows respectively. You can rotate the device image in different orientations along 360 degrees. The front view displays the components installed and the interfaces configured on the device. Click Refresh to update the contents of the page. Mouse over the device image to see brief information of components and interfaces in tooltips. Click a particular component or interface to display detailed information about the component or interface in the lower portion of the page.

Related Documentation

- [Viewing a Graphical Image of the Optical Interface Components on page 1487](#)

Ethernet DWDM Interface Wavelength Overview

Dense wavelength-division multiplexing (DWDM) interfaces are supported on 10-Gigabit Ethernet DWDM PICs, MICs, and MPCs; the 10-Gigabit Ethernet LAN/WAN OTN PIC; and the 100-Gigabit Ethernet DWDM OTN PIC. When a tunable optic transceiver is available, you can configure the DWDM interfaces with full C-band International Telecommunication Union (ITU)-Grid tunable optics, as defined in the following specifications:

- *Intel TXN13600 Optical Transceiver I2C Interface and Customer EEPROM Preliminary Specification*, July 2004.
- *I2C Reference Document for 300-Pin MSA 10G and 40G Transponder*, Edition 4, August 04, 2003.

By default, the wavelength is 1550.12 nanometers (nm), which corresponds to 193.40 terahertz (THz).

Related Documentation

- [Attenuation and Dispersion in a Fiber-Optic Cable on PTX Series Routers Overview on page 1380](#)
- [Understanding Pre-FEC BER Monitoring and BER Thresholds on page 1381](#)
- [DWDM Controllers Overview on page 1384](#)

Attenuation and Dispersion in a Fiber-Optic Cable on PTX Series Routers Overview

Correct functioning of an optical data link depends on modulated light reaching the receiver with enough power to be demodulated correctly. *Attenuation* is the reduction in the power of the light signal as it is transmitted. Attenuation is caused by passive media components, such as cables, cable splices, and connectors. While attenuation is significantly lower for optical fiber than for other media, it still occurs in both multimode and single-mode transmission. An efficient optical data link must have enough light available to overcome attenuation.

Dispersion is the spreading of the signal in time. The following two types of dispersion can affect an optical data link:

- Chromatic dispersion—Spreading of the signal in time resulting from the different speeds of light rays
- Modal dispersion—Spreading of the signal in time resulting from the different propagation modes in the fiber

For multimode transmission, modal dispersion, rather than chromatic dispersion or attenuation, usually limits the maximum bit rate and link length. For single-mode transmission, modal dispersion is not a factor. However, at higher bit rates and over longer distances, chromatic dispersion rather than modal dispersion limits maximum link length.

An efficient optical data link must have enough light to exceed the minimum power that the receiver requires to operate within its specifications. In addition, the total dispersion must be less than the limits specified for the type of link in Telcordia Technologies

document GR-253-CORE (Section 4.3) and International Telecommunications Union (ITU) document G.957.

When chromatic dispersion is at the maximum allowed, its effect can be considered as a power penalty in the power budget. The optical power budget must allow for the sum of component attenuation, power penalties (including those from dispersion), and a safety margin for unexpected losses.

Related Documentation

- [Ethernet DWDM Interface Wavelength Overview on page 1380](#)
- [Understanding Pre-FEC BER Monitoring and BER Thresholds on page 1381](#)
- [DWDM Controllers Overview on page 1384](#)

Understanding Pre-FEC BER Monitoring and BER Thresholds

Optical transport network (OTN) interfaces on PTX Series Packet Transport Routers support monitoring the condition of an OTN link by using the pre-forward error correction (pre-FEC) bit error rate (BER). The following PICs support pre-FEC BER monitoring:

- P1-PTX-2-100G-WDM
- P2-100GE-OTN
- PTX-5-100G-WDM
- P1-PTX-24-10G-W-SFPP

With pre-FEC BER monitoring enabled, when the configured pre-FEC BER signal degrade threshold is reached, the PIC stops forwarding packets to the remote interface and raises an interface alarm. Ingress packets continue to be processed. If pre-FEC BER monitoring is used with MPLS fast reroute or another link protection method, then traffic is rerouted to a different interface.

You can also configure backward fast reroute to insert the local pre-FEC status into transmitted OTN frames, notifying the remote interface of signal degradation. The remote interface can use the information to reroute traffic to a different interface. If you use pre-FEC BER monitoring together with backward fast reroute, then notification of signal degradation and rerouting of traffic occurs in less time than that required through a Layer 3 protocol.

Include the **signal-degrade-monitor-enable** and **backward-frr-enable** statements at the **[edit interfaces *interface-name* otn-options preemptive-fast-reroute]** hierarchy level to enable pre-FEC BER monitoring and backward fast reroute.



NOTE: When you configure pre-FEC BER signal degrade monitoring, we recommend that you configure both the **signal-degrade-monitor-enable** and the **backward-frr-enable** statements.

You can also configure the pre-FEC BER thresholds that raise or clear a signal degrade alarm and the time interval for the thresholds. If the BER thresholds and interval are not configured, the default values are used.

The pre-FEC BER signal degrade threshold value defines a specific amount of system margin relative to the BER correction limit (or FEC limit) of the PIC's receive FEC decoder. The FEC limit is fixed on each PIC—it is intrinsic to the FEC decoder implementation.



NOTE: The following examples use Q^2 -factor measurements (also known as Q -factor). Q^2 -factor is expressed in units of decibels relative to a Q^2 -factor of zero (dBQ). Q^2 -factor enables you to describe system margin in linear terms in contrast to BER values, which are nonlinear in nature. After you determine the thresholds, you must convert the threshold values from Q^2 -factor to BER to enter them in the CLI by using scientific notation. BER can be converted to Q^2 -factor by using the following equation:

$$Q^2\text{-factor} = 20 * \log_{10} (\text{sqrt}(2) * \text{erfcinv}(2 * \text{BER}))$$



TIP: To convert between Q^2 -factor and BER in a spreadsheet program, you can approximate the values by using the following formulas:

- To calculate Q^2 -factor:

$$= 20 * \text{LOG10}(-\text{NORMSINV}(\text{BER}))$$

- To calculate BER:

$$= 1 - \text{NORMSDIST}(10^{(0.05 * Q^2\text{-factor})})$$

Table 201 on page 1382 shows the relationship between the fixed FEC limit, the configurable signal degrade threshold, and the configurable clear threshold for different PICs. In this example, approximately 1 dBQ of system margin has been set between the FEC limit, signal degrade threshold, and clear threshold.

Table 201: Example—Signal Degrade and Clear Threshold Values at 1 dBQ

PIC	FEC Type	FEC Limit		Signal Degrade Threshold		Clear Threshold	
		Q^2 -Factor	BER	Q^2 -Factor	BER	Q^2 -Factor	BER
P1-PTX-2-100G-WDM	SD-FEC	6.7 dBQ	1.5E-2	7.7 dBQ	7.5E-3	8.7 dBQ	3.0E-3
P2-100GE-OTN	G.709 GFEC	11.5 dBQ	8.0E-5	12.5 dBQ	1.1E-5	13.5 dBQ	1.0E-6

Table 201: Example—Signal Degrade and Clear Threshold Values at 1 dBQ (continued)

PIC	FEC Type	FEC Limit		Signal Degrade Threshold		Clear Threshold	
		Q ² -Factor	BER	Q ² -Factor	BER	Q ² -Factor	BER
P1-PTX-24-10G-W-SFPP	G.975.11.4 (UFEC)	9.1 dBQ	2.2E-3	10.1 dBQ	6.9E-4	11.1 dBQ	1.6E-4
	G.975.11.7 (EFEC)	9.6 dBQ	1.3E-3	10.6 dBQ	3.6E-4	11.6 dBQ	7.5E-5
	G.709 GFEC	11.5 dBQ	8.0E-5	12.5 dBQ	1.1E-5	13.5 dBQ	1.0E-6

To adjust the signal degrade threshold, you must first decide on a new system margin target and then calculate the respective BER value (using the equation to convert from Q²-factor to BER). [Table 202 on page 1383](#) shows the values if 3 dBQ of system margin relative to the FEC limit is desired for the signal degrade threshold (while maintaining the clear threshold at 1 dBQ relative to the signal degrade threshold).



NOTE: The choice of system margin is subjective, as you might want to optimize your thresholds based on different link characteristics and fault tolerance and stability objectives. For guidance about configuring pre-FEC BER monitoring and BER thresholds, contact your Juniper Networks representative.

Table 202: Example—Signal Degrade and Clear Thresholds After Configuration

PIC	FEC Type	FEC Limit		Signal Degrade Threshold		Clear Threshold	
		Q ² -Factor	BER	Q ² -Factor	BER	Q ² -Factor	BER
P1-PTX-2-100G-WDM	SD-FEC	6.7 dBQ	1.5E-2	9.7 dBQ	1.1E-3	10.7 dBQ	2.9E-4
P2-100GE-OTN	G.709 GFEC	11.5 dBQ	8.0E-5	14.5 dBQ	4.9E-8	15.5 dBQ	1.1E-9
P1-PTX-24-10G-W-SFPP	G.975.11.4 (UFEC)	9.1 dBQ	2.2E-3	12.1 dBQ	2.8E-5	13.1 dBQ	3.1E-6
	G.975.11.7 (EFEC)	9.6 dBQ	1.3E-3	12.6 dBQ	1.1E-5	13.6 dBQ	9.1E-7
	G.709 GFEC	11.5 dBQ	8.0E-5	14.5 dBQ	4.8E-8	15.5 dBQ	1.1E-9

Include the **ber-threshold-signal-degrade**, **ber-threshold-clear**, and **interval** statements at the **[edit interfaces *interface-name* otn-options signal-degrade]** hierarchy level to configure the BER thresholds and time interval.



NOTE: Configuring a high BER threshold for signal degradation and a long interval might cause the internal counter register to be saturated. Such a configuration is ignored by the router, and the default values are used instead. A system log message is logged for this error.

**Related
Documentation**

- [Ethernet DWDM Interface Wavelength Overview on page 1380](#)
- [Attenuation and Dispersion in a Fiber-Optic Cable on PTX Series Routers Overview on page 1380](#)
- [DWDM Controllers Overview on page 1384](#)

DWDM Controllers Overview

Dense wavelength division multiplexing (DWDM) module support is based on the Optical Transport Network (OTN) protocol that is specified in ITU-T G.709. This standard combines the benefits of SONET/SDH technology with the multiwavelength networks of DWDM. It also enables forward error correction (FEC) that can allow a reduction in network costs by reducing the number of regenerators used. To enable multiservice transport, OTN uses the concept of a wrapped overhead (OH). To understand this format, the following elements are involved:

- Optical channel payload unit (OPU) OH information is added to the information payload to form the OPU. The OPU OH includes information to support the adaptation of client signals.
- Optical channel data unit (ODU) OH is added to the OPU to create the ODU. The ODU OH includes information for maintenance and operational functions to support optical channels.
- Optical channel transport unit (OTU) OH together with the FEC is added to form the OTU. The OTU OH includes information for operational functions to support the transport by way of one or more optical channel connections.
- Optical channel (OCh) OH is added to form the OCh. The OCh provides the OTN management functionality and contains four subparts: the OPU, ODU, OTU, and frame alignment signal (FAS).

**Related
Documentation**

- [Ethernet DWDM Interface Wavelength Overview on page 1380](#)
- [Attenuation and Dispersion in a Fiber-Optic Cable on PTX Series Routers Overview on page 1380](#)
- [Understanding Pre-FEC BER Monitoring and BER Thresholds on page 1381](#)

PTX5000 PIC Description

- [PTX5000 PIC Slots on page 1385](#)
- [PTX5000 PIC Function on page 1385](#)
- [PICs Supported on the PTX5000 on page 1385](#)
- [PTX5000 PIC Components on page 1385](#)

PTX5000 PIC Slots

Each FPC has two PIC slots. Blank PICs resemble other PICs but do not provide any physical connection or activity. When a PIC slot is not occupied by a PIC, you must insert a blank PIC to fill the empty slot and ensure proper cooling of the system. PICs are hot-removable and hot-insertable.

PTX5000 PIC Function

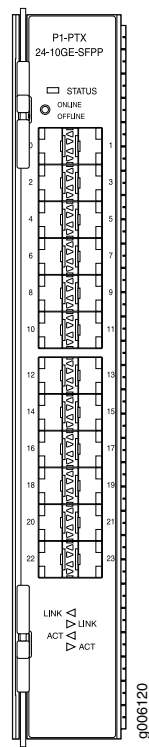
PICs provide the physical connection to various network media types, receiving incoming packets from the network and transmitting outgoing packets to the network. During this process, each PIC performs framing and line-speed signaling for its media type. Before transmitting outgoing data packets, the PICs encapsulate the packets received from the FPCs.

PICs Supported on the PTX5000

See *PICs Supported on the PTX Series* for a complete list of PICs supported on the PTX5000.

PTX5000 PIC Components

[Figure 65 on page 1386](#) shows an example of a PIC supported on the PTX5000. PICs have an upper ejector handle and a lower ejector handle.

Figure 65: PIC Faceplate

Related Documentation

- [100-Gigabit Ethernet OTN Options Configuration Overview on page 1440](#)
- [PTX3000 PIC Description on page 1386](#)

PTX3000 PIC Description

- [PIC Slots on page 1386](#)
- [PIC Function on page 1388](#)
- [PICs Supported on page 1388](#)
- [PIC Components on page 1388](#)

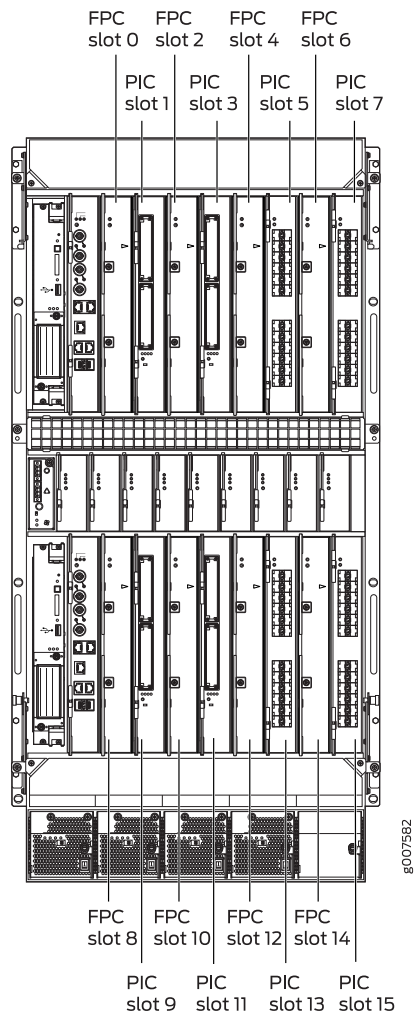
PIC Slots

Up to eight PICs install vertically in the front of the PTX3000 ([Figure 66 on page 1387](#)). The PIC slots are numbered 1, 3, 5, and 7 in the upper chassis, and 9, 11, 13, and 15 in the lower chassis.

The PIC in the slot to the right of an FPC is associated with that FPC. Each PIC requires an FPC to be installed in the adjacent FPC slot to its left as specified in [Table 203 on page 1387](#). For example, the PIC in slot 1 is associated with the FPC in slot 0.

When a slot is not occupied by a PIC, you must insert a blank PIC to fill the empty slot and ensure proper cooling of the system. Blank PICs resemble other PICs but do not provide any physical connection or activity. PICs are hot-removable and hot-insertable.

Figure 66: PIC Slots



NOTE: In the CLI, all PTX3000 PICs are represented as pic0.

Table 203: CLI Representation of PIC Slots

FPC Slot in Chassis	PIC Slot in Chassis	CLI Representation of PIC Slots
0	1	<code>fpc0-pic0-port-number</code>
2	3	<code>fpc2-pic0-port-number</code>
4	5	<code>fpc4-pic0-port-number</code>
6	7	<code>fpc6-pic0-port-number</code>
8	9	<code>fpc8-pic0-port-number</code>

Table 203: CLI Representation of PIC Slots (continued)

FPC Slot in Chassis	PIC Slot in Chassis	CLI Representation of PIC Slots
10	11	<code>fpc10-pic0-port-number</code>
12	13	<code>fpc12-pic0-port-number</code>
14	15	<code>fpc14-pic0-port-number</code>

PIC Function

PICs provide the physical connection to various network media types, receiving incoming packets from the network and transmitting outgoing packets to the network. During this process, each PIC performs framing and line-speed signaling for its media type. Before transmitting outgoing data packets, the PICs encapsulate the packets received from the FPCs.

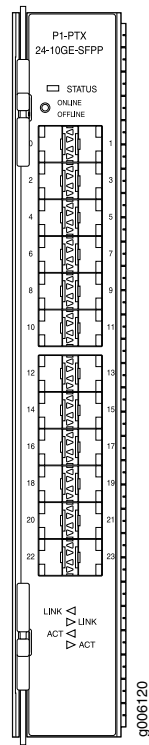
PICs Supported

See *PICs Supported on the PTX Series* for a complete list of PICs supported on the PTX3000.

PIC Components

[Figure 67 on page 1389](#) shows an example of a PIC supported on the PTX3000. PICs have an upper ejector handle and a lower ejector handle.

Figure 67: PIC Faceplate



**Related
Documentation**

- [100-Gigabit Ethernet OTN Options Configuration Overview on page 1440](#)
- [PTX5000 PIC Description on page 1385](#)

100-Gigabit Ethernet OTN Optical Interface Specifications

The 100-Gigabit Ethernet OTN (Optical Transport Network) optical interface standards described below are supported on PTX Series routers.

To determine which transceivers support each 100-Gigabit Ethernet OTN standard, see *Supported Network Interface Standards by Transceiver for PTX Series Routers*. The “Cables and Connectors” section in the description for each PIC lists which standards and transceivers are supported for that device.

- [OTU4 4I1-9D1F Optical Interface Specifications on page 1389](#)

OTU4 4I1-9D1F Optical Interface Specifications

Table 204 on page 1390 shows the optical interface specifications for the OTU4 4I1-9D1F standard.

Table 204: OTU4 411-9D1F (ITU-T 959.1) Optical Interface Specifications

Parameter	DML Laser	EML Laser
Optical interface	Single-mode	Same as DML laser
Standard	ITU-T 959.1	Same as DML laser
Maximum distance	ITU-T G.652 fiber, 6.2 miles (10 km)	Same as DML laser
Central frequency	1294.53 through 1296.59 nm 1299.02 through 1301.09 nm 1303.54 through 1305.63 nm 1308.09 through 1310.19 nm	Same as DML laser
Mean channel output power	−0.6 through 4.0 dBm per lane	−2.5 through 2.9 dBm per lane
Mean channel input power	−6.9 through 4.0 dBm	−8.8 through 2.9 dBm
Minimum equivalent sensitivity per lane	−8.4 dBm	−10.3 dBm

Related Documentation

- [100-Gigabit Ethernet OTN Options Configuration Overview on page 1440](#)
- [PTX5000 PIC Description on page 1385](#)
- [PTX3000 PIC Description on page 1386](#)

100-Gigabit DWDM OTN PIC Optical Interface Specifications

PTX Series routers support the following 100-Gigabit (Dense Wavelength Division Multiplexing) OTN (Optical Transport Network) fixed transceiver PIC:

- P1-PTX-2-100G-WDM—Designed for metro, regional, or long-haul applications.

[Table 205 on page 1390](#) and [Table 206 on page 1391](#) show the optical interface specifications for the 100-Gigabit DWDM OTN PIC transceivers.

Table 205: 100-Gigabit DWDM OTN PIC Optical Interface Specifications

Specifications	P1-PTX-2-100G-WDM
Transceiver type	<ul style="list-style-type: none"> • DWDM integrated transceiver
Standards	<ul style="list-style-type: none"> • ITU-T G.709—Interfaces for the optical transport network. • ITU-T G.798—Characteristics of optical transport network hierarchy equipment functional blocks • ITU-T G.694.1—Spectral grids for WDM applications: DWDM frequency grid • RFC 3591—Definitions of Managed Objects for the Optical Interface Type

Table 205: 100-Gigabit DWDM OTN PIC Optical Interface Specifications (continued)

Specifications	P1-PTX-2-100G-WDM
Optical interface	<ul style="list-style-type: none"> Single-mode optical fiber (ITU-T G.652)
Line interface	<ul style="list-style-type: none"> Line rate: 127.156441 Gbps Modulation format: Dual polarization-quadrature phase-shift keying (DP-QPSK), non-return-to-zero (NRZ) FEC type: Soft decision Channel-plan wavelength range: 1529.55 through 1567.54 nm Channel-plan frequency range: 191.25 through 196.00 THz Channel spacing: 50 GHz Channel tunability: 96 channels—see Table 206 on page 1391
Optical transmitter	<ul style="list-style-type: none"> Output power (on): –2 dBm Output power (off): ≤ –45 dBm Wavelength accuracy: +/–2.5 GHz Channel tuning time: ≤30 seconds
Optical receiver	<ul style="list-style-type: none"> Average receive power (input power range): –18 to –5 dBm Input sensitivity (unamplified/dark-fiber applications): –28 dBm LO wavelength accuracy: +/–2.5 GHz Channel tuning time: ≤30 seconds Damage input power threshold: +10 dBm Minimum OSNR (back-to-back): 13.5 dB typical Minimum OSNR (back-to-back): 14.5 dB worst-case, EOL Chromatic dispersion tolerance: +/–50,000 ps/nm PMD tolerance: 25 ps (mean DGD) Polarization tracking: 150 krad/s

[Table 206 on page 1391](#) provides the supported wavelengths in both terahertz (THz) and nanometers (nm).

Table 206: 100-Gigabit DWDM OTN Supported Wavelengths

100-GHz Grid		50-GHz Offset	
THz	nm	THz	nm
–	–	191.25	1567.54
191.30	1567.13	191.35	1566.72
191.40	1566.31	191.45	1565.90
191.50	1565.50	191.55	1565.09
191.60	1564.68	191.65	1564.27

Table 206: 100-Gigabit DWDM OTN Supported Wavelengths (continued)

100-GHz Grid		50-GHz Offset	
THz	nm	THz	nm
191.70	1563.86	191.75	1563.45
191.80	1563.05	191.85	1562.64
191.90	1562.23	191.95	1561.83
192.00	1561.42	192.05	1561.01
192.10	1560.61	192.15	1560.20
192.20	1559.79	192.25	1559.39
192.30	1558.98	192.35	1558.58
192.40	1558.17	192.45	1557.77
192.50	1557.36	192.55	1556.96
192.60	1556.55	192.65	1556.15
192.70	1555.75	192.75	1555.34
192.80	1554.94	192.85	1554.54
192.90	1554.13	192.95	1553.73
193.00	1553.33	193.05	1552.93
193.10	1552.52	193.15	1552.12
193.20	1551.72	193.25	1551.32
193.30	1550.92	193.35	1550.52
193.40	1550.12	193.45	1549.72
193.50	1549.32	193.55	1548.91
193.60	1548.51	193.65	1548.11
193.70	1547.72	193.75	1547.32
193.80	1546.92	193.85	1546.52
193.90	1546.12	193.95	1545.72

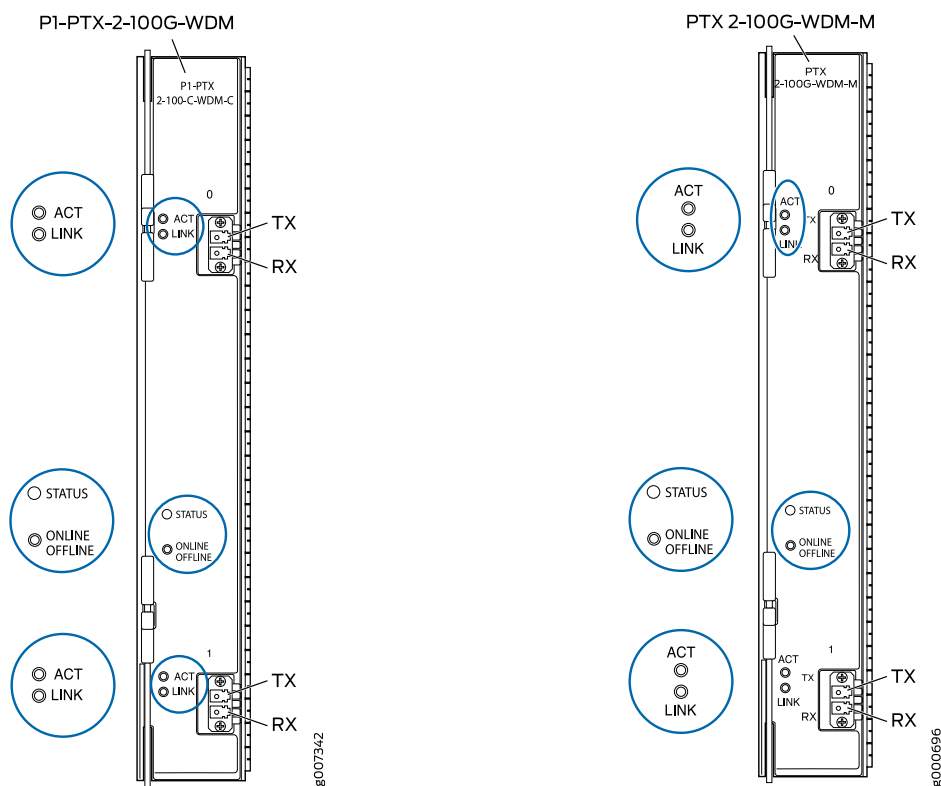
Table 206: 100-Gigabit DWDM OTN Supported Wavelengths (continued)

100-GHz Grid		50-GHz Offset	
THz	nm	THz	nm
194.00	1545.32	194.05	1544.92
194.10	1544.53	194.15	1544.13
194.20	1543.73	194.25	1543.33
194.30	1542.94	194.35	1542.54
194.40	1542.14	194.45	1541.75
194.50	1541.35	194.55	1540.95
194.60	1540.56	194.65	1540.16
194.70	1539.77	194.75	1539.37
194.80	1538.98	194.85	1538.58
194.90	1538.19	194.95	1537.79
195.00	1537.40	195.05	1537.00
195.10	1536.61	195.15	1536.22
195.20	1535.82	195.25	1535.43
195.30	1535.04	195.35	1534.64
195.40	1534.25	195.45	1533.86
195.50	1533.47	195.55	1533.07
195.60	1532.68	195.65	1532.29
195.70	1531.90	195.75	1531.51
195.80	1531.12	195.85	1530.72
195.90	1530.33	195.95	1529.94
196.00	1529.55	—	—

Related Documentation • [100-Gigabit Ethernet OTN Options Configuration Overview on page 1440](#)

- [PTX5000 PIC Description on page 1385](#)
- [PTX3000 PIC Description on page 1386](#)

100-Gigabit DWDM OTN PIC (PTX Series)



- [Software Release on page 1394](#)
- [Hardware Features on page 1395](#)
- [Software Features on page 1395](#)
- [Cables and Connectors on page 1397](#)
- [LEDs on page 1397](#)
- [Alarms, Errors, and Events on page 1397](#)

Software Release

PTX Series routers support the following 100-Gigabit DWDM (dense wavelength division multiplexing) OTN (optical transport network) PICs:

- 100-Gigabit DWDM OTN PIC (P1-PTX-2-100G-WDM):
 - PTX3000: Junos OS Release 13.3 and later

- PTX5000: Junos OS Release 13.2 and later

For information about which FPCs support this PIC, see *PTX Series PIC/FPC Compatibility*.

Hardware Features

- Model number:
 - P1-PTX-2-100G-WDM—Designed for metro, regional, or long-haul applications.
- Two 100-Gigabit DWDM OTN ports
- Power requirements: 6.48 A @ –48 V (311 W)
- Transparent transport of two 100-Gigabit Ethernet signals with OTU4V framing
- ITU-standard OTN performance monitoring and alarm management
- Dual polarization-quadrature phase-shift keying (DP-QPSK) modulation and soft-decision forward error correction (SD-FEC) for long haul and metro applications
- 96 channels on C-band ITU grid with 50-GHz spacing
- Full-duplex mode
- Maximum transmission units (MTUs) up to 9500 bytes
- Latency: 32 μ s (TX + RX)



NOTE: The 100-Gigabit DWDM OTN PIC is designed to comply with NEBS regulations on the PTX5000 router when used in typical configurations. The typical configuration for a PTX5000 router is up to eight FPCs, with one 100-Gigabit DWDM OTN PIC and one 100-Gigabit Ethernet PIC with CFP, 40-Gigabit Ethernet PIC with CFP, or 10-Gigabit Ethernet PIC with SFP+ installed in the same FPC.

The 100-Gigabit DWDM OTN PIC is designed to comply with NEBS regulations on the PTX3000 router when used in typical configurations at 40°C (104°F) at sea level. The typical configuration for a PTX3000 router is up to eight FPCs, with one 100-Gigabit DWDM OTN PIC next to each FPC in the top row only. The 100-Gigabit Ethernet PIC with CFP, 40-Gigabit Ethernet PIC with CFP, or 10-Gigabit Ethernet PIC with SFP+ are supported next to any FPC.

Software Features

Table 207 on page 1395 shows the first supported release for each software feature.

Table 207: Software Features Supported

Software Feature	PTX3000 First Supported Junos OS Release	PTX5000 First Supported Junos OS Release
Compliant with ITU G.709 and G.798	<ul style="list-style-type: none"> • P1-PTX-2-100G-WDM: 13.3 	<ul style="list-style-type: none"> • P1-PTX-2-100G-WDM: 13.2

Table 207: Software Features Supported (continued)

Software Feature	PTX3000 First Supported Junos OS Release	PTX5000 First Supported Junos OS Release
Provides a transport interface and state model (GR-1093)	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.3 	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.2
Performance monitoring such as alarms, threshold-crossing alarms, OTU/ODU error seconds and pre-FEC statistics	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.3 	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.2
SNMP management of the PIC based on RFC 3591, Managed Objects for the Optical Interface Type <ul style="list-style-type: none"> Set functionality Juniper Networks Black-Link MIB IFOTN MIB Optics MIB FRU MIB 	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.3 	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.2
IEEE 802.1ag OAM	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.3 	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.2
IEEE 802.3ah OAM	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.3 	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.2
IFINFO/IFMON	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.3 	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.2
IEEE 802.3ad link aggregation	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.3 	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.2
Pre-FEC BER monitoring provides interrupt-driven link-signal-degrade BER-based detection for MPLS fast reroute	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.3 	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.2
Flexible Ethernet services encapsulation	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.3 	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.2
Flexible VLAN tagging	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.3 	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.2
Source address MAC accounting per logical interface	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.3 	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.2
Source address MAC filter per port	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.3 PTX-2-100G-WDM-M: 14.2R3 	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.2
Source address MAC filter per logical interface	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.3 	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.2 PTX-2-100G-WDM-M: 14.2R3
Destination address MAC filter per port	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.3 	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.2
Up to 8000 logical interfaces shared across all ports on a single PFE	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.3 	<ul style="list-style-type: none"> P1-PTX-2-100G-WDM: 13.2

Cables and Connectors

- Single-mode optical fiber (ITU-T G.652)
- Duplex LC connector (Rx and Tx)
- Optical interface specifications

LEDs

The **STATUS** LED is located above the **ONLINE OFFLINE** button. The **LINK** and **ACT** LEDs are located next to each port. [Table 208 on page 1397](#) describes the functions of these LEDs.

Table 208: 100-Gigabit DWDM OTN PIC LEDs

Label	Color	State	Description
STATUS	Green	On steadily	PIC is online with no alarms or failures.
	Yellow	On steadily	PIC is initializing.
	Red	On steadily	PIC is online but has errors or alarms.
	–	Off	PIC is offline or not enabled.
LINK for each port:	Green	On steadily	Port is online with no alarms or failures, and the link is up.
	Yellow		Port has detected an alarm or failure.
	Red	On steadily	Port has detected a media alarm or failure.
	–	Off	Port is off or not enabled.
ACT for each port	Green	Flashing	Activity detected. Port is sending or receiving packets.
	–	Off	No packet activity detected on the port.

Alarms, Errors, and Events

Chassis and PIC:

- PIC (FRU) inserted or removed
- PIC (FRU) Admin InService/OutOfService, Oper Unequipped/Init/Normal/Mismatch/Fault/Upgrade
- Mismatch equipment
- Temperature alarm
- Fan alarm

Port (interface):

- Interface Admin InService/OutOfService/ServiceMA/OutOfServiceMA, Oper Init/Normal/Fault/Degraded

OTN (optical transport network):

- LOS (loss of signal)
- LOF (loss of frame)
- LOM (loss of multiframe)
- SSF (server signal failure)
- TSF (trail signal fail)

OTU (optical channel transport unit):

- OTU-FEC-DEG (forward error correction degraded)
- OTU-FEC-EXE (excessive errors, FEC_FAIL from the transponder)
- OTU-AIS (alarm indication signal or all ones signal)
- OTU-BDI (backward defect identification)
- OTU-IAE (incoming alignment error)
- OTU-BIAE (backward incoming alignment error)
- OTU-TTIM (destination access point identifier [DAPI], source access point identifier [SAPI], or both mismatch from expected to received)
- OTU-DEG (OTU degraded)

ODU (optical channel data unit):

- CSF (client signal failure)
- ODU-DM-TIMEOUT (DM timeout)
- ODU-LCK (ODU lock triggers for path monitoring and TCM levels 1 through 6)
- ODU-AIS (alarm indication signal or all ones signal)
- ODU-OCI (open connection error)
- ODU-BDI (backward defect indication)
- ODU-DEG (ODU degraded)
- ODU-IAE (incoming alignment error)
- ODU-DAPI-TTIM (DAPI or DAPI/SAPI mismatch from expected to receive)
- ODU-SAPI-TTIM (SAPI or DAPI/SAPI mismatch from expected to receive)
- ODU-BEI (backward error indication)
- ODU-BEI-ERR (backward error indication error)
- ODU-BIP8-ERR (bit interleaved parity 8 error)

- ODU-SSF (server signal fail)
- ODU-TSF (trail signal fail)
- ODU-SD (signal degrade)

OPU (optical channel payload):

- OPU-PTM (payload type mismatch)

Optics:

- TX output power

Card-related status:

- Transceiver temperature high alarm
- Transceiver temperature high warning
- Transceiver temperature low alarm
- Transceiver temperature low warning
- Transceiver voltage high alarm
- Transceiver voltage high warning
- Transceiver voltage low alarm
- Transceiver voltage low warning
- Transceiver temperature monitor A/D value
- Transceiver power supply monitor A/D value (voltage)

Network lane transmit-related status:

- TX laser current bias high alarm
- TX laser current bias high warning
- TX laser current bias low alarm
- TX laser current bias low warning
- TX laser temperature high alarm
- TX laser temperature high warning
- TX laser temperature low alarm
- TX laser temperature low warning
- TX output optical power high alarm
- TX output optical power high warning
- TX output optical power low alarm
- TX output optical power low warning
- TX laser TEC fault

- TX laser wavelength unlocked fault
- TX modulator bias high alarm
- TX modulator bias high warning
- TX modulator bias low alarm
- TX modulator bias low warning
- TX loss of signal fault
- TX current laser output power
- TX minimum laser output power over a performance monitoring interval
- TX average laser output power over a performance monitoring interval
- TX maximum laser output power over a performance monitoring interval

Network lane receive-related status:

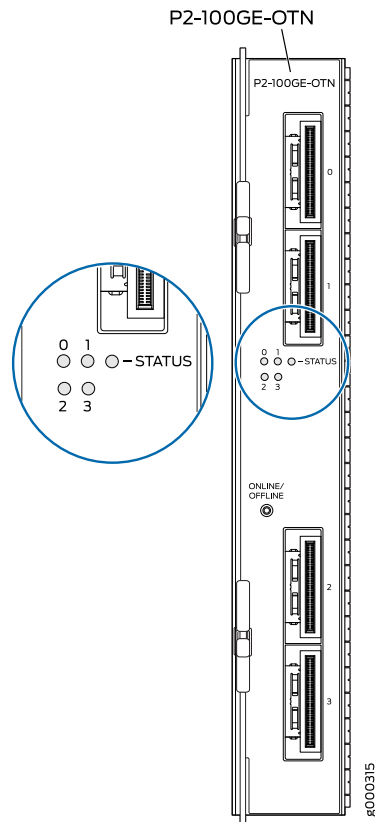
- RX laser bias current high alarm
- RX laser bias current high warning
- RX laser bias current low alarm
- RX laser bias current low warning
- RX input optical power high alarm
- RX input optical power high warning
- RX input optical power low alarm
- RX input optical power low warning
- RX laser output high alarm
- RX laser output high warning
- RX laser output low alarm
- RX laser output low warning
- RX laser temperature high alarm
- RX laser temperature high warning
- RX laser temperature low alarm
- RX laser temperature low warning
- RX LOS
- RX Laser wavelength unlocked fault
- RX laser TEC fault
- RX current chromatic dispersion
- RX average chromatic dispersion over a performance monitoring interval
- RX minimum chromatic dispersion over a performance monitoring interval

- RX maximum chromatic dispersion over a performance monitoring interval
- RX current Q
- RX average Q over a performance monitoring interval
- RX minimum Q over a performance monitoring interval
- RX maximum Q over a performance monitoring interval
- RX current carrier frequency offset
- RX average carrier frequency offset over a performance monitoring interval
- RX minimum carrier frequency offset over a performance monitoring interval
- RX maximum carrier frequency offset over a performance monitoring interval
- RX current SNR (signal-to-noise ratio)
- RX average SNR
- RX minimum SNR
- RX maximum SNR
- RX modem sync detect fault occurred over a performance monitoring interval
- RX modem lock fault occurred over a performance monitoring interval
- RX loss of alignment occurred over a performance monitoring interval
- RX out of alignment occurred over a performance monitoring interval
- RX deskew lock fault occurred over a performance monitoring interval
- RX LOS occurred over a performance monitoring interval
- RX current laser output power
- RX minimum laser output power over a performance monitoring interval
- RX average laser output power over a performance monitoring interval
- RX maximum laser output power over a performance monitoring interval

**Related
Documentation**

- [100-Gigabit Ethernet OTN Options Configuration Overview on page 1440](#)
- [PTX5000 PIC Description on page 1385](#)
- [PTX3000 PIC Description on page 1386](#)

100-Gigabit Ethernet OTN PIC with CFP2 (PTX Series)



- [Software Release on page 1402](#)
- [Hardware Features on page 1402](#)
- [Software Features on page 1403](#)
- [Cables and Connectors on page 1403](#)
- [LEDs on page 1404](#)

Software Release

- PTX5000: Junos OS Release 14.1R2 and later

Hardware Features

- Four ports that can be configured as 100-Gigabit Ethernet, 100-Gigabit OTN, or a combination of 100-Gigabit Ethernet and 100-Gigabit Ethernet OTN interfaces.
- Model number: P2-100GE-OTN
- Name in the CLI: **4x100GE OTN CFP2**

- Power requirements: 14.50A@ –12 V (176 W)
- Large maximum transmission units (MTUs): up to 9500 bytes

Software Features

Table 209 on page 1403 shows the first supported release for each software feature.

Table 209: Software Features Supported

Software Feature	First Supported Junos OS Release on PTX5000
Flexible Ethernet services encapsulation	14.1R2
Flexible VLAN tagging	14.1R2
IFINFO / IFMON	14.1R2
IEEE 802.1 ag OAM	14.1R2
IEEE 802.3 ah OAM	14.1R2
IEEE 802.3ad link aggregation	14.1R2
Interrupt-driven link-down detection for MPLS FRR	14.1R2
MAC accounting per logical interface for source addresses	14.1R2
MAC filter per port for destination addresses and source addresses	14.1R2
MAC filter per logical interface for source addresses	14.1R2
SNMP	14.1R2
Up to 4000 logical interfaces shared across all ports on a single PFE	14.1R2

Cables and Connectors

The following transceivers are supported on this PIC:

- CFP2-100G-LR4-D—Supports both 100GBASE-LR4 and OTU4 4I1-9D1F
 - Cable: See *100-Gigabit Ethernet 100GBASE-R Optical Interface Specifications* or *100-Gigabit Ethernet OTN Optical Interface Specifications*
 - Connector: LC
- CFP2-100G-SR10-D—Supports 100GBASE-SR10



NOTE: This transceiver supports Ethernet only, OTN is not supported.

- Cable: See *100-Gigabit Ethernet 100GBASE-R Optical Interface Specifications*
- Connector: 24-fiber MPO
- CFP2-100GBASE-LR4—Supports 100GBASE-LR4
 - Cable: See *100-Gigabit Ethernet 100GBASE-R Optical Interface Specifications*
 - Connector: LC
- CFP2-100GBASE-SR10—Supports 100GBASE-SR10
 - Cable:
 - Connector: 24-fiber MPO

LEDs

The **STATUS** LED is located to the left of the **ONLINE/OFFLINE** button. One LED is located next to each port to indicate the link activity of the port. [Table 210 on page 1404](#) describes the functions of these LEDs.

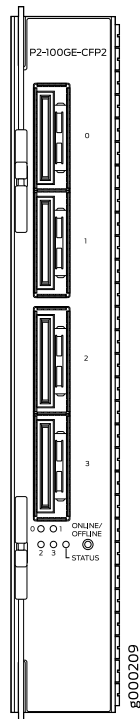
Table 210: 100-Gigabit Ethernet OTN PIC with CFP2 LEDs

Label	Color	State	Description
STATUS	Green	On steadily	PIC is online with no alarms or failures.
	Yellow	On steadily	PIC is initializing.
	Red	On steadily	PIC is in failed state.
	—	Off	PIC is offline or not enabled.
Single LED per port, labeled 0, 1, 2, and 3	Green	On steadily	Port is online with no alarms or failures, and the link is up.
		Blinking	Activity detected. Port is sending or receiving packets.
	Red	On steadily	Port is on but the link is down, and the port has detected a failure with alarms.
	—	Off	Port is off or not enabled.

Related Documentation

- [100-Gigabit Ethernet OTN Options Configuration Overview on page 1440](#)
- [PTX5000 PIC Description on page 1385](#)
- [PTX3000 PIC Description on page 1386](#)

100-Gigabit Ethernet PIC with CFP2 (PTX Series)



- [Software Release on page 1405](#)
- [Hardware Features on page 1405](#)
- [Software Features on page 1406](#)
- [Cables and Connectors on page 1406](#)
- [LEDs on page 1407](#)
- [Alarms, Errors, and Events on page 1407](#)

Software Release

- PTX5000: Junos OS Release 14.1 and later

Hardware Features

- Four 100-Gigabit Ethernet ports
- Model number: P2-100GE-CFP2
- Name in the CLI: **4x100GE CFP2**
- Power requirements: 1.66A@ -48 V (90W)
- Large maximum transmission units (MTUs): up to 9500 bytes

Software Features

Table 211 on page 1406 shows the first supported release for each software feature.

Table 211: Software Features Supported

Software Feature	PTX5000 First Supported Junos OS Release
Flexible-ethernet-services encapsulation	14.1
Flexible VLAN tagging	14.1
IFINFO / IFMON	14.1
IEEE 802.1 ag OAM	14.1
IEEE 802.3 ah OAM	14.1
IEEE 802.3ad link aggregation	14.1
Interrupt-driven link-down detection for MPLS FRR	14.1
MAC accounting per logical interface for source addresses	14.1
MAC filter per port for destination addresses and source addresses	14.1
MAC filter per logical interface for source addresses	14.1
SNMP	14.1
Up to 4000 logical interfaces share across all ports on a single PFE	14.1

Cables and Connectors

The following transceivers are supported on this PIC:

- CFP2-100G-LR4-D—Supports 100GBASE-LR4
 - Cable: See *100-Gigabit Ethernet 100GBASE-R Optical Interface Specifications*
 - Connector: LC
- CFP2-100G-SR10-D—Supports 100GBASE-SR10
 - Cable: See *100-Gigabit Ethernet 100GBASE-R Optical Interface Specifications*
 - Connector: 24-fiber MPO
- CFP2-100GBASE-LR4—Supports 100GBASE-LR4
 - Cable: See *100-Gigabit Ethernet 100GBASE-R Optical Interface Specifications*

- Connector: LC
- CFP2-100GBASE-SR10—Supports 100GBASE-SR10
 - Cable: See *100-Gigabit Ethernet 100GBASE-R Optical Interface Specifications*
- Connector: 24-fiber MPO



NOTE: The dual-rate transceiver (CFP2-100G-LR4-D) cannot be configured to use OTN framing when used in this PIC. The 100-Gigabit Ethernet OTN PIC with CFP2 (P2-100GE-OTN) supports OTN framing.

LEDs

The **STATUS** LED is located to the left of the **ONLINE/OFFLINE** button. One LED is located next to each port to indicate the link activity of the port. [Table 212 on page 1407](#) describes the functions of these LEDs.

Table 212: 100-Gigabit Ethernet PIC with CFP2 LEDs

Label	Color	State	Description
STATUS	Green	On steadily	PIC is online with no alarms or failures.
	Yellow	On steadily	PIC is initializing.
	Red	On steadily	PIC has an error or failure.
	—	Off	PIC is offline or not enabled and safe to remove from the router.
Single LED per port	Green	On steadily	Port is online with no alarms or errors, and the link is up.
		Blinking	There is link activity on the port.
	Red	On steadily	Port is on but the link is down, and the port has detected a failure.
	—	Off	Port is off or not enabled.

Alarms, Errors, and Events

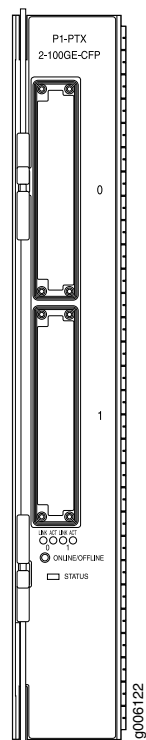
- Laser bias current high/low alarms and warnings
- Laser Rx power high/low alarms and warnings
- Module not ready alarm
- Module low power alarm
- Module temperature high/low alarms and warnings
- Rx CDR loss of lock alarm

- Rx loss of signal alarm
- Module not ready alarm
- Tx CDR loss of lock alarm

Related Documentation

- [100-Gigabit Ethernet OTN Options Configuration Overview on page 1440](#)
- [PTX5000 PIC Description on page 1385](#)
- [PTX3000 PIC Description on page 1386](#)

100-Gigabit Ethernet PIC with CFP (PTX Series)



- [Software Release on page 1408](#)
- [Hardware Features on page 1409](#)
- [Software Features on page 1409](#)
- [Cables and Connectors on page 1411](#)
- [LEDs on page 1412](#)
- [Alarms, Errors, and Events on page 1413](#)

Software Release

- PTX3000: Junos OS Release 13.2R2 and later

- PTX5000:



NOTE: PTX5000 does not support Junos OS Release 13.1.

- Junos OS Release 12.1X48 and later 12.1X48 releases
- Junos OS Release 12.3 and later 12.3 releases
- Junos OS Release 13.2 and later releases



NOTE: PTX5000 does not support Junos OS Releases 12.1, 12.2, or 13.1.

Hardware Features

- Two 100-Gigabit Ethernet CFP ports
- Model number P1-PTX-2-100GE-CFP
- Name in the CLI: **2x 100GE CFP**
- Power requirements: 1.6 A @ –48 V (75 W)
- Large maximum transmission units (MTUs):
 - Junos OS Release 12.1X48: up to 9192 bytes
 - Junos OS Release 12.1X48R2 and later 12.1X48 releases: up to 9500 bytes
 - Junos OS Release 12.3 and later 12.3 releases: up to 9500 bytes

Software Features

Table 213 on page 1409 shows the first supported release for each software feature.

Table 213: Software Features Supported

Software Feature	PTX3000 First Supported Junos OS Release	PTX5000 First Supported Junos OS Release
Flexible-ethernet-services encapsulation	13.2R2	12.1X48
		12.3
		13.2
Flexible VLAN tagging	13.2R2	12.1X48
		12.3
		13.2

Table 213: Software Features Supported (continued)

Software Feature	PTX3000 First Supported Junos OS Release	PTX5000 First Supported Junos OS Release
IFINFO / IFMON	13.2R2	12.1X48
		12.3
		13.2
IEEE 802.1 ag OAM	13.2R2	12.1X48
		12.3
		13.2
IEEE 802.3 ah OAM	13.2R2	12.1X48
		12.3
		13.2
IEEE 802.3ad link aggregation	13.2R2	12.1X48
		12.3
		13.2
Interrupt-driven link-down detection for MPLS FRR	13.2R2	12.1X48
		12.3
		13.2
MAC accounting per logical interface for source addresses	13.2R2	12.1X48
		12.3
		13.2
MAC filter per port for destination addresses and source addresses	13.2R2	12.1X48
		12.3
		13.2
MAC filter per logical interface for source addresses	13.2R2	12.1X48
		12.3
		13.2
SNMP	13.2R2	12.1X48
		12.3
		13.2

Table 213: Software Features Supported (continued)

Software Feature	PTX3000 First Supported Junos OS Release	PTX5000 First Supported Junos OS Release
Up to 8000 logical interfaces share across all ports on a single PFE	13.2R2	12.1X48
		12.3
		13.2

Cables and Connectors

- 100GBASE-ER4 (model number: CFP-100GBASE-ER4)
 - Duplex LC connector (RX and TX)
 - Junos OS Release 12.1X48R4 and later 12.1X48 releases
 - Junos OS Release 12.3 and later 12.3 releases
 - Junos OS Release 13.2 and later releases
- 100GBASE-ER4 (model number: CFP-GEN2-CGE-ER4 and part number: 740-049763)
 - Duplex LC connector (RX and TX)
 - Junos OS Release 12.3R5 and later 12.3 releases
 - Junos OS Release 13.2R3 and later 13.2 releases
 - Junos OS Release 13.3 and later releases



NOTE: The “GEN2” optics have been redesigned with newer versions of internal components for reduced power consumption.

- 100GBASE-LR4 (model number: CFP-100GBASE-LR4)
 - Duplex SC connector (RX and TX)
 - Junos OS Release 12.1X48 and later 12.1X48 releases
 - Junos OS Release 12.3 and later 12.3 releases
 - Junos OS Release 13.2 and later releases
- 100GBASE-LR4 (model number: CFP-GEN2-100GBASE-LR4 and part number: 740-047682)
 - Duplex LC connector (RX and TX)
 - Junos OS Release 12.3R5 and later 12.3 releases
 - Junos OS Release 13.2R3 and later 13.2 releases
 - Junos OS Release 13.3 and later releases



NOTE: The “GEN2” optics have been redesigned with newer versions of internal components for reduced power consumption.

- 100GBASE-SR10 (model number: CFP-100GBASE-SR10)
 - 24-fiber MPO connectors
 - Junos OS Release 12.1X48R3 and later 12.1X48 releases
 - Junos OS Release 12.3 and later 12.3 releases
 - Junos OS Release 13.2 and later releases
- 100GBASE-ZR (model number: CFP-100GBASE-ZR)
 - Duplex LC connector (RX and TX)
 - Supported in Junos OS Release 13.3R6, 14.1R4, 14.2R3, and 15.1R1 and later
 - Provides advanced dual polarization-quadrature phase shift keying (DP-QPSK) coherent digital signal processing (DSP) and forward error correction (FEC)-enabled robust tolerance to optical impairments and supports 80 km reach over single mode fiber
 - The transceiver is not specified as part of IEEE 802.3 but is built according to Juniper Networks specifications.
- Optical interface specifications—see [100-Gigabit Ethernet 100GBASE-R Optical Interface Specifications](#)

LEDs

The **STATUS** LED is located above the **ONLINE OFFLINE** button. The **LINK** and **ACT** LEDs are located next to each port. [Table 214 on page 1412](#) describes the functions of these LEDs.

Table 214: 100-Gigabit Ethernet PIC with CFP LEDs

Label	Color	State	Description
STATUS	Green	On steadily	PIC is online with no alarms or failures.
	Yellow	On steadily	PIC is initializing.
	Red	On steadily	PIC is online but has errors or alarms.
	—	Off	PIC is offline or not enabled.

Table 214: 100-Gigabit Ethernet PIC with CFP LEDs (continued)

Label	Color	State	Description
LINK for each port:	Green	On steadily	Port is online with no alarms or failures, and the link is up.
	Red	On steadily	Port is on but the link is down, and the port has detected a failure with alarms.
	–	Off	Port is off or not enabled.
ACT for each port	Green	Flashing	Activity detected. Port is sending or receiving packets.
	–	Off	No packet activity detected on the port.

Alarms, Errors, and Events

- Alarm indication signal (AIS)
- Laser bias current high/low alarms and warnings
- Laser Rx power high/low alarms and warnings
- Module not ready alarm
- Module power down alarm
- Module temperature high/low alarms and warnings
- Rx CDR loss of lock alarm
- Rx loss of signal alarm
- Rx not ready alarm
- Tx CDR loss of lock alarm
- Tx data not ready alarm
- Tx laser fault alarm
- Tx not ready alarm

Related Documentation

- [100-Gigabit Ethernet OTN Options Configuration Overview on page 1440](#)
- [PTX5000 PIC Description on page 1385](#)
- [PTX3000 PIC Description on page 1386](#)

100GbE PICs for PTX Series Routers

Juniper Networks 4-port 100GbE PICs enable service providers to deploy high-density 100G services in a wide variety of short-reach, long-reach, and DWDM scenarios. Using modular 100-gigabit pluggable transceiver (CFP2) optics, the 4-port 100GbE PICs are designed for second-generation PTX Series Packet Transport Routers line cards (FPC2) and provide line-rate performance in Ethernet and optical transport network (OTN) applications.

Juniper Networks® PTX Series Packet Transport Routers are architected for industry-leading system density in a transport-focused design that delivers the ability to scale, rapidly qualify and deploy, and reliably support the core—all at almost half the power of other core routers. The second generation of PTX Series hardware uses an optimized packaging of the successful Juniper Networks Junos® Express chip for robust, line-rate, and low-latency packet performance at up to 960 Gbps per slot. The 4-port 100GbE PIC family extends the existing PTX Series PIC portfolio by offering cost-optimized flexibility of dense 100GbE solutions to service providers. The mix and match of 4-port 100GbE PICs allows for up to 64 short-reach, long-reach, and tunable 100GbE interfaces per chassis for ultra-high speed interconnect applications. A PTX Series router fully equipped with second-generation line cards can demonstrate efficiency as high as 1.2 W/Gbps.

Architecture and Key Components

The 4-port 100GbE PICs for PTX Series line cards leverage the proven Junos Express technology in octal-Packet Forwarding Engine (PFE) configuration (FPC2). This approach combines proven and qualified hardware with advanced packaging and the latest in modular optical technology.

The 4-port 100GbE CFP2 PIC supports Ethernet over shortreach, long-reach, and extended long-reach distances in 100GbE SR10, LR4, and ER4 formats.

The 4-port 100GbE Ethernet/OTN CFP2 PIC is designed for the highest flexibility in local, and metro applications with Ethernet and OTN framing.

The 4-port 100GbE CFP2 PIC provides the benefits of a pluggable optical module in popular short-reach and long-reach applications, where OTN framing is not required. This includes the following applications:

- Intra-POP connectivity
- 100GbE fanout to 10GbE-optimized edge routers
- Router to DWDM shelf connections

The 4-port 100GbE CFP2 Ethernet/OTN PIC is the most flexible 100GbE quad-port option, with connectivity to a broad range of long-haul equipment. The 4-port 100GbE CFP2 Ethernet/OTN PIC supports OTN performance monitoring, and full control over OTN features via the Juniper Networks Junos operating system.

- Related Documentation**
- [100-Gigabit Ethernet OTN Options Configuration Overview on page 1440](#)
 - [PTX5000 PIC Description on page 1385](#)
 - [PTX3000 PIC Description on page 1386](#)

P2-10G-40G-QSFPP PIC Overview

Starting with Junos OS Release 14.1R2 and 14.2R1, PTX5000 supports the P2-10G-40G-QSFPP PIC on the FPC2-PTX-P1A FPC.

All the ports on the P2-10G-40G-QSFPP PIC are plugged into quad small form-factor pluggable plus transceivers (QSFP+) that, in turn, are connected to fiber-optic cables that support both 10-Gigabit Ethernet standards and 40-Gigabit Ethernet standards, thereby enabling you to configure the PIC to operate either in 10-Gigabit Ethernet mode or in 40-Gigabit Ethernet mode.

Starting from Junos OS Release 15.1, you can perform the following on the P2-10G-40G-QSFPP PIC on PTX5000 routers:

- You can configure the interfaces on this PIC to be a part of the mixed rates and mixed mode aggregated Ethernet bundles.
- Port-based pseudowire class of service (CoS) classification which includes Layer 3 IPv4, IPv6, and MPLS classification for interfaces with ethernet-ccc encapsulation.

The following sections describe the P2-10G-40G-QSFPP PIC and the various framing modes that are supported on it:

- [Understanding Dual Configuration on P2-10G-40G-QSFPP PIC on page 1415](#)
- [Port Numbering on P2-10G-40G-QSFPP PIC on page 1416](#)
- [10-Gigabit Ethernet Mode on page 1418](#)
- [40-Gigabit Ethernet Mode on page 1418](#)

Understanding Dual Configuration on P2-10G-40G-QSFPP PIC

All the ports on the P2-10G-40G-QSFPP PIC are QSFP+ based—that is, all the ports are connected to fiber-optic cables by means of QSFP+ transceivers.

The QSFP+ module—which includes the transceiver and the fiber-optic cable—supports the following standards on the P2-10G-40G-QSFPP PIC:

- 10-Gigabit Ethernet in LAN PHY framing mode (also known as native Ethernet mode) and WAN PHY framing mode.
- 40-Gigabit Ethernet in LAN PHY framing mode.

The P2-10G-40G-QSFPP PIC provides forty-eight 10-Gigabit Ethernet ports or twelve 40-Gigabit Ethernet ports. The PIC can be configured either in 10-Gigabit Ethernet mode or in 40-Gigabit Ethernet mode with the **set chassis fpc *fpc-number* pic *pic-number* pic-mode (10G | 40G)** configuration command. By default, the PIC is configured in 10-Gigabit Ethernet LAN PHY framing mode.

**NOTE:**

If you want configure the PIC in 10-Gigabit Ethernet mode to operate in 40-Gigabit Ethernet mode, you must:

1. Delete all the interfaces in the PIC at the [edit interfaces] hierarchy level.
2. Configure the PIC to operate in 40-Gigabit Ethernet mode by using the `set chassis fpc fpc-slot pic pic-slot pic-mode 40G` configuration command and commit.

The PIC reboots and starts operating in the new mode.

The same procedure is applicable when you can configure the PIC in 40-Gigabit Ethernet PIC to operate in 10-Gigabit Ethernet mode. In this case, you must execute the `set chassis fpc fpc-slot pic pic-slot pic-mode 10G` configuration mode command.

To check the current diagnostics of the PIC, you must run the relevant operational mode CLI commands such as `show chassis hardware`, `show interfaces`, `show interfaces diagnostics optics interface-name`, and so on.

Port Numbering on P2-10G-40G-QSFPF PIC

Table 215 on page 1416 shows the port numbering in 40-Gigabit Ethernet mode and in 10-Gigabit Ethernet mode.

Table 215: Port Numbering Table

QSFP+ Port Number	Port Numbering in 40-Gigabit Ethernet Mode	Port Numbering in 10-Gigabit Ethernet Mode
0	et-1/1/0	et-1/1/0:0
		et-1/1/0:1
		et-1/1/0:2
		et-1/1/0:3
1	et-1/1/1	et-1/1/1:0
		et-1/1/1:1
		et-1/1/1:2
		et-1/1/1:3
2	et-1/1/2	et-1/1/2:0
		et-1/1/2:1
		et-1/1/2:2
		et-1/1/2:3

Table 215: Port Numbering Table (continued)

QSFP+ Port Number	Port Numbering in 40-Gigabit Ethernet Mode	Port Numbering in 10-Gigabit Ethernet Mode
3	et-1/1/3	et-1/1/3:0
		et-1/1/3:1
		et-1/1/3:2
		et-1/1/3:3
4	et-1/1/4	et-1/1/4:0
		et-1/1/4:1
		et-1/1/4:2
		et-1/1/4:3
5	et-1/1/5	et-1/1/5:0
		et-1/1/5:1
		et-1/1/5:2
		et-1/1/5:3
6	et-1/1/6	et-1/1/6:0
		et-1/1/6:1
		et-1/1/6:2
		et-1/1/6:3
7	et-1/1/7	et-1/1/7:0
		et-1/1/7:1
		et-1/1/7:2
		et-1/1/7:3
8	et-1/1/8	et-1/1/8:0
		et-1/1/8:1
		et-1/1/8:2
		et-1/1/8:3
9	et-1/1/9	et-1/1/9:0
		et-1/1/9:1
		et-1/1/9:2
		et-1/1/9:3

Table 215: Port Numbering Table (continued)

QSFP+ Port Number	Port Numbering in 40-Gigabit Ethernet Mode	Port Numbering in 10-Gigabit Ethernet Mode
10	et-1/1/10	et-1/1/10:0
		et-1/1/10:1
		et-1/1/10:2
		et-1/1/10:3
11	et-1/1/11	et-1/1/11:0
		et-1/1/11:1
		et-1/1/11:2
		et-1/1/11:3

10-Gigabit Ethernet Mode

A 10-Gigabit Ethernet interface can operate in 10-Gigabit Ethernet LAN PHY framing mode or 10-Gigabit Ethernet WAN PHY framing mode.

You can configure a 10-Gigabit Ethernet interface at the **[edit interface *interface-name* framing-mode (lan-phy | wan-phy)]** hierarchy level to operate in 10-Gigabit Ethernet LAN PHY framing mode or in 10-Gigabit Ethernet WAN PHY framing mode.

Each P2-10G-40G-QSFPP PIC provides 48 physical interfaces. The interfaces are represented by the *et-fpc/pic/QSFP+ port:channel* interface naming convention, where the value of the *QSFP+ port* option ranges from 0 through 11 and the value of the *channel* option ranges from 0 through 3.

When a P2-10G-40G-QSFPP PIC is configured in 10-Gigabit Ethernet framing mode, it can operate in one of the following framing modes:

- LAN PHY framing mode. Note that by default, the PIC is in 10-Gigabit Ethernet LAN PHY framing mode.



NOTE: The ports are set to LAN PHY framing mode by default when the **framing-mode** statement is not configured at the **[edit interface *interface-name*]** hierarchy level.

- WAN PHY framing mode

40-Gigabit Ethernet Mode

You can configure twelve 40-Gigabit Ethernet interfaces that operate in LAN PHY framing mode. The interfaces are represented by the *et-fpc/pic/QSFP+ port* interface naming convention, where the value of the *QSFP+ port* option ranges from 0 through 11.

Understanding the P2-100GE-OTN PIC

Starting with Junos OS Release 14.1R2 and 14.2, a 100-Gigabit Ethernet OTN PIC—P2-100GE-OTN—is supported on the FPC2-PTX-P1A FPC in PTX5000 routers. The P2-100GE-OTN PIC provides 4-port 100-Gigabit Ethernet interfaces, which are independently configurable in LAN PHY framing mode or in optical channel transport unit 4 (OTU4) mode. Each interface is terminated by means of a CFP2 transceiver. The FPC2-PTX-P1A FPC supports two P2-100GE-OTN PICs, in which each 100-Gigabit Ethernet port is mapped to a Packet Forwarding Engine in the FPC.

Starting from Junos OS Release 15.1, you can perform the following on the P2-100GE-OTN PIC on PTX5000 routers:

- You can configure the interfaces on this PIC to be a part of the mixed rates and mixed mode aggregated Ethernet bundles.
- Port-based pseudowire class of service (CoS) classification which includes Layer 3 IPv4, IPv6, and MPLS classification for interfaces with ethernet-ccc encapsulation.

The following sections explain this PIC in detail:

- [Interface Features on page 1419](#)
- [Layer 2 and Layer 3 Features on page 1421](#)
- [OTN Alarms and Defects on page 1422](#)
- [TCA Alarms on page 1422](#)

Interface Features

The following interface features are supported on a P2-100GE-OTN PIC:

- 4-port 100-Gigabit Ethernet interfaces, which are independently configurable in LAN PHY framing mode or in OTU4 signal mode. Each interface is terminated by means of a CFP2 transceiver.
- Each port maps to a single Packet Forwarding Engine in the FPC2-PTX-P1A FPC.
- The interfaces are named with prefix *et*.
- Gigabit Ethernet local loopback.
- Link-level pause frames—You can halt the Ethernet interface from transmitting packets for a configured period of time.
- Interface hold timer and interface damping—You can set the **hold-time** statement (in milliseconds) to damp interface transitions.
- External clock
- Nonstandard tag protocol identifier (TPID):
 - For each 100-Gigabit Ethernet port, you can configure up to eight TPIDs by using the **tag-protocol-id** statement at the **[edit interfaces interface-name gige-ethernet-switch-profile]** hierarchy level.

- The **tag-protocol-id** statement can be configured only on the first port (port 0) of the PIC. If any other (nonzero) port has the **tag-protocol-id** configuration, the Routing Engine registers an error in the system log and the configuration is ignored.
- The **tag-protocol-id** statement configured on port 0 of the PIC also applies to the rest of the ports on that PIC.
- The interface *Link Down* event always generates an interrupt; however, the interface *Link Up* event does not generate an interrupt. Therefore, the interface link-up event is detected during the 1-second PIC periodic polling process.
- Generic forward error correction (GFEC) (G.709) and no-FEC modes of operation.
- Diagnostics tools:
 - Line loopback
 - Local loopback
- Fast reroute (FRR)—Based on configurable pre-FEC, bit error rate (BER) is supported and is configured using the **ber-threshold-signal-degrade** statement at the **[edit interfaces interface-name otn-options signal-degrade]** hierarchy level.
- *jnx-ifotn.mib* and *otn-mib* as defined in RFC 3591. Note that according to Junos OS security standard, configurable parameters are not supported through SNMP. Only the *get* operation is available through SNMP.
- FEC statistics—corrected errors and corrected error ratio.
- OTN payload pseudorandom binary sequence (PRBS) generation and checking by enabling or disabling PRBS with the **prbs** or **no-prbs** statement at the **[edit interfaces interface-name otn-options]** hierarchy level.
- Optical channel data unit (ODU)-level delay measurement.
- At the physical interface level, **flexible-ethernet-service**, **ethernet-ccc**, and **ethernet-tcc** encapsulations are supported. For the **flexible-ethernet-service** encapsulation, the logical level supports **enet2**, **vlan-ccc**, and **vlan-tcc** encapsulations.
- At the logical interface level, **dix**, **vlan-ccc**, and **vlan-tcc** encapsulations are supported.
- Interoperability between 100-Gigabit Ethernet interfaces with CFP transceiver and 100-Gigabit Ethernet interfaces with CFP2 transceiver in LAN PHY framing mode and in OTU4 mode.

The following features are not supported on the P2-100GE-OTN PIC:

- Source MAC learning for accounting
- MAC policing
- Physical interface-level encapsulations—**vlan-ccc**, **extended-vlan-ccc**, and **extended-vlan-tcc**
- Logical interface-level encapsulation—**vlan-vpls**
- VLAN rewrite for **ccc** encapsulation
- Per-queue flow control

- Generic framing procedure-framed (GFP-F) mapping modes over OTN
- General communication channel (GCC)
- OTN interface-level Automatic Protection Switching (APS)
- Insertion, monitoring, and display of OTN header overhead byte
- Black link MIB for integration with transponders
- Optical harness support
- Transport interface and state model (GR-1093)
- Trace tone support
- 15-minute and 1-day performance monitoring counters and historic counters

Layer 2 and Layer 3 Features

The following Layer 2 and Layer 3 features are supported on the P2-100GE-OTN PIC:

- MAC detect link up and link down based on local fault signal or remote fault signal.
- MAC statistics.
- Flow control.
- MAC oversized packet counters based on default MTU value or user-configured MTU value.
- Per-port destination address MAC filter.
- Per-port source address MAC filter.
- Per-physical interface source address MAC filter.
- Per-logical interface source address MAC accounting.
- Maximum of 1000 source MAC filter per physical interface.
- Maximum of 32,000 filter terms to share across all filter features.
- Aggregated Ethernet supports 64 child links that can be configured using the **set chassis aggregated-devices maximum-links** configuration command.
- Maximum of 1024 logical interfaces on an aggregated Ethernet physical interface.
- Support for VLAN tagging, flexible VLAN tagging, and stacked VLAN tagging.
- LACP.
- Link protection.
- 802.3 ah OAM.
- 802.1 ag OAM.
- MPLS FRR.
- SNMP.
- Supports per-VLAN queuing (using Packet Forwarding Engine).

OTN Alarms and Defects

The following OTN alarms and defects are supported on the P2-100GE-OTN PIC:

- LOS—Loss Of Signal
- LOF—Loss Of Frame
- LOM—Loss Of Multiframe
- OTU—Degrade
- OTU—AIS
- OTU—IAE
- OTU—BDI
- OTU—TTIM
- OTU—Signal Degrade
- OTU—Signal Fail
- ODU—Signal Fail
- OTU-FEC—Degrade
- OTU-FEC—Excessive errors
- ODU—Signal Degrade
- ODU—AIS
- ODU—BDI
- ODU—OCI
- ODU—LCK
- ODU—TTIM
- OPU—PTM

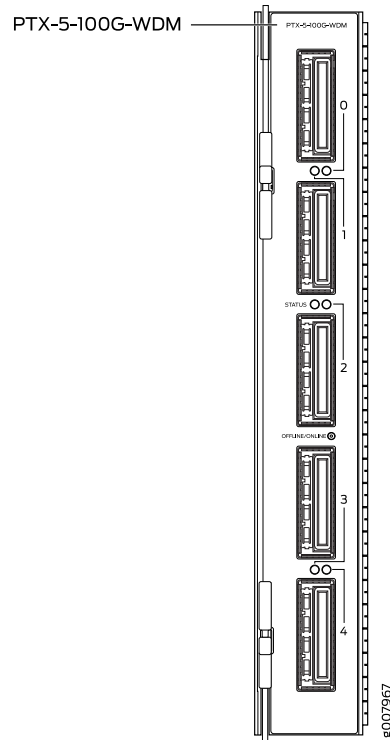
TCA Alarms

Threshold-crossing alarms (TCA) are alarms that are activated when a certain configurable threshold—near-end measurement threshold or far-end measurement threshold—is crossed and remains so until the end of the 15 minute interval for parameters such as OTU and ODU. The following alarms are supported:

- Background block error threshold (BBE)
- Errored seconds threshold (ES)
- Severely errored seconds threshold (SES)
- Unavailable seconds threshold (UAS)

- Related Documentation**
- [100-Gigabit Ethernet OTN Options Configuration Overview on page 1440](#)
 - [PTX5000 PIC Description on page 1385](#)
 - [PTX3000 PIC Description on page 1386](#)

100-Gigabit DWDM OTN PIC with CFP2 (PTX Series)



- [Software Release on page 1423](#)
- [Hardware Features on page 1424](#)
- [Software Features on page 1425](#)
- [Cables and Connectors on page 1426](#)
- [LEDs on page 1426](#)
- [Alarms, Errors, and Events on page 1426](#)

Software Release

- PTX3000: Junos OS Release 15.1F6 and later
- PTX5000: Junos OS Release 15.1F6 and later

Hardware Features

- Model number: PTX-5-100G-WDM
- Name in the CLI: **5X100GE DWDM CFP2-ACO**
- Five 100-Gigabit DWDM OTN ports
- Power requirement (including transceiver)
- Weight: 5.2 lb (2.4 kg)
- Supports CFP2-ACO pluggable optics
- Transparent transport of a 100-Gigabit Ethernet signal with OTU4(V) framing
- ITU-standard OTN performance monitoring and alarm management
- Dual polarization-quadrature phase-shift keying (DP-QPSK) modulation
- Supports two types of forward error correction (FEC):
 - Soft-decision FEC (SDFEC)
 - G.709 FEC (GFEC)
- 100 channels on C-band ITU grid with 50-GHz spacing
- Latency:
 - SDFEC: 14 μ s (TX + RX)
 - GFEC: 6 μ s (TX + RX)
- Interoperable with the CFP-100GBASE-ZR transceiver supported on the 100-Gigabit Ethernet MIC with CFP (MIC3-3D-1X100GE-CFP) on MX Series routers and the 100-Gigabit Ethernet PIC with CFP (P1-PTX-2-100GE-CFP) on PTX Series routers.



NOTE: The 5-port 100-Gigabit DWDM OTN PIC is not directly interoperable with the 2-port 100-Gigabit DWDM OTN PIC, but they can both operate over the same DWDM line system.



NOTE: The 5-port 100-Gigabit DWDM OTN PIC is designed to comply with NEBS regulations on the PTX3000 and PTX5000 routers when these routers are used in typical configurations.

In a typical configuration, a PTX3000 router supports up to eight FPCs, with up to four 5-port 100-Gigabit DWDM OTN PICs installed next to any FPC. You can install other PICs next to any other FPC.

In a typical configuration, a PTX5000 router supports up to eight FPCs, with up to eight 5-port 100-Gigabit DWDM OTN PICs in any FPC slot. You can install other PICs in any FPC slot.

Software Features

Table 207 on page 1395 shows the first supported release for each software feature.

Table 216: Software Features Supported

Software Feature	PTX3000 First Supported Junos OS Release	PTX5000 First Supported Junos OS Release
Compliant with ITU G.709 and G.798	15.1F6	15.1F6
Provides a transport interface and state model (GR-1093)	15.1F6	15.1F6
Performance monitoring such as alarms, threshold-crossing alarms, OTU/ODU error seconds and pre-FEC statistics	15.1F6	15.1F6
SNMP management of the PIC based on RFC 3591, Managed Objects for the Optical Interface Type <ul style="list-style-type: none"> Set functionality Juniper Networks Black-Link MIB IFOTN MIB Optics MIB FRU MIB 	15.1F6	15.1F6
IEEE 802.1ag OAM	15.1F6	15.1F6
IEEE 802.3ah OAM	15.1F6	15.1F6
IFINFO/IFMON	15.1F6	15.1F6
IEEE 802.3ad link aggregation	15.1F6	15.1F6
Pre-FEC BER monitoring provides interrupt-driven link-signal-degrade BER-based detection for MPLS fast reroute	15.1F6	15.1F6
User-configurable optics options: <ul style="list-style-type: none"> TX laser enable/disable TX output power TX/RX wavelength RX LOS warning/alarm thresholds Threshold crossing alarms (TCAs) 	15.1F6	15.1F6
User configurable card options: <ul style="list-style-type: none"> FEC mode (SDFEC/GFEC) Differential encoding mode TCAs Proactive protection (FRR) threshold / interval 	15.1F6	15.1F6

Cables and Connectors

Fiber-optic 100-gigabit CFP2-ACO transceiver

- Connector: Duplex LC
- Model number: TCFP2-100G-C



NOTE: When inserting the CFP2 transceiver, ensure that the transceiver sits tightly in the port. You will hear a distinct click sound when the latch locks into the corresponding port. The latch must be fully engaged in the corresponding port for the CFP2 transceiver to function properly. Failing to do so will result in loss of connection.

To verify that the CFP2 transceiver module is inserted properly, give a gentle pull by grasping the sides of the module. The module should sit tightly.

LEDs

The **STATUS** LED is located in the center of the PIC faceplate adjacent to the link and activity LED for port 2. The link and activity LEDs are located between the ports and are numbered 0 through 4. [Table 217 on page 1426](#) describes the functions of these LEDs.

Table 217: 100-Gigabit DWDM OTN PIC with CFP2 LEDs

Label	Color	State	Description
STATUS	Green	On steadily	PIC is initialized and online with no alarms or failures.
	Red	On steadily	PIC is online but has errors or alarms.
	–	Off	PIC is offline or not enabled.
Link and activity LED for each port	Green	On steadily	Port is online with no alarms or failures, and the link is up.
		Blinking	Activity is detected on the link.
	Red	On steadily	Port has detected a media alarm or failure.
	–	Off	Port is off or not enabled.

Alarms, Errors, and Events



NOTE: For OTN alarms, see [Table 218 on page 1431](#)

Chassis and PIC:

- PIC (FRU) inserted or removed
- PIC (FRU) Administrative State: In Service, Out Of Service
- PIC (FRU) Operational State: Unequipped, Init, Normal, Mismatch, Fault, Upgrade
- Mismatch equipment
- Temperature alarm

Port (interface):

- Interface Administrative State: In Service, Out Of Service, Service MA, Out of Service MA
- Interface Operational State: Init, Normal, Fault, Degraded

Optical channel transport unit (OTU) threshold-crossing alarms (TCAs):

- OTU-TCA-BBE—15 minute background block error TCA
- OTU-TCA-ES—15 minute far-end errored seconds TCA
- OTU-TCA-SES—15 minute severely errored seconds TCA
- OTU-TCA-UAS—15 minute unavailable seconds TCA

Optical channel data unit (ODU) TCAs:

- ODU-TCA-BBE—15 minute background block error TCA
- ODU-TCA-ES—15 minute far-end errored seconds TCA
- ODU-TCA-SES—15 minute severely errored seconds TCA
- ODU-TCA-UAS—15 minute unavailable seconds TCA



TIP: You can view OTU and ODU TCAs using the `show interfaces transport pm otn operational-mode` CLI command.

Optics-related status:

- TX output power
- TX current output power
- TX average output power over a performance monitoring interval
- TX minimum output power over a performance monitoring interval
- TX maximum output power over a performance monitoring interval
- RX current input power
- RX average input power over a performance monitoring interval
- RX minimum input power over a performance monitoring interval

- RX maximum input power over a performance monitoring interval
- Transceiver temperature high alarm
- Transceiver temperature high warning
- Transceiver temperature low alarm
- Transceiver temperature low warning
- Transceiver voltage high alarm
- Transceiver voltage high warning
- Transceiver voltage low alarm
- Transceiver voltage low warning
- Transceiver temperature monitor A/D value
- Transceiver power supply monitor A/D value (voltage)
- TX laser current bias high alarm
- TX laser current bias high warning
- TX laser current bias low alarm
- TX laser current bias low warning
- TX laser temperature high alarm
- TX laser temperature high warning
- TX laser temperature low alarm
- TX laser temperature low warning
- TX output optical power high alarm
- TX output optical power high warning
- TX output optical power low alarm
- TX output optical power low warning
- TX laser TEC fault
- TX laser wavelength unlocked fault
- TX modulator bias high alarm
- TX modulator bias high warning
- TX modulator bias low alarm
- TX modulator bias low warning
- TX LOS fault
- TX current laser output power
- TX minimum laser output power over a performance monitoring interval
- TX average laser output power over a performance monitoring interval

- TX maximum laser output power over a performance monitoring interval
- RX laser bias current high alarm
- RX laser bias current high warning
- RX laser bias current low alarm
- RX laser bias current low warning
- RX input optical power high alarm
- RX input optical power high warning
- RX input optical power low alarm
- RX input optical power low warning
- RX laser output high alarm
- RX laser output high warning
- RX laser output low alarm
- RX laser output low warning
- RX current laser output power
- RX minimum laser output power over a performance monitoring interval
- RX average laser output power over a performance monitoring interval
- RX maximum laser output power over a performance monitoring interval
- RX laser temperature high alarm
- RX laser temperature high warning
- RX laser temperature low alarm
- RX laser temperature low warning
- RX LOS fault
- RX LOS occurred over a performance monitoring interval
- RX laser wavelength unlocked fault
- RX laser TEC fault

Network lane receive-related status:

- RX current chromatic dispersion
- RX average chromatic dispersion over a performance monitoring interval
- RX minimum chromatic dispersion over a performance monitoring interval
- RX maximum chromatic dispersion over a performance monitoring interval
- RX current differential group delay
- RX average differential group delay over a performance monitoring interval
- RX minimum differential group delay over a performance monitoring interval

- RX maximum differential group delay over a performance monitoring interval
- RX current Q value
- RX average Q value over a performance monitoring interval
- RX minimum Q value over a performance monitoring interval
- RX maximum Q value over a performance monitoring interval
- RX current signal-to-noise ratio (SNR)
- RX average SNR
- RX minimum SNR
- RX maximum SNR
- RX current carrier frequency offset
- RX average carrier frequency offset over a performance monitoring interval
- RX minimum carrier frequency offset over a performance monitoring interval
- RX maximum carrier frequency offset over a performance monitoring interval
- RX modem sync detect fault occurred over a performance monitoring interval
- RX modem lock fault occurred over a performance monitoring interval
- RX loss of alignment occurred over a performance monitoring interval
- RX out of alignment occurred over a performance monitoring interval
- RX deskew lock fault occurred over a performance monitoring interval

FEC statistics:

- Corrected Errors
- Uncorrected Words
- Corrected Error Ratio



TIP: You can view FEC statistics using the `show interfaces interface-name extensive operational-mode` CLI command.

[Table 218 on page 1431](#) describes the OTN alarms and defects that can occur on the PIC and the link status when the alarm or defect occurs.



TIP: You can view OTN alarms and defects using the `show interfaces interface-name extensive operational-mode` CLI command.

Table 218: OTN Alarms and Defects

Category	Alarm	Description	Link Status
OTN	LOS	Loss of signal	Link down
	LOF	Loss of frame	Link down
	LOM	Loss of multiframe	Link down
	Wavelength Lock	Wavelength lock	Warning
OTN FEC	FEC Degrade (OTU-FEC-DEG)	Forward error correction degraded	Link down if FRR is enabled
	FEC Excessive (OTU-FEC-EXE)	Excessive errors, FEC_FAIL from the transponder	Possible link down
OTN OTU	OTU-AIS	Alarm indication signal or all ones signal	Link down
	OTU-BDI	Backward defect identification	Link down
	OTU-IAE	Incoming alignment error	Warning
	OTU-TTIM	Destination access point identifier (DAPI), source access point identifier (SAPI), or both mismatch from expected to received	Can cause link down if otu-ttim-act-enable is configured at the edit interfaces interface-name otn-options hierarchy
	OTU-BIAE	Backward incoming alignment error	Warning
	OTU-TSF	OTU trail signal fail	Warning
	OTU-SSF	OTU server signal fail	Warning

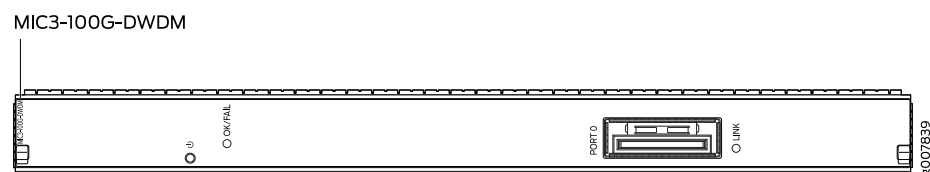
Table 218: OTN Alarms and Defects (continued)

Category	Alarm	Description	Link Status
OTN ODU	ODU-AIS	Alarm indication signal or all ones signal	Link down
	ODU-OCI	Open connection error	Link down
	ODU-LCK	ODU lock triggers for path monitoring and TCM levels 1 through 6	Link down
	ODU-BDI	Backward defect indication	Link down
	ODU-TTIM	DAPI or SAPI mismatch from expected to received	Can cause link down if odu-ttim-act-enable is configured at the [edit interfaces interface-name otn-options] hierarchy
	ODU-IAE	Incoming alignment error	Warning
	ODU-LTC	Loss of tandem connection	Warning
	ODU-CSF	Client signal failure	Warning
	ODU-TSF	Trail signal fail	Warning
	ODU-SSF	Server signal fail	Warning
	ODU-PTIM	Payload type mismatch	Link down

Related Documentation

- [100-Gigabit DWDM OTN MIC with CFP2 on page 1432](#)
- [Configuring the 10-Gigabit or 100-Gigabit Ethernet DWDM Interface Wavelength on page 1442](#)

100-Gigabit DWDM OTN MIC with CFP2



Software release

- Junos 15.1F5 and later

Description	<ul style="list-style-type: none"> • One 100-Gigabit DWDM OTN port • Power requirements (including transceiver) at different temperatures: <ul style="list-style-type: none"> • 55° C: 1.90 A @ 48 V (91 W) • 25° C: 1.73 A @ 48 V (83 W) • Weight: 2.3 lb (1.04 kg) • Model number: MIC3-100G-DWDM • Name in the CLI: 1X100GE DWDM CFP2-ACO
Hardware features	<ul style="list-style-type: none"> • Dual-wide MIC that installs into two MIC slots • Supports CFP2 analog coherent optics (CFP2-ACO) • Transparent transport of a 100-Gigabit Ethernet signal with OTU4V framing • ITU-standard OTN performance monitoring and alarm management • Dual-polarization quadrature phase shift keying (DP-QPSK) modulation • Supports three types of forward error correction (FEC): <ul style="list-style-type: none"> • Soft-decision FEC (SD-FEC) • High-gain FEC (HG-FEC) • G.709 FEC (GFEC) • 100 channels on C-band ITU grid with 50-GHz spacing • Latency: <ul style="list-style-type: none"> • SD-FEC: 14 μs (TX + RX) • HG-FEC: 22 μs (TX + RX) • GFEC: 6 μs (TX + RX) • Interoperable with the CFP-100GBASE-ZR transceiver supported on the 100-Gigabit Ethernet MIC with CFP (MIC3-3D-1X100GE-CFP) on MX Series routers and the 100-Gigabit Ethernet PIC with CFP (P1-PTX-2-100GE-CFP) on PTX Series routers. <p>NOTE: The 1-port 100-Gigabit DWDM OTN MIC is not directly interoperable with the 2-port 100-Gigabit DWDM OTN PIC (P1-PTX-2-100G-WDM), but they can both operate over the same DWDM line system.</p>

Software features	<ul style="list-style-type: none"> Compliant with ITU G.709 and G.798 Provides a transport interface and state model (GR-1093) Performance monitoring features such as alarms, threshold-crossing alarms, OTU/ODU error seconds and FEC and bit error rate (BER) statistics SNMP management of the MIC based on <i>RFC 3591, Managed Objects for the Optical Interface Type</i>, including the following: <ul style="list-style-type: none"> Set functionality Black Link MIB IFOTN MIB Optics MIB FRU MIB Pre-FEC BER monitoring provides interrupt-driven, BER-based detection of link signal degradation for MPLS fast reroute. User-configurable optics options: <ul style="list-style-type: none"> Transmit (TX) laser enable and disable TX output power Wavelength Receive (RX) LOS warning or alarm thresholds Threshold crossing alarms (TCAs) <p>User-configurable card options:</p> <ul style="list-style-type: none"> FEC mode (SD-FEC, HG-FEC, or GFEC) TCAs
Cables and connectors	<p>Fiber-optic 100-gigabit CFP2-ACO transceiver</p> <ul style="list-style-type: none"> Connector: Duplex LC/UPC Model number: TCFP2-100G-C <p>NOTE: When inserting the C form-factor pluggable 2 (CFP2) transceiver, ensure that the transceiver sits tightly in the port. You hear a distinct click sound when the latch locks into the corresponding port. The latch must be fully engaged in the corresponding port for the CFP2 transceiver to function properly. Failing to do so can result in loss of connection.</p> <p>To verify that the CFP2 transceiver module is inserted properly, give a gentle pull by grasping the sides of the module. The module should sit tightly.</p>
LEDs	<p>OK/FAIL LED, one bicolor:</p> <ul style="list-style-type: none"> Off—MIC is powered off. Green—MIC is initialized and online, functioning normally. Amber—MIC is coming online, or is in fault state. <p>LINK LED, one bicolor per port:</p> <ul style="list-style-type: none"> Off—Port is offline. Solid green—Link is up. Red—Port failure is detected. <p>NOTE: The port is labeled Port 0.</p>

Alarms, Errors, and Events

NOTE: For OTN alarms, see [Table 219 on page 1439](#).

Chassis and MIC:

- MIC (FRU) inserted or removed
- MIC (FRU) Administrative State: In Service, Out Of Service
- MIC (FRU) Operational State: Unequipped, Init, Normal, Mismatch, Fault, Upgrade
- Mismatch equipment
- Temperature alarm

Port (interface):

- Interface Administrative State: In Service, Out Of Service, Service MA, Out of Service MA
- Interface Operational State: Init, Normal, Fault, Degraded

Optical channel transport unit (OTU) TCAs:

- OTU-TCA-BBE—15-minute background block error TCA
- OTU-TCA-ES—15-minute far-end errored seconds TCA
- OTU-TCA-SES—15-minute severely errored seconds TCA
- OTU-TCA-UAS—15-minute unavailable seconds TCA

Optical channel data unit (ODU) TCAs:

- ODU-TCA-BBE—15-minute background block error TCA
- ODU-TCA-ES—15-minute far-end errored seconds TCA
- ODU-TCA-SES—15-minute severely errored seconds TCA
- ODU-TCA-UAS—15-minute unavailable seconds TCA

TIP: You can view OTU and ODU TCAs by using the **show interfaces transport pm otn** operational-mode CLI command.



NOTE: If you insert an invalid CFP module, the CLI displays **unsupported module** and a syslog message is generated.

Optics-related status:

- Module temperature
- Module voltage
- Module temperature alarm:
 - High alarm
 - Low alarm
 - High warning
 - Low warning
- Module voltage alarm:
 - High alarm
 - Low alarm
 - High warning
 - Low warning
- Module not ready alarm
- Module low power alarm
- Module initialization incomplete alarm
- Module fault alarm
- TX laser disabled alarm
- RX loss of signal alarm
- Modem lock state
- TX output power:
 - Current TX output power
 - Minimum over a performance monitoring interval
 - Maximum over a performance monitoring interval
 - Average over a performance monitoring interval
- TX power alarm:
 - High alarm
 - Low alarm
 - High warning
 - Low warning
- RX input power (signal)
- RX input power (total):
 - Current RX input power (total)
 - Minimum over a performance monitoring interval
 - Maximum over a performance monitoring interval
 - Average over a performance monitoring interval
- RX power alarm:
 - High alarm
 - Low alarm
 - High warning
 - Low warning
- RX loss of signal alarm
- Wavelength unlocked alarm

TIP: You can view optics-related status by using the **show interfaces transport pm optics** and **show interfaces diagnostics optics** operational-mode CLI commands.

Network lane receive-related status:

- Chromatic dispersion:
 - Current chromatic dispersion
 - Minimum over a performance monitoring interval
 - Maximum over a performance monitoring interval
 - Average over a performance monitoring interval
- Differential group delay:
 - Current differential group delay
 - Minimum over a performance monitoring interval
 - Maximum over a performance monitoring interval
 - Average over a performance monitoring interval
- Q²-factor:
 - Current Q²-factor
 - Minimum over a performance monitoring interval
 - Maximum over a performance monitoring interval
 - Average over a performance monitoring interval
- Carrier frequency offset
 - Current carrier frequency offset
 - Minimum over a performance monitoring interval
 - Maximum over a performance monitoring interval
 - Average over a performance monitoring interval
- Signal-to-noise ratio (SNR)
 - Current SNR
 - Minimum over a performance monitoring interval
 - Maximum over a performance monitoring interval
 - Average over a performance monitoring interval

TIP: You can view network lane receive-related status by using the **show interfaces transport pm optics** operational-mode CLI command.

FEC statistics:

- Corrected Errors—the number of bits received that were in error, but corrected.
- Uncorrected Words—the number of FEC codewords received that were uncorrectable.
- Corrected Error Ratio—the number of corrected bits divided by the number of bits received

TIP: You can view FEC statistics by using the **show interfaces interface-name extensive** operational-mode CLI command.

Table 219 on page 1439 describes the OTN alarms and defects that can occur on the MIC and the link status when the alarm or defect occurs.



TIP: You can view OTN alarms and defects by using the **show interfaces interface-name extensive** operational-mode CLI command.

Table 219: OTN Alarms and Defects

Category	Alarm	Description	Link Status
OTN	LOS	Loss of signal	Link down
	LOF	Loss of frame	Link down
	LOM	Loss of multiframe	Link down
OTN FEC	FEC Degrade (OTU-FEC-DEG)	Forward error correction degraded	Link down if FRR is enabled
	FEC Excessive (OTU-FEC-EXE)	There are uncorrected words and there are errors in the frame header	Possible link down
OTN OTU	OTU-AIS	Alarm indication signal or all ones signal	Link down
	OTU-BDI	Backward defect identification	Link down
	OTU-IAE	Incoming alignment error	Warning
	OTU-TTIM	Destination access point identifier (DAPI), source access point identifier (SAPI), or both mismatch from expected to received	Can cause the link to be down if otu-ttim-act-enable is configured at the [edit interfaces <i>interface-name</i> otn-options] hierarchy level
	OTU-BIAE	Backward incoming alignment error	Warning
	OTU-TSF	OTU trail signal fail	Warning
	OTU-SSF	OTU server signal fail	Warning

Table 219: OTN Alarms and Defects (continued)

Category	Alarm	Description	Link Status
OTN ODU	ODU-AIS	Alarm indication signal or all ones signal	Link down
	ODU-OCI	Open connection error	Link down
	ODU-LCK	ODU lock triggers for path monitoring and TCM levels 1 through 6	Link down
	ODU-BDI	Backward defect indication	Link down
	ODU-TTIM	DAPI or SAPI mismatch from expected to received	Can cause the link to be down if odu-ttim-act-enable is configured at the [edit interfaces <i>interface-name</i> otn-options] hierarchy level
	ODU-IAE	Incoming alignment error	Warning
	ODU-LTC	Loss of tandem connection	Warning
	ODU-CSF	Client signal failure	Warning
	ODU-TSF	Trail signal fail	Warning
	ODU-SSF	Server signal fail	Warning
	ODU-PTIM	Payload type mismatch	Link down

Related Documentation

- [Configuring the 10-Gigabit or 100-Gigabit Ethernet DWDM Interface Wavelength on page 1442](#)

100-Gigabit Ethernet OTN Options Configuration Overview

PTX Series routers support optical transport network (OTN) interfaces, including the 100-Gigabit Ethernet DWDM OTN PIC, and support:

- Transparent transport of two 100-Gigabit Ethernet signals with Optical Channel Transport Unit 4 (OTU4) framing
- International Telecommunications Union (ITU)-standard OTN performance monitoring and alarm management
- Dual polarization quadrature phase shift keying (DP-QPSK) modulation and soft-decision forward error correction (SD-FEC) for long haul and metro applications
- Pre-forward error correction (pre-FEC)-based bit error rate (BER). Fast reroute (FRR) uses the pre-FEC BER as an indication of the condition of an OTN link

Use the **set optics-options** statement at the **[edit interfaces *interfaceType-fpc/pic/port*]** hierarchy level to configure the optics options.

You can optionally configure pre-FEC BER monitoring as a condition for MPLS FRR. Pre-FEC BER FRR uses pre-FEC BER as an indication of the condition of an optical transport network (OTN) link. When the pre-FEC BER degrade threshold is reached, the PIC stops forwarding packets to the remote interface and raises an interface alarm. Ingress packets continue to be processed. When Pre-FEC BER FRR is used with MPLS FRR or another link protection method, traffic is then rerouted to a different interface. The BER threshold and duration for calculating the BER can be configured by the user. Use the **set signal-degrade** statement at the **[edit interfaces *interfaceType-fpc/pic/port* otn-options]** hierarchy level to configure the BER threshold. Use the **set signal-degrade-monitor-enable** statement at the **[edit interfaces *interfaceType-fpc/pic/port* otn-options preemptive-fast-reroute]** hierarchy level to enable signal degrade monitoring.

You can optionally enable backward FRR to inject local pre-FEC status into the transmitted OTN frames, notifying the remote interface. The remote interface then reroutes traffic to a different interface. When you use pre-FEC BER FRR and backward FRR, notification of signal degradation and rerouting of traffic can occur in less time than through a Layer 3 protocol. Use the **set backward-frr-enable** statement at the **[edit interfaces *interfaceType-fpc/pic/port* otn-options preemptive-fast-reroute]** hierarchy level.



NOTE: The backward FRR feature works only between two Juniper Networks 100-Gbps DWDM OTN PICs.

MX2020, MX2010, MX960, MX480, and MX240 routers support OTN interfaces on MPC5E and MPC6E. MPC5E-100G10G and MPC5EQ-100G10G support 100-Gigabit Ethernet OTN interfaces and 10-Gigabit Ethernet OTN interfaces on MX240, MX480, and MX960 routers. The OTN MIC MIC6-100G-CFP2 on MPC6E supports OTN on 100-Gigabit Ethernet interfaces on MX2020 and MX2010 routers. OTN support on the specified MX Series routers includes:

- International Telecommunications Union (ITU)-standard OTN performance monitoring and alarm management
- Transparent transport of two 100-Gigabit Ethernet signals with optical channel transport unit 4 (OTU4) framing.
- Generic forward error correction (Generic FEC)

To configure the OTN options for PTX Series routers and specific MX Series routers, use the **set otn-options** statement at the **[edit interfaces *interfaceType-fpc/pic/port*]** hierarchy level.

Related Documentation

- [Ethernet DWDM Interface Wavelength Overview on page 1380](#)
- [Attenuation and Dispersion in a Fiber-Optic Cable on PTX Series Routers Overview on page 1380](#)
- [Understanding Pre-FEC BER Monitoring and BER Thresholds on page 1381](#)

- [DWDM Controllers Overview on page 1384](#)

Configuring the 10-Gigabit or 100-Gigabit Ethernet DWDM Interface Wavelength

To configure the wavelength on 10-Gigabit Ethernet or 100-Gigabit Ethernet dense wavelength-division multiplexing (DWDM) and OTN interfaces, include the **wavelength** statement at the **[edit interfaces *interface-name* optics-options]** hierarchy level:

```
[edit interfaces interface-name optics-options]
wavelength nm;
```

To display the currently tuned wavelength and frequency for the interface, use the **show interfaces *interface-name*** operational mode command.

For interface diagnostics, issue the **show interfaces diagnostics optics *interface-name*** operational mode command.

[Table 220 on page 1442](#) shows configurable wavelengths and the corresponding frequency for each configurable wavelength.

Table 220: Wavelength-to-Frequency Conversion Matrix

Wavelength (nm)	Frequency (THz)	Wavelength (nm)	Frequency (THz)	Wavelength (nm)	Frequency (THz)
1528.38	196.15	1542.14	194.40	1556.15	192.65
1528.77	196.10	1542.54	194.35	1556.55	192.60
1529.16	196.05	1542.94	194.30	1556.96	192.55
1529.55	196.00	1543.33	194.25	1557.36	192.50
1529.94	195.95	1543.73	194.20	1557.77	192.45
1530.33	195.90	1544.13	194.15	1558.17	192.40
1530.72	195.85	1544.53	194.10	1558.58	192.35
1531.12	195.80	1544.92	194.05	1558.98	192.30
1531.51	195.75	1545.32	194.00	1559.39	192.25
1531.90	195.70	1545.72	193.95	1559.79	192.20
1532.29	195.65	1546.12	193.90	1560.20	192.15
1532.68	195.60	1546.52	193.85	1560.61	192.10
1533.07	195.55	1546.92	193.80	1561.01	192.05

Table 220: Wavelength-to-Frequency Conversion Matrix (continued)

Wavelength (nm)	Frequency (THz)	Wavelength (nm)	Frequency (THz)	Wavelength (nm)	Frequency (THz)
1533.47	195.50	1547.32	193.75	1561.42	192.00
1533.86	195.45	1547.72	193.70	1561.83	191.95
1534.25	195.40	1548.11	193.65	1562.23	191.90
1534.64	195.35	1548.51	193.60	1562.64	191.85
1535.04	195.30	1548.91	193.55	1563.05	191.80
1535.43	195.25	1549.32	193.50	1563.45	191.75
1535.82	195.20	1549.72	193.45	1563.86	191.70
1536.22	195.15	1550.12	193.40	1564.27	191.65
1536.61	195.10	1550.52	193.35	1564.68	191.60
1537.00	195.05	1550.92	193.30	1565.09	191.55
1537.40	195.00	1551.32	193.25	1565.50	191.50
1537.79	194.95	1551.72	193.20	1565.90	191.45
1538.19	194.90	1552.12	193.15	1566.31	191.40
1538.58	194.85	1552.52	193.10	1566.72	191.35
1538.98	194.80	1552.93	193.05	1567.13	191.30
1539.37	194.75	1553.33	193.00	1567.54	191.25
1539.77	194.70	1553.73	192.95	1567.95	191.20
1540.16	194.65	1554.13	192.90	1568.36	191.15
1540.56	194.60	1554.54	192.85	1568.77	191.10
1540.95	194.55	1554.94	192.80		
1541.35	194.50	1555.34	192.75		
1541.75	194.45	1555.75	192.70		

- Related Documentation**
- [100-Gigabit Ethernet OTN Options Configuration Overview on page 1440](#)

CHAPTER 52

Overview of Optical ILAs and IPLCs

- [Optical ILA Hardware Component Overview on page 1445](#)
- [Optical ILA Cooling System Description on page 1446](#)
- [Optical ILA AC Power Supply Description on page 1447](#)
- [Optical ILA DC Power Supply Description on page 1448](#)
- [Optical ILA Chassis Status LEDs on page 1449](#)
- [Optical ILA Component Redundancy on page 1451](#)
- [Optical ILA Field-Replaceable Units on page 1452](#)
- [Optical ILA Management Panel on page 1453](#)
- [Optical ILA Management Port LEDs on page 1454](#)
- [Optical Inline Amplifier Description on page 1455](#)
- [Optical ILA Power Supply LEDs on page 1457](#)
- [PTX3000 IPLC Description on page 1459](#)
- [IPLC Architecture and Functional Components Overview on page 1466](#)
- [Understanding IPLC Base and Expansion Modules on page 1469](#)
- [Understanding the IPLC Configuration on page 1471](#)
- [PTX3000 IPLC LED on page 1477](#)
- [Communication of SNMP Traps Between Optical ILA and NMS Systems on page 1478](#)
- [Communication of SNMPv2 and SNMPv3 Commands over OSC Between an Optical ILA and NMS on page 1478](#)
- [Overview of Configuring and Managing Optical ILAs from Connectivity Services Director Using DMI on page 1479](#)
- [IPLC Specifications on page 1481](#)
- [Understanding the Performance Monitors and TCAs for IPLCs on page 1482](#)

Optical ILA Hardware Component Overview

Table 221 on page 1446 describes the hardware components for the optical ILA.

Table 221: Optical ILA Hardware Components

Component	Spare Model Number
Chassis	PTX-ILA-M-AC
	PTX-ILA-M-DC
Fan module	FAN-ILA-S
Power supplies	JPSU-150-AC-AFO
	JPSU-150-DC-AFO

Related Documentation

- [Optical ILA Cooling System Description on page 1446](#)
- [Optical ILA AC Power Supply Description on page 1447](#)
- [Optical ILA DC Power Supply Description on page 1448](#)
- [Optical ILA Chassis Status LEDs on page 1449](#)

Optical ILA Cooling System Description

The cooling system in an optical ILA consists of three 12.4 W fan modules installed in the field-replaceable unit (FRU) panel and two counter-rotating fans housed in each of the power supplies.

The cooling system brings air into the vents in the front panel and exhausts warmed air through the fans. This type of airflow is known as *airflow out* or *front-to-back* airflow. When installed, the chassis must be positioned so that the FRUs are next to the hot air exhaust.



NOTE: Under normal operating conditions, the fan modules operate at a moderate speed. Temperature sensors in the chassis monitor the temperature within the chassis. The system raises an alarm if a fan module fails or if the ambient temperature inside the chassis rises above the acceptable range.

- [Fan Modules on page 1446](#)

Fan Modules

The fan modules in an optical ILA are hot-removable and hot-insertable FRUs. These fan modules can be hot-swapped—you do not need to power off the optical ILA or disrupt the optical ILA function to replace a fan module. The fan module slots are numbered 0 through 2 from left to right when viewing chassis from the FRU panel side (see [Figure 68 on page 1447](#)). [Figure 69 on page 1447](#) shows the fan module for the optical ILA. The numbers are located on the top-side of the chassis.

Figure 68: Fan Numbering

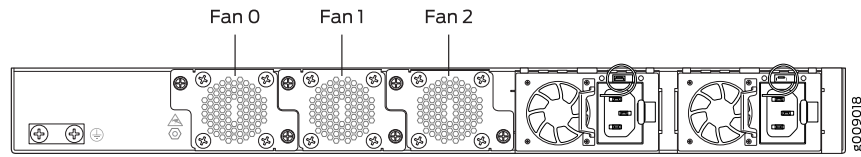
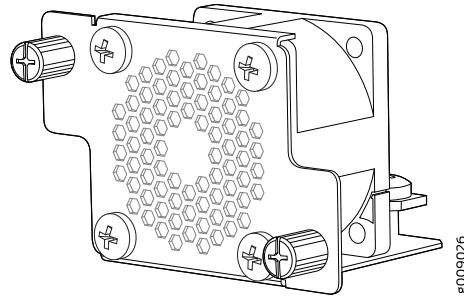


Figure 69: Fan Module



NOTE: All three fan modules must be installed for optimal operation of the optical ILA. The optical ILA continues to operate for a period of time 30 seconds during the replacement of the fan module without thermal shutdown.

Related Documentation

- [Optical ILA Hardware Component Overview on page 1445](#)
- [Optical ILA AC Power Supply Description on page 1447](#)
- [Optical ILA DC Power Supply Description on page 1448](#)
- [Optical ILA Chassis Status LEDs on page 1449](#)

Optical ILA AC Power Supply Description

The AC power supplies in the optical ILA (see [Figure 71 on page 1448](#)) are hot-removable and hot-insertable field-replaceable units (FRUs) that you can install without powering off the optical ILA or disrupting the optical ILA function. The optical ILA has two AC power supplies. Both the power supplies are initially installed at the factory. See [Figure 70 on page 1447](#) for the power numbering scheme, the power supply number is located on the top-side of the chassis.

Figure 70: Power Supply Numbering

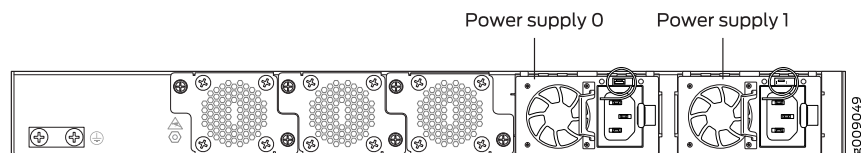
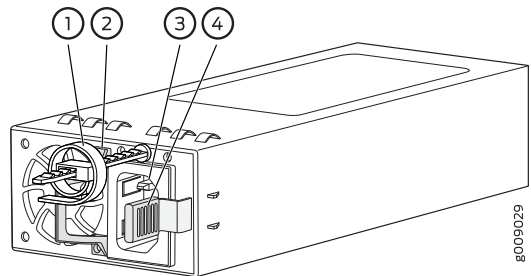


Figure 71: AC Power Supply in an Optical ILA



1— Power cord retainer	3— Male power connector
2— Handle	4— Ejector lever

Each of the 150-W power supplies has a single AC input. The power supply provides 12-VDC output with a standby voltage of 12 VDC. An optical ILA has twice the number of power supplies needed to power all the components in the device, which is known as *1+1 redundancy*. When the optical ILA has both power supplies installed and connected to power, the device has full power redundancy. If a power supply fails or is removed, another power supply balances the electrical load without interruption.

The fans in the power supply provide front-to-back airflow, which is also known as *airflow out (AFO)*.



CAUTION: To avoid electrical injury, carefully follow instructions in *Connecting AC Power to an Optical ILA*, *Installing a Power Supply in an Optical ILA*, and *Removing a Power Supply from an Optical ILA*.

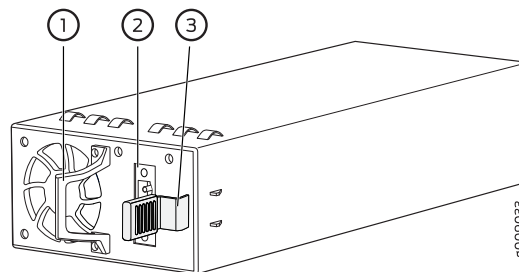
Related Documentation

- [Optical ILA Hardware Component Overview on page 1445](#)
- [Optical ILA Cooling System Description on page 1446](#)
- [Optical ILA DC Power Supply Description on page 1448](#)
- [Optical ILA Chassis Status LEDs on page 1449](#)

Optical ILA DC Power Supply Description

The DC power supplies in the optical ILA (see [Figure 72 on page 1449](#)) are hot-removable and hot-insertable field-replaceable units (FRUs) that you can install without powering off the optical ILA or disrupting the ILA function. The DC version of the optical ILA has two DC power supplies. Both the power supplies are initially installed at the factory.

Figure 72: DC Power Supply in an Optical ILA



1— Handle

2— DC terminal

3— Ejector lever

Each of the two 150-W power supplies has a single DC input. The power supply provides 12 VDC output with a standby voltage of 12 VDC. An optical ILA has twice the number of power supplies needed to power all the components in the device, which is known as *1+1 redundancy*. When the optical ILA has both power supplies installed and connected to power, the device has full power redundancy. If a power supply fails or is removed, the other or second power supply balances the electrical load without interruption.

The fans in the power supply provide port-to-FRU airflow, which is also known as *airflow out (AFO)*.



CAUTION: To avoid electrical injury, carefully follow instructions in *Connecting DC Power to an Optical ILA*, *Installing a Power Supply in an Optical ILA*, and *Removing a Power Supply from an Optical ILA*.



NOTE: We recommend that the 48-VDC facility DC source be equipped with a circuit breaker rated at 10 A (–48 VDC) minimum, or as required by local code.

Related Documentation

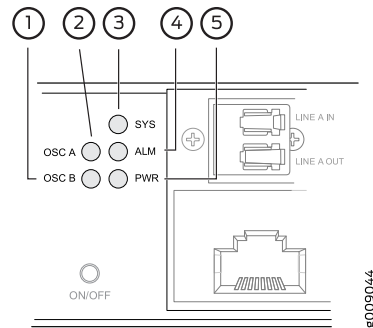
- [Optical ILA Hardware Component Overview on page 1445](#)
- [Optical ILA Cooling System Description on page 1446](#)
- [Optical ILA AC Power Supply Description on page 1447](#)
- [Optical ILA Chassis Status LEDs on page 1449](#)

Optical ILA Chassis Status LEDs

The optical ILA has five status LEDs on the front panel of the chassis (see [Figure 73 on page 1450](#))—two Optical Supervisory Channel status LEDs (OSC A and OSC B), a system status LED (SYS), an alarm LED (ALM), and a power LED (PWR). The OSC is a separate channel that carries overhead information for network management.

purposes. The OSC, which is an important section in every DWDM system, carries voice and data between sites for monitoring and controlling specifications in the system.

Figure 73: Chassis Status LEDs on an Optical ILA



1—OSC B (OSC B) LED	4—Alarm (ALM) LED
2—OSC A (OSC A) LED	5—Power (PWR) LED
3—System status (SYS) LED	

Table 222 on page 1450 describes the chassis status LEDs on an optical ILA.

Table 222: Optical ILA Chassis Status LEDs

Name	Color	State	Description
OSC A status (OSC A) LED	Unlit	Off	The power is off.
	Red	On steadily	No OSC signal is received from the downstream device.
	Amber	On steadily	OSC signal received from the upstream device indicates a fault.
	Green	On steadily	OSC signal is communicating normally.
OSC B status (OSC B) LED	Unlit	Off	The power is off.
	Red	On steadily	No OSC signal is received from the downstream device.
	Amber	On steadily	OSC signal received from the upstream device indicates a fault.
	Green	On steadily	OSC signal is communicating normally.

Table 222: Optical ILA Chassis Status LEDs (continued)

Name	Color	State	Description
System status (SYS) LED	Unlit	Off	The power is off, or the optical ILA is not connected to any power source.
	Green	On steadily	The optical ILA software has booted.
	Green	Blinking	The optical ILA is active and is communicating with upstream and downstream network elements.
Alarm (ALM) LED	Unlit	Off	The optical ILA is off, or there is no alarm.
	Red	On steadily	A major hardware fault has occurred, such as a temperature alarm or a power or pump failure, and the unit has halted. The CLI is still accessible.
	Amber	On steadily	A minor alarm has occurred, such as a software error.
	Green	Solid	The optical ILA is operating properly.
Power (PWR)	Unlit	Off	The optical ILA is powered off or there is no power to the device.
	Amber	On steadily	The optical ILA is powered by a single power supply. The second power supply is either missing or not connected to a power source.
	Green	On steadily	The optical ILA is powered with two redundant power supplies.

Related Documentation

- [Optical ILA Hardware Component Overview on page 1445](#)
- [Optical ILA Cooling System Description on page 1446](#)
- [Optical ILA AC Power Supply Description on page 1447](#)
- [Optical ILA DC Power Supply Description on page 1448](#)

Optical ILA Component Redundancy

The following hardware components provide redundancy on the optical ILA models:

- Cooling system—The optical ILA has three fan modules. Each fan module is a redundant unit containing one fan. If a fan module fails and the remaining fan modules are unable to keep the optical ILA within the desired temperature thresholds, chassis alarms are raised and the optical ILA can shut down.

- The optical ILA ships with two power supplies that provide 1+1 redundancy. If one power supply fails or is removed, the second power supply balances the electrical load without interruption and still provides 1+1 redundancy while the failing power supply is replaced.

Related Documentation

- [Optical ILA Field-Replaceable Units on page 1452](#)
- [Optical ILA Management Panel on page 1453](#)
- [Optical ILA Management Port LEDs on page 1454](#)

Optical ILA Field-Replaceable Units

Field-replaceable units (FRUs) are components that you can replace at your site. The optical ILA FRUs are hot-removable and hot-insertable—you can remove and replace them without powering off the optical ILA or disrupting the optical ILA function.



CAUTION: Replace a failed fan module with a new fan module within 30 seconds of removal to prevent chassis overheating.

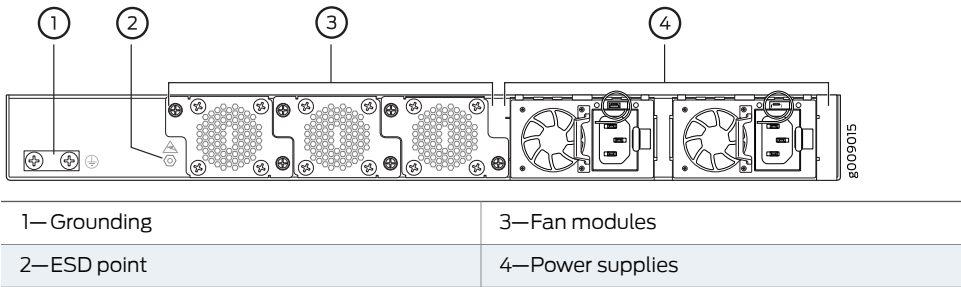
[Table 223 on page 1452](#) lists the FRUs for the optical ILA and actions to take before removing them.

Table 223: Required Actions Before Removing a FRU from the Optical ILA

FRU	Required Actions Before Removal
Power supplies (2)	Disconnect the AC power and remove the AC power cord or cable for the power supply unit. Disconnect the DC power and remove the power connector. NOTE: You need a minimum of one powered power supply for the optical ILA to operate properly..
Fan modules (3)	None.

See [Figure 74 on page 1452](#) shows the FRU panel on an optical ILA.

Figure 74: Optical ILA FRU Panel





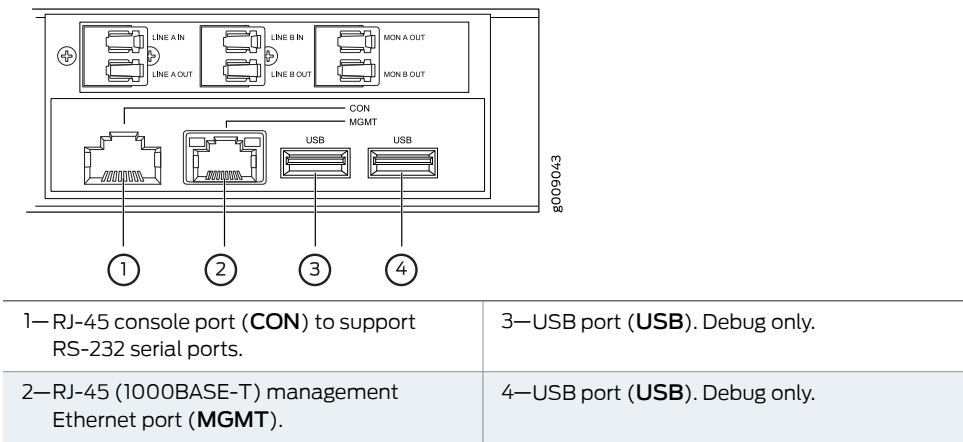
NOTE: If you have a Juniper Care service contract, register any addition, change, or upgrade of hardware components at <https://www.juniper.net/customers/support/tools/updateinstallbase/>. Failure to do so can result in significant delays if you need replacement parts. This note does not apply if you replace existing components with the same type of component.

- Related Documentation
- [Optical ILA Component Redundancy on page 1451](#)
 - [Optical ILA Management Panel on page 1453](#)
 - [Optical ILA Management Port LEDs on page 1454](#)

Optical ILA Management Panel

The optical ILA management panel is found on the front panel (see [Figure 75 on page 1453](#)).

Figure 75: Optical ILA Management Panel Components



You manage the optical ILA by using the command-line interface (CLI), which is accessible through the console and out-of-band management ports on the management panel. In addition, the front panel has system status LEDs that alert you to minor or major alarms or other issues with the amplifier. [Figure 75 on page 1453](#) shows the management panel in detail.

You can also manage the optical ILA through Connectivity Services Director (CSD), which is a Junos Space application developed to manage the optical functionality provided by optical ILAs and integrated photonic line cards (IPLCs) that are installed in the PTX3000 routers. CSD is managed over a data communications network (DCN). CSD presents a topological network view in an intuitive, comprehensive, and cohesive manner that enables you to visualize optical sites, links, and services and a site view that provides status, configuration, alarms/faults, and performance monitoring functionality on the optical interfaces. By using CSD, you can perform the following tasks for an optical ILA:

- View the optical interface specifications that are currently applied on the device, such as wavelength and power.
- Modify the existing parameters of the optical port to suit your network needs or resolve any alarms caused by certain interface settings.
- View the active alarms generated for the optical interface to analyze and resolve the condition that triggered the alarm on the device.
- Configure threshold-crossing alarms (TCAs) for the optical interface.
- View the performance monitoring details in statistical and graphical formats for the optical interface.

Related Documentation

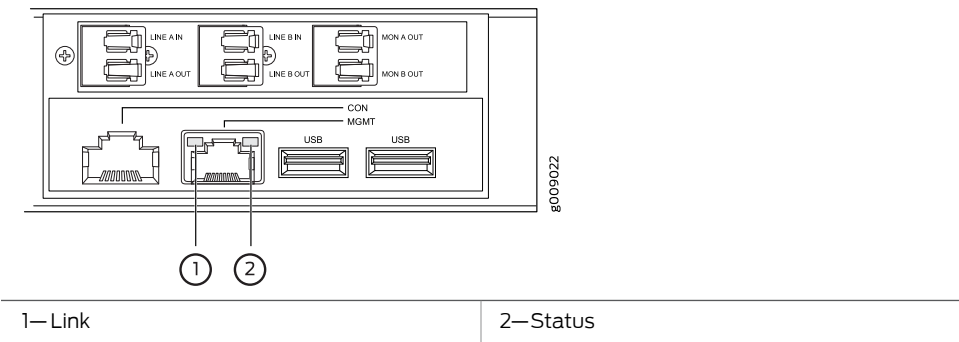
- [Optical ILA Component Redundancy on page 1451](#)
- [Optical ILA Field-Replaceable Units on page 1452](#)
- [Optical ILA Management Port LEDs on page 1454](#)

Optical ILA Management Port LEDs

There is a management port on the optical ILA, located on the management panel. The port is labeled **MGMT**.

The management port is an Ethernet port that supports an RJ-45 connector and has separate LEDs for status and activity. [Figure 76 on page 1454](#) shows the location of the LEDs.

Figure 76: Management Port LEDs on the Optical ILA



[Table 224 on page 1454](#) describes the RJ-45 management port LEDs.

Table 224: Optical ILA RJ-45 Management Port LEDs

LED	Color	State	Description
Link	Unlit	Off	No link is established, there is a fault, or the link is down.
	Yellow	Blinking	A link is established, and there is link activity.

Table 224: Optical ILA RJ-45 Management Port LEDs (continued)

LED	Color	State	Description
Status	Unlit	Off	Link is down.
	Green	On steadily	Link is up.
		Blinking	There is data activity.

- Related Documentation**
- [Optical ILA Component Redundancy on page 1451](#)
 - [Optical ILA Field-Replaceable Units on page 1452](#)
 - [Optical ILA Management Panel on page 1453](#)

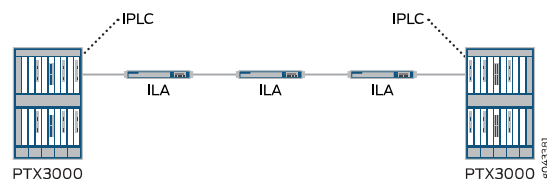
Optical Inline Amplifier Description

The Juniper Networks Optical Inline Amplifier is a fixed stand-alone erbium-doped fiber amplifier (EDFA) with dual AC or DC power supplies. The optical inline amplifier (ILA) supports bidirectional optical inline amplification. The optical ILA provides periodic amplification of a dense wavelength-division multiplexing (DWDM) signal to enable long-distance transmission as it propagates along the fiber. The optical ILA is typically placed between 50 miles (80 km) and 62 miles (100 km) apart along the length of the fiber. The optical ILA is used in conjunction with the integrated photonic line card (IPLC) that is installed in the Juniper Networks PTX3000 Packet Transport Routers.. The optical ILA connects to the IPLC through the **LINE IN** and **LINE OUT** LC port connectors on the front panel. It also connects to other optical ILAs through the LC port connectors.

The optical ILA operates with redundant hot-swappable pluggable power supplies that are either AC or DC. The optical ILA can be managed by using Connectivity Services Director (CSD), or by using the CLI console commands. The optical ILA does not support the Junos operating system (Junos OS).

[Figure 77 on page 1455](#) shows a point-to-point configuration with the optical ILA and IPLC.

Figure 77: Point-to-Point Configuration



In this example, the optical ILA is connected to the IPLC in the PTX3000 chassis, which is connected to compatible PICs in the same chassis through the add and drop ports. The multiplexed wavelengths from the IPLC are amplified and transmitted in a single fiber toward the line (through the **Line OUT** port on the IPLC) which is connected to the optical ILA (through the **LINE IN** port on the ILA). Based on the distance, you can have multiple ILAs connected. In this example, there are three ILAs to enable long-distance

transmission. The amplified signals received by the IPLC in the remote chassis, are demultiplexed into individual wavelengths and sent to the respective add and drop ports (which are connected to the compatible PICs/MICs) in that PTX3000 chassis.

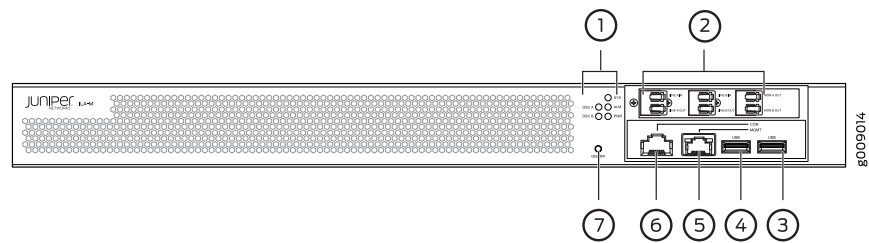
For more information about the IPLCs, see the *PTX3000 Packet Transport Router Hardware Guide*. For information about configuring the IPLCs, see the *Integrated Photonic Line Card (IPLC) Feature Guide*.

- [Front Panel on page 1456](#)
- [FRU Panel on page 1456](#)

Front Panel

The front panel of the optical ILA contains six LC port connectors, the **ON/OFF** button, the console and management ports, the system status LEDs, and the USB ports. [Figure 78 on page 1456](#) shows the front panel of the optical ILA.

Figure 78: Optical ILA Front Panel

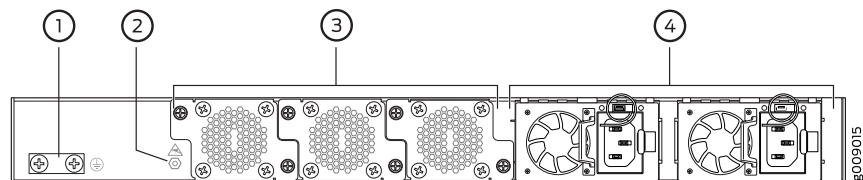


1—Status LEDs	5—Management (MGMT) Ethernet port
2—LC port connectors	6—Console (CON) port
3—USB (USB) port	7—On/off button (ON/OFF)
4—USB (USB) port	

FRU Panel

The field-replaceable unit (FRU) panel of the optical ILA contains the fan modules and power supplies for the optical ILA. [Figure 79 on page 1456](#) shows the optical ILA FRU panel.

Figure 79: Optical ILA FRU Panel



1—Grounding points	3—Fan modules
2—ESD point	4—Power supplies

The cooling system in an optical ILA consists of three 12.4-W fan modules. These fan modules can be hot-swapped—you do not need to power off the optical ILA or disrupt the functioning of the optical ILA to replace a fan module. The optical ILA has two 150-W

power supplies, either AC or DC depending on your configuration. The power supplies need to be both AC or both DC. Only one power supply is required to power the device, while the second power supply provides redundancy.

- Related Documentation
- [Optical ILA Power Supply LEDs on page 1457](#)

Optical ILA Power Supply LEDs

Each optical ILA power supply has two LEDs on the power supply faceplate. [Figure 80 on page 1457](#) shows the location of the LEDs on an optical ILA AC power supply. [Figure 81 on page 1457](#) shows the location of the LEDs on an optical ILA DC power supply.

Figure 80: AC Power Supply LEDs

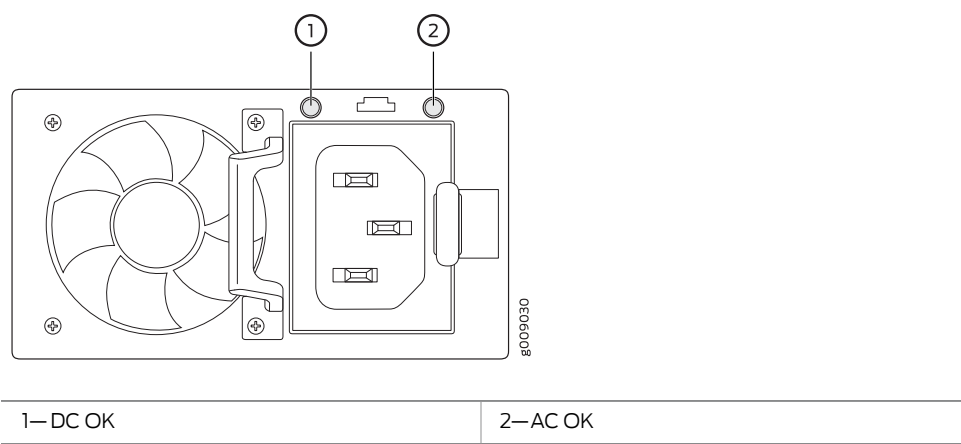
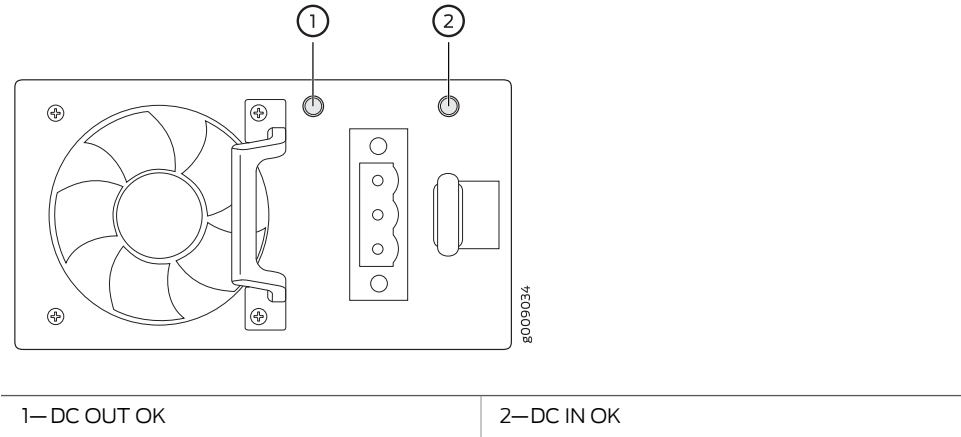


Figure 81: DC Power Supply LEDs



Use [Table 225 on page 1458](#) and [Table 226 on page 1458](#) to interpret the state of the power supply LEDs.

Table 225: Optical ILA AC Power Supply LED

Name	Color	State	Description
DC OK (left side of FRU panel)	Unlit	Off	There is no power to any of the power supplies.
	Green	Blinking (1 Hz)	The power supply is present and only on standby mode.
		On steadily	The power supply output is on and operating correctly.
	Red	On steadily	There is a power supply failure.
		Blinking (0.5 Hz)	No AC power to this power supply only.
AC OK (right side of FRU panel)	Unlit	Off	There is no power to any of the power supplies.
	Green	On steadily	The power supply is present and only on standby mode.
		On steadily	The power supply output is on and operating correctly.
	Red	On steadily	There is a power supply failure.
		Blinking (0.5 Hz)	No AC power to this power supply only.

Table 226: Optical ILA DC Power Supply LED

Name	Color	State	Description
DC OUT OK (left side of FRU panel)	Unlit	Off	There is no power to the power supplies.
	Green	On steadily	The power supply DC output is on and operating correctly.
		Blinking ((1 Hz))	The power supply is present and on standby mode.
	Red	On steadily	There is a power supply failure.
		Blinking (0.5 Hz)	There is no DC power to this power supply only.
DC IN OK (right side of the FRU panel)	Unlit	Off	There is no power to the power supplies.
	Green	On steadily	The power supply is present and on standby mode.
		On steadily	The power supply DC output is on and operating correctly.
	Red	On steadily	There is a power supply failure.
		Blinking (0.5 Hz)	There is no DC power to this power supply only.

Related Documentation • [Optical Inline Amplifier Description on page 1455](#)

PTX3000 IPLC Description

The integrated photonic line card (IPLC) base module (PTX-IPLC-B-32) is an integrated optical card that provides the combined functionalities of optical multiplexing and demultiplexing, optical amplification, optical equalization, and optical channel monitoring. The IPLC multiplexes and enables amplification of up to 32 individual wavelengths for transmission over single-mode optical fiber (through the add and drop ports on the front panel). The add and drop ports on the front panel of the IPLC connect to compatible dense wavelength-division multiplexing (DWDM) PICs or MICs. The wavelengths from the add and drop ports on the IPLC are amplified, monitored, and controlled and then transmitted toward the line direction (through the **Line IN** and **Line OUT** ports on the front panel). In the reverse direction the received signals from the line are amplified to enable long distance transmission and then demultiplexed into individual wavelengths and sent to the respective add and drop ports on the front panel.

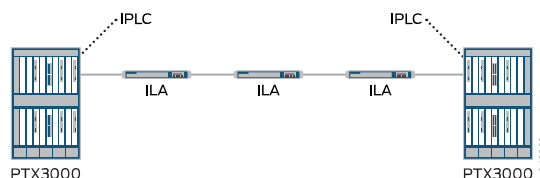
The IPLC expansion module (PTX-IPLC-E-32) is an optical multiplexing and demultiplexing card that interfaces with the IPLC base module to increase the add/drop capacity of the system up to 64 channels.

In a PTX3000 chassis, you can install an IPLC in any of the FPC or PIC slots. The IPLCs install vertically in the front of the PTX3000. Up to 16 IPLCs or 8 base modules and 8 expansion modules are supported in a PTX3000 chassis. Each expansion module must be connected to a base module. The IPLC connects directly to the integrated DWDM PICs/MICs (for example; the P1-PTX-2-100G-WDM or PTX-5-100G-WDM) in the same chassis, or an external chassis through the IPLC front panel add and drop ports. Also, the IPLC can connect to another IPLC in the same chassis through the bi-directional express ports (**XPN IN** and **XPN OUT**) to enable an optical bypass function.

The IPLC can also connect to an optical inline amplifier (ILA) in the network to enable transmission across longer spans. See the *Optical Inline Amplifier Hardware Guide* for more details about the optical ILA.

Figure 82 on page 1459 shows a point-to-point configuration for an IPLC.

Figure 82: Point-to-Point Configuration



In this example, the IPLC in the PTX3000 chassis is connected to compatible PICs in the same chassis through the add and drop ports. The wavelengths from the add and drop ports on the IPLC are multiplexed and then amplified, monitored, and transmitted in a single fiber toward the line (through the **Line OUT** port on the IPLC) and connected to the IPLC (through the **Line IN** port) in the remote PTX3000 chassis through the optical ILA. The IPLC connects to the optical ILA through the **Line IN** and **Line OUT** ports. The optical ILAs provide periodic amplification of the signal to enable long distance

transmission and are typically placed between 50 miles (80 km) and 62 miles (100 km) apart. The signals received by the IPLC in the remote chassis, are demultiplexed into individual wavelengths and sent to the respective add and drop ports (which are connected to the compatible PICs) in that PTX3000 chassis.

For information on configuring the IPLCs, see the *Integrated Photonic Line Card (IPLC) Feature Guide*.

- [IPLC Base Module on page 1460](#)
- [IPLC Expansion Module on page 1463](#)

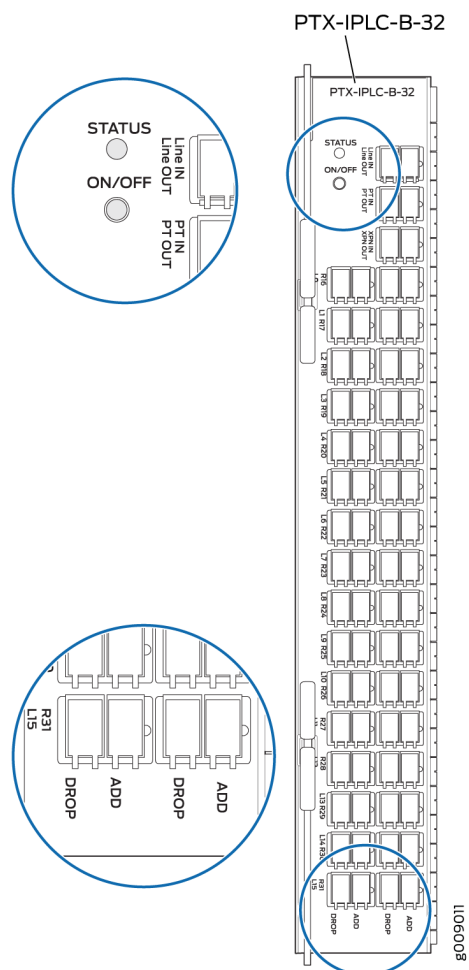
IPLC Base Module

The IPLC base module provides the following optical functions:

- Multiplexing and demultiplexing of up to 32 channels spaced at 100 GHz.
- Amplification of the aggregate multiplexed wavelengths to enable long distance transmission.
- Per channel power monitoring and control through the use of an on-board optical channel monitor (OCM) and wavelength selective switch (WSS).
- Bypass of optical channels between pairs of IPLCs for low-cost optical networking. Two IPLC base modules installed in the same chassis can form an optical bypass. In addition, adding an expansion module (connected to an IPLC base module) can expand the number of channels supported beyond the 32 channels, up to 64 channels.
- Support for the optical supervisory channel (OSC) is transmitted through an OC-3 1510nm signal that enables the IPLC to communicate with the remote IPLC or communicate and manage the optical ILA.

IPLC Base Module Components

Figure 83: IPLC Base Module Faceplate



Each IPLC base module weighs 6.3 lb. (2.85 kg). See [Figure 83 on page 1461](#). The add and drop ports are numbered 0 to 31 and the port numbers are denoted by R and L. For example, as shown in the lower magnified view in [Figure 83 on page 1461](#), L15 refers to the add and drop port on the left side and R31 refers to the add and drop port on the right side on the front panel.

The IPLC base module consists of these components:

- **STATUS** LED that displays the status of the IPLC.
- **ON/OFF** button that resets the IPLC.
- **Line IN** and **Line OUT** ports—An input and an output port to connect to another optical network element. You can use these ports to connect to another IPLC or to the optical ILA.

- **PT IN** and **PT OUT** ports—An input and an output port to connect to an another IPLC base module. Two IPLCs can be installed in the same chassis to form an optical express-in bypass.
- **XPN IN** (expansion-in) and **XPN OUT** (expansion-out) ports—An input and an output port to connect to an IPLC expansion module.
- **ADD** and **DROP** ports—A total of 32 pairs of ports (32 add ports and 32 drop ports) for 32 DWDM channels.



NOTE: All the ports on the IPLC use fiber-optic cables with LC connectors.

Table 227 on page 1462 provides the supported wavelength allocation on the IPLC ports.

Table 227: Supported Wavelength Allocation for the IPLC Base Module (PTX-IPLC-B-32)

Frequency (THz)	Central Wavelength (nm)	Port number on the IPLC Base module
192.05	1561.01	0
192.15	1560.20	1
192.25	1559.39	2
192.35	1558.58	3
192.45	1557.77	4
192.55	1556.96	5
192.65	1556.15	6
192.75	1555.34	7
192.85	1554.54	8
192.95	1553.73	9
193.05	1552.93	10
193.15	1552.12	11
193.25	1551.32	12
193.35	1550.52	13
193.45	1549.72	14
193.55	1548.91	15

Table 227: Supported Wavelength Allocation for the IPLC Base Module (PTX-IPLC-B-32) (continued)

193.65	1548.11	16
193.75	1547.32	17
193.85	1546.52	18
193.95	1545.72	19
194.05	1544.92	20
194.15	1544.13	21
194.25	1543.33	22
194.35	1542.54	23
194.45	1541.75	24
194.55	1540.95	25
194.65	1540.16	26
194.75	1539.37	27
194.85	1538.58	28
194.95	1537.79	29
195.05	1537.00	30
195.15	1536.22	31

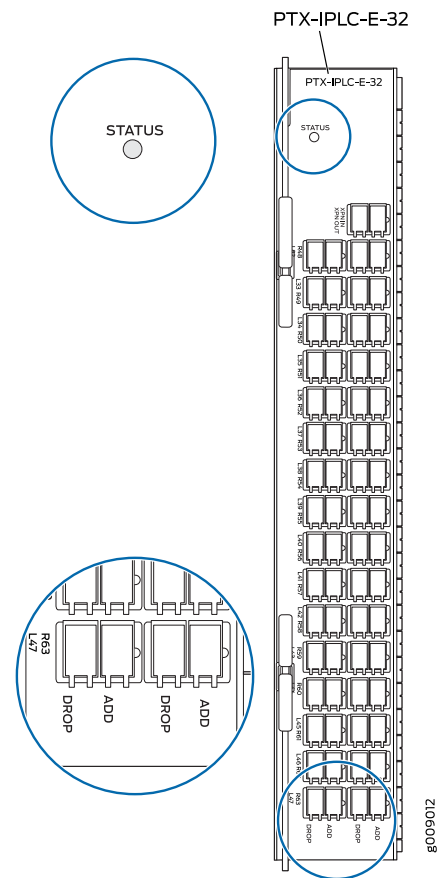
IPLC Expansion Module

The IPLC expansion module connects to the IPLC base module through the **XPN IN** and **XPN OUT** ports. It provides the following optical functions:

- Increases the total optical DWDM channel capacity by 32 ports. It does not interface directly with the network.
- Provides multiplexing and demultiplexing of up to 32 channels spaced at 100 GHz.

IPLC Components

Figure 84: IPLC Expansion Module Faceplate



Each IPLC expansion module weighs 3.3 lb. (1.49 kg). See [Figure 84 on page 1464](#). The add and drop ports are numbered 32 to 64 and the port numbers are denoted by R and L. For example, as shown in the lower magnified view in [Figure 84 on page 1464](#), L47 refers to the add and drop port on the left side and R63 refers to the add and drop port on the right side on the front panel. The IPLC expansion module consists of these components:

- STATUS LED that displays the status of the IPLC.
- **XPN IN** (expansion-in) and **XPN OUT** (expansion-out) ports—A pair of input and output ports to connect to the IPLC base module.
- **ADD** and **DROP** ports—A total of 32 pairs of ports (32 add ports and 32 drop ports) for 32 DWDM channels.



NOTE: All the ports on the IPLC use fiber-optic cables with LC connectors.

[Table 228 on page 1465](#) provides the supported wavelength allocation on the ports.

Table 228: Supported Wavelength Allocation for the IPLC Expansion Module (PTX-IPLC-E-32)

Frequency (THz)	Central Wavelength (nm)	Port number on the IPLC Expansion Module
192.10	1560.61	32
192.20	1559.79	33
192.30	1558.98	34
192.40	1558.17	35
192.50	1557.36	36
192.60	1556.55	37
192.70	1555.75	38
192.80	1554.94	39
192.90	1554.13	40
193.00	1553.33	41
193.10	1552.52	42
193.20	1551.72	43
193.30	1550.92	44
193.40	1550.12	45
193.50	1549.32	46
193.60	1548.51	47
193.70	1547.72	48
193.80	1546.92	49
193.90	1546.12	50
194.00	1545.32	51
194.10	1544.53	52
194.20	1543.73	53
194.30	1542.94	54

Table 228: Supported Wavelength Allocation for the IPLC Expansion Module (PTX-IPLC-E-32) (continued)

Frequency (THz)	Central Wavelength (nm)	Port number on the IPLC Expansion Module
194.40	1542.14	55
194.50	1541.35	56
194.60	1540.56	57
194.70	1539.77	58
194.80	1538.98	59
194.90	1538.19	60
195.00	1537.40	61
195.10	1536.61	62
195.20	1535.82	63

Related Documentation

- [IPLC Architecture and Functional Components Overview on page 1466](#)
- [Understanding IPLC Base and Expansion Modules on page 1469](#)
- [Understanding the IPLC Configuration on page 1471](#)
- [PTX3000 IPLC LED on page 1477](#)

IPLC Architecture and Functional Components Overview

This topic provides an operational and configuration overview of the IPLC.

- [Architecture Overview on page 1466](#)
- [Functional Component Overview on page 1467](#)

Architecture Overview

The IPLC base module accepts and then multiplexes 32 individual wavelengths (connected through the **ADD** and **DROP** ports on the front panel) into a single fiber pair. If you require more than 32 channels, you can connect the optional IPLC expansion module to the IPLC base module to increase the port capacity of the node to 64 ports.

The wavelengths from the **ADD** and **DROP** ports are then amplified, monitored, and controlled and then transmitted towards the optical network over the **Line OUT** port on front panel of the IPLC base module. In the reverse direction, the received signals from the optical network on the **Line IN** port are amplified to overcome for loss in the optical fiber and then demultiplexed into individual wavelengths and sent to the configured **ADD** and **DROP** ports on the front panel.

The 32 channels provided by the IPLC base module are known as the *odd* channels. The 32 channels provided by the optional IPLC expansion module are known as the *even* channels. This odd and even designation reflects the default wavelengths the channels support.

In the multiplexing-add path, the 32 even channels from the IPLC expansion module are interleaved with the 32 odd channels from the IPLC base module. In the demultiplexing-drop path, the 32 even channels are separated from the odd channels using a deinterleaver. All 64 channels go through the main common components used for amplification and equalization. All 32 channels on the IPLC base module are 100 GHz spaced, per the ITU-T Grid Specifications (G.694.1). The 32 channels on the IPLC expansion module are offset from the IPLC base module channels by 50 Hz.

Single Node Two Optical Line Terminations

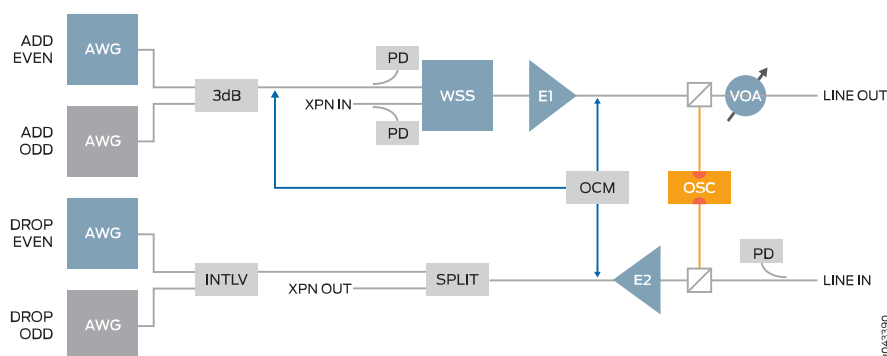
The IPLC architecture can also support two-line terminations on a single node. To form a single node that supports two-line terminations, simply connect two IPLC base modules together through the **PT IN-PT OUT** ports on the front panel and enter a few simple configuration statements in the Junos OS CLI. The IPLC base module and the expansion module each require a single FPC or PIC chassis slot. This minimizes slot requirements and ensures shelf capacity is not sacrificed in single-node east-west or north-south configurations. These minimal slot requirements are especially important if you are configuring a single-node, two-line termination that requires 64 channels using the IPLC expansion modules.

The IPLC base module supports 32 dense wavelength division multiplexing (DWDM) channels. Using the IPLC expansion module, you can increase the number of supported DWDM channels to 64.

Functional Component Overview

The high-level optical functional block diagram of the combined functions of both the IPLC base module and the IPLC expansion module are shown in [Figure 85 on page 1467](#).

Figure 85: Combined Functions of the IPLC Base and Expansion Modules



IPLC Base Module Functional Components

The main building blocks of the IPLC base module architecture are as follows:

- A 2x1 WSS on the add path to select wavelengths from among all channels presented from the 32 add ports of the IPLC base module (shown in blue in [Figure 85 on page 1467](#)) and from the 32 add ports on the IPLC expansion module (shown in gray in [Figure 85 on page 1467](#)).
- A booster erbium-doped fiber amplifier (EDFA) (E1) followed by a variable optical attenuator (VOA) to compensate for the loss of the WSS, multiplexer, and 3 dB coupler.
- A variable gain preamplifier EDFA (E2) to compensate for the loss of the preceding fiber span.
- An optical channel monitor (OCM) with three points of observation including the following:
 - Booster EDFA (E1) output
 - Preamplifier EDFA (E2) output
 - The combined channels of the local add function at the input of the WSS, which indicates which channels (both odd and even channels) are being added locally
 - An optical supervisory channel (OSC), which communicates inband with the far end IPLC modules and is used for the analysis of the fiber span characteristics, performance monitoring, and IPLC fault handing. Simple topology discovery logic communicates with the ILAs and PTX3000 nodes.
- An optical splitter is used to broadcast the received signal from the output of the preamplifier (E2) toward both **DROP** and **PT IN** and **PT OUT** ports
- Four power monitors:
 - **AWG Add**—Monitors the input of the WSS measuring the total input power of the combined channels of the local add function
 - **Express In**—Monitors the input of the WSS measuring the total input power at the input to the WSS coming from the **PT IN** and **PT OUT** express ports
 - **Line IN**—Monitors the input at the **Line IN** port, for detection of the incoming line signal optical power
 - **Line OUT**—Monitors the output at the **Line OUT** port, for detection of the outgoing line signal optical power

IPLC Expansion Module Functional Components

The IPLC expansion module is a passive multiplexer/demultiplexer that interfaces only with the IPLC base module. The IPLC expansion module receives its sole input from and delivers its sole output to the IPLC base module through the **PT IN** and **PT OUT** ports. As such, it does not interface directly with the network or the high-speed backplane of the PTX3000 router. [Figure 85 on page 1467](#) shows the main building blocks for both the IPLC base module and expansion module.

The main building blocks of the IPLC expansion module architecture are as follows:

- Add filter capable of multiplexing 32 DWDM channels of certain wavelengths

- Drop filter capable of demultiplexing 32 DWDM channels having the same certain wavelengths
- Demultiplexing filter whose input (which is also the sole input to the expansion module) is monitored through a power detector. The power detector determines whether light is present. If light is present, the power detector determines whether the light has reached the expansion module through the patch cord between the IPLC base module and the IPLC expansion module.

Related Documentation

- [PTX3000 IPLC Description on page 1459](#)
- [Understanding IPLC Base and Expansion Modules on page 1469](#)
- [Understanding the IPLC Configuration on page 1471](#)
- [PTX3000 IPLC LED on page 1477](#)

Understanding IPLC Base and Expansion Modules

This topic provides an overview of the integrated photonic line card (IPLC) base module and expansion module, and includes the following sections:

- [Overview on page 1469](#)
- [Configuring, Managing, and Monitoring the IPLC on page 1470](#)
- [High Availability, Resiliency, and Integrity on page 1470](#)
- [Usability, Serviceability, Security and Troubleshooting on page 1470](#)
- [Usage Scenarios on page 1471](#)

Overview

The IPLC supports wavelengths up to 100 Gbps and enables ad-hoc allocation of network bandwidth for high-demand, real-time applications, and network services that are delivered over an optical fiber infrastructure. The IPLC base module provides the combined functionality of a 32-port reconfigurable optical add-drop multiplexer (ROADM), optical amplification, optical equalization, and optical channel monitoring on a single card. The IPLC base module also interfaces with the optional IPLC expansion module, which increases the port capacity to 64 add-drop ports.

Figure 86: IPLC Point-to-Point Configuration

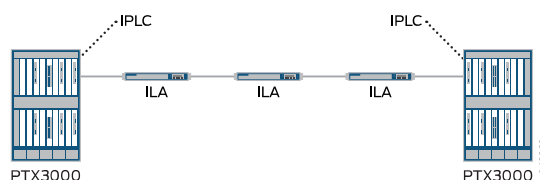


Figure 86 on page 1469 shows a typical IPLC point-to-point configuration. In this configuration, the **Line IN** and **Line OUT** ports on the front of the IPLC base modules are connected to Juniper Networks' optical inline amplifier (ILA) in the optical fiber network.

Optical ILA nodes are typically placed into the network where the fiber length is greater than 80–100 km.

For ring configurations or for other east-west or north-south two-line deployment scenarios, you can connect two IPLC base modules together to form a single-node that consists of two 32-port ROADMs, each with its own line-side fiber span.

Configuring, Managing, and Monitoring the IPLC

You configure, manage, and monitor IPLC modules in a similar fashion to a standard PTX3000 Series interface, by entering a minimum set of CLI commands and making the proper connections between the ports on the IPLC front panel and the PTX Series interfaces.

SNMP

You can also use SNMP to configure the IPLC performance monitor thresholds, and monitor and manage the IPLC modules

Connectivity Services Director

Optionally, you can use the Junos Space Connectivity Services Director to configure, manage, and monitor the IPLC and the optical ILA.

Optical Supervisory Channel

The IPLC uses an in-band optical supervisory channel to communicate with the IPLC expansion module, as well as with remote IPLC modules and optical ILA nodes.

High Availability, Resiliency, and Integrity

Because the IPLC modules do not connect to the PTX Series high-speed backplane, upgrades to the system software and resets do not affect traffic running on the IPLC modules. From an optical perspective, the IPLC modules tolerate both fast and slow changes in physical conditions. For example, if a large number of optical channels disappear due to a fiber cut, the IPLC has sophisticated control circuitry that prevents any errors on the remaining channels. Similarly, slow degradation of the fiber plant is also accommodated to ensure optimal performance across the lifespan of the system.

To ensure error-free transmission across both long fiber runs and large numbers of wavelengths on spans, the IPLC base module automatically controls the power of each channel.

Usability, Serviceability, Security and Troubleshooting

Traditionally, wavelength-division multiplexing (WDM) systems and subsystems have relied on a high degree of manual configuration and fine-tuning from expert users to enable signals to be transmitted error free across the inherently analog medium of optical fiber. The IPLC automates these activities to the point that adding a wavelength is as simple as configuring a port on the router. No optical expertise is required because the IPLC automates the introduction, removal, and balancing of optical channels and you simply need to enable the traffic-carrying port by setting some basic Junos CLI commands.

Unlike traditional WDM systems, the IPLC and optical ILA can accommodate fiber spans between 0 dB and 30 dB with a single hardware variant, simplifying network designs and reducing spare inventory requirements.

WDM networks typically contain many elements and identifying underlying failure points is often complex. With the IPLC, if at any point traffic is interrupted, the system raises a number of alarms to notify the management and control layers of the system and also, to help quickly and easily identify the root cause of the failure.

Performance Monitors

Alarms and analog performance monitors are available to allow expert or non-expert users easily identify and localize faults. Performance monitors monitor analog data and alarms enabling you to quickly view the health of the IPLC. You can quickly and easily configure and enable alarm thresholds at the various monitoring points on the IPLC module.

Usage Scenarios

Optical Bypass Node Configuration

Two IPLCs can be installed in the same shelf to form an Optical Bypass. In addition, should need arise, two Optical Passive Expansion Cards (OPECs) can be added (one connected to each IPLC card). In the latter case, the expansion cards expand the number of channels supported beyond the initial 32 channels.

You can also connect two IPLC modules to form an Optical Bypass node. In this case, the EXPRESS IN and EXPRESS OUT of one card connected to the EXPRESS OUT and EXPRESS IN of the other card respectively.

Optical bypasses are software configurable and controlled through the IPLC's wavelength selective switch (WSS) so there is no need for manual intervention. The IPLCs software optical bypass enables wavelengths that do not terminate on the given node to be passed through to the remote node without optical-electrical-optical (OEO) conversion.

Related Documentation

- [PTX3000 IPLC Description on page 1459](#)
- [IPLC Architecture and Functional Components Overview on page 1466](#)
- [Understanding the IPLC Configuration on page 1471](#)
- [PTX3000 IPLC LED on page 1477](#)

Understanding the IPLC Configuration

This topic describes the basic configuration process for the IPLC modules and includes the following sections:

- [Understanding the Front Panel Connections on page 1472](#)
- [Slot Placement in the Chassis on page 1472](#)

- [Understanding How to Configure the Add and Drop Ports on page 1472](#)
- [Frequency, Wavelength, and Port Default Mapping Configuration on page 1473](#)

Understanding the Front Panel Connections

The IPLC base module and expansion module are slide-in cards that each occupy a single slot within the PTX3000 chassis. Unlike line cards, the IPLC does not connect into the high-speed data backplane of the chassis, but rather provides the following optical functions that you connect through the front panel:

- **Line IN** and **Line OUT** ports—An input and an output port to connect to the optical line system, such as the optical ILA.
- **PT IN** and **PT OUT** ports—An input and an output port to connect to another IPLC base module. You can use these ports to connect two IPLC base modules together to form a single-node that provides two line-side terminations.
- **XPN IN** and **XPN OUT** ports—An input and an output port to connect to an IPLC expansion module
- **ADD** and **DROP** ports—A total of 32 pairs of ports (32 **ADD** ports and 32 **DROP** ports) for 32 DWDM channels

The IPLC modules are designed to connect the **ADD** and **DROP** ports on the front panel to compatible 10-Gigabit or 100-Gigabit DWDM PICs in the same chassis, or to PICs or MICs in a remote chassis.

Slot Placement in the Chassis



BEST PRACTICE: We recommend that you place the IPLC modules into the same FPC/PIC slot pair on the PTX3000 chassis.

The IPLC base module and expansion module each require a single FPC slot. This minimizes slot requirements and ensures that shelf capacity is not sacrificed in single-node east-west or north-south configurations. These slot requirements are especially important if you are configuring a single-node two-line termination that requires 64 channels by using the IPLC expansion modules.

Understanding How to Configure the Add and Drop Ports

The IPLC supports three possible modes of operation for IPLC add and drop ports as follows:

- **blocked**—(Default) If there is no explicit configuration for the IPLC wavelength, the wavelength is in blocked mode.
- **switch**—Switches the specified IPLC wavelength to an optical interface on the same or different chassis, including a remote chassis.

To switch a wavelength to an optical interface on the same chassis, enter the following in the CLI:


```
user@host# set chassis fpc fpc-slot optical-options wavelength nm switch
interface-name
```

To switch a wavelength to an optical interface on a remote chassis, enter the following in the CLI:

```
user@host# set chassis fpc fpc-slot optical-options wavelength nm switch remote
```

- **wss-express-in**—Optically bypass the specified wavelength. For example to configure wavelength 1550.12 on the IPLC in slot 1 to be bypassed:

```
user@host# set chassis fpc 1 optical-options wavelength 1550.12 wss-express-in
```

Configuring a wavelength in express-in mode is a two-step process. First, you must define the association between the two IPLCs and then you specify the wavelength. For example, the following configuration creates the association between the two IPLC modules in slot 1 and slot 6:

```
user@host# set chassis fpc 1 optical-options express-in fpc 6
```

After you create the association between the two IPLCs, you must configure the wavelengths in express-in mode, in either one of the IPLC slots. For example:

```
user@host# set chassis fpc 1 optical-options wavelength nm wss-express-in
user@host# set chassis fpc 6 optical-options wavelength nm wss-express-in
```

The preceding statements configure wavelength1 and wavelength 2 in express-in mode for IPLCs modules in slot 1 and slot 6.

Frequency, Wavelength, and Port Default Mapping Configuration

All port wavelength frequencies are controlled by the IPLC's WSS and configured on a wavelength-by-wavelength basis. [Table 229 on page 1473](#) lists the default port, frequency, and wavelength mapping for both of the IPLC modules.

Table 229: Default Port, Frequency, and Wavelength Mapping

Frequency [THz]	Central Wavelength [nm]	Present on IPLC Module	Label on IPLC Module	Present on IPLC Expansion Module	Label on IPLC Expansion Module
192.05	1561.01	Yes	0	No	No
192.1	1560.61	No	No	Yes	32
192.15	1560.2	Yes	1	No	No
192.2	1559.79	No	No	Yes	33
192.25	1559.39	Yes	2	No	No

Table 229: Default Port, Frequency, and Wavelength Mapping (continued)

Frequency [THz]	Central Wavelength [nm]	Present on IPLC Module	Label on IPLC Module	Present on IPLC Expansion Module	Label on IPLC Expansion Module
192.3	1558.98	No	No	Yes	34
192.35	1558.58	Yes	3	No	No
192.4	1558.17	No	No	Yes	35
192.45	1557.77	Yes	4	No	No
192.5	1557.36	No	No	Yes	36
192.55	1556.96	Yes	5	No	No
192.6	1556.55	No	No	Yes	37
192.65	1556.15	Yes	6	No	No
192.7	1555.75	No	No	Yes	38
192.75	1555.34	Yes	7	No	No
192.8	1554.94	No	No	Yes	39
192.85	1554.54	Yes	8	No	No
192.9	1554.13	No	No	Yes	40
192.95	1553.73	Yes	9	No	No
193	1553.33	No	No	Yes	41
193.05	1552.93	Yes	10	No	No
193.1	1552.52	No	No	Yes	42
193.15	1552.12	Yes	11	No	No
193.2	1551.72	No	No	Yes	43
193.25	1551.32	Yes	12	No	No
193.3	1550.92	No	No	Yes	44
193.35	1550.52	Yes	13	No	No
193.4	1550.12	No	No	Yes	45

Table 229: Default Port, Frequency, and Wavelength Mapping (continued)

Frequency [THz]	Central Wavelength [nm]	Present on IPLC Module	Label on IPLC Module	Present on IPLC Expansion Module	Label on IPLC Expansion Module
193.45	1549.72	Yes	14	No	No
193.5	1549.32	No	No	Yes	46
193.55	1548.91	Yes	15	No	No
193.6	1548.51	No	No	Yes	47
193.65	1548.11	Yes	16	No	No
193.7	1547.72	No	No	Yes	48
193.75	1547.32	Yes	17	No	No
193.8	1546.92	No	No	Yes	49
193.85	1546.52	Yes	18		
193.9	1546.12	No	No	Yes	50
193.95	1545.72	Yes	19	No	No
194	1545.32	No	No	Yes	51
194.05	1544.92	Yes	20	No	No
194.1	1544.53	No	No	Yes	52
194.15	1544.13	Yes	21	No	No
194.2	1543.73	No	No	Yes	53
194.25	1543.33	Yes	22	No	No
194.3	1542.94	No	No	Yes	54
194.35	1542.54	Yes	23	No	No
194.4	1542.14	No	No	Yes	55
194.45	1541.75	Yes	24	No	No
194.5	1541.35	No	No	Yes	56
194.55	1540.95	Yes	25	No	No

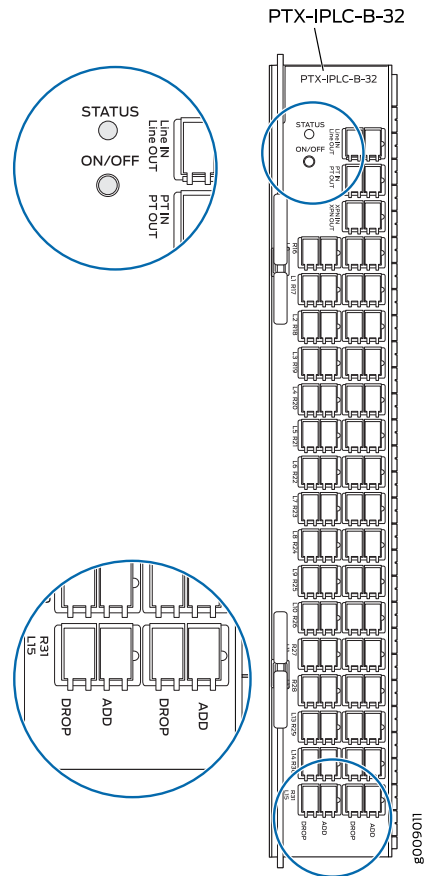
Table 229: Default Port, Frequency, and Wavelength Mapping (continued)

Frequency [THz]	Central Wavelength [nm]	Present on IPLC Module	Label on IPLC Module	Present on IPLC Expansion Module	Label on IPLC Expansion Module
194.6	1540.56	No	No	Yes	57
194.65	1540.16	Yes	26	No	No
194.7	1539.77	No	No	Yes	58
194.75	1539.37	Yes	27	No	No
194.8	1538.98	No	No	Yes	59
194.85	1538.58	Yes	28	No	No
194.9	1538.19	No	No	Yes	60
194.95	1537.79	Yes	29	No	No
195.00	1537.40	No	No	Yes	61
195.05	1537.00	Yes	30	No	No
195.10	1536.61	No	No	Yes	62
195.15	1536.22	Yes	31	No	No
195.20	1535.82	No	No	Yes	63

- Related Documentation**
- [PTX3000 IPLC Description on page 1459](#)
 - [IPLC Architecture and Functional Components Overview on page 1466](#)
 - [Understanding IPLC Base and Expansion Modules on page 1469](#)
 - [PTX3000 IPLC LED on page 1477](#)

PTX3000 IPLC LED

Figure 87: IPLC LED



An IPLC base module and an IPLC expansion module each has one LED—labeled **STATUS**. [Table 230 on page 1477](#) describes the functions of the LED.

Table 230: PTX3000 IPLC LED

Label	Color	State	Description
STATUS	Green	On steadily	IPLC is online.
		Blinking	IPLC is booting.
	Red	On steadily	IPLC is in a failed state.
		Off	IPLC is offline.

- Related Documentation**
- [PTX3000 IPLC Description on page 1459](#)
 - [IPLC Architecture and Functional Components Overview on page 1466](#)

- [Understanding IPLC Base and Expansion Modules on page 1469](#)
- [Understanding the IPLC Configuration on page 1471](#)

Communication of SNMP Traps Between Optical ILA and NMS Systems

SNMP traps are required to be propagated from an optical ILA to the network management system (NMS) server such as Connectivity Services Director. Each optical ILA needs to be able to configure trap destinations. Because an IPLC acts as a gateway, the traps are first received by the IPLC. From the IPLC, these traps are transmitted to the appropriate destination. The IPLC maintains information about the trap destination configuration per optical ILA. The optical ILA sends its traps to the anchor IPLC by default. The following traps are available from optical ILA:

- Temperature (abnormal, clear)
- Voltage (abnormal, clear)
- Fan temperature/speed (abnormal, clear)
- Software version (abnormal, clear)
- Optical ILA communication (abnormal, clear)
- EDFA temperature
- EDFA RFL
- Pump trap

Related Documentation

- [Communication of SNMPv2 and SNMPv3 Commands over OSC Between an Optical ILA and NMS on page 1478](#)
- [Overview of Configuring and Managing Optical ILAs from Connectivity Services Director Using DMI on page 1479](#)
- [IPLC Specifications on page 1481](#)
- [Understanding the Performance Monitors and TCAs for IPLCs on page 1482](#)

Communication of SNMPv2 and SNMPv3 Commands over OSC Between an Optical ILA and NMS

Each optical LA device has two bidirectional optical interfaces carrying the optical supervisory channel (OSC). The OSC signal (OC3) from two OSC ports is sent to the OSC field-programmable gate array (FPGA). The OSC FPGA creates Ethernet packets and sends them to a BCM or internal Gigabit Ethernet interface. The OSC traffic from two SFP 0/1 ports is multiplexed to processor Gigabit Ethernet interface (for example, port 3). The software uses the Gigabit Ethernet interface driver to transmit and receive OSC packets. The front panel RJ45 is also connected to the BCM switch. This interface can also be used for management. Both OSC and front panel RJ45 can be used simultaneously. The management packets from RJ45 interface are separated from OSC

management packets. These can be sent over separate CPU GbE interface (for example, port 2 of BCM switch) by maintaining port 1 and port 2 in a VLAN.

Each optical ILA is connected to other ILAs and IPLC using optical ports. There are two optical ports for each optical ILA, designated as OSC A and OSC B. For IP connectivity over OSC, IPLC is used as a gateway. There is no direct IP connectivity between the optical ILA and external servers. The NMS server, such as Connectivity Services Director, sends the SNMP commands meant for an optical ILA to the Routing Engine of the PTX3000 router, with community string indicating the destination optical ILA. The mapping of optical ILA and SNMP community string is configured using the Junos OS CLI interface.

- Related Documentation**
- [Overview of Configuring and Managing Optical ILAs from Connectivity Services Director Using DMI on page 1479](#)
 - [IPLC Specifications on page 1481](#)
 - [Understanding the Performance Monitors and TCAs for IPLCs on page 1482](#)

Overview of Configuring and Managing Optical ILAs from Connectivity Services Director Using DMI

Connectivity Services Director uses the Juniper Networks Device Management Interface (DMI) to the managed devices to collect the data. If you have a Junos Space fabric, Connectivity Services Director balances the load of polling the managed devices across the nodes in the fabric. Direct SNMP communication is absent between the NMS server such as Connectivity Services Director and the optical ILA because of IPLC design.

The requirements from Connectivity Services Director are as follows:

- Connectivity Services Director needs to be able to retrieve the optical ILA performance, fault, and image-upgrade status. In addition, Connectivity Services Director must be able to send configuration and upgrade commands to the optical ILA. IPLC can set or get the optical ILA configuration and management parameters through SNMP (or any other method), save them locally and expose these through the Junos OS CLI. Connectivity Services Director is able to access these parameters through DMI.
- This implementation requires an optical ILA management client in optical ILA and optical ILA management server in IPLC. The management server queries the parameters periodically. Similarly, the CLI commands are used to set parameters related to optical ILA and initiate operations such as upgrade, which are sent as SNMP messages to the optical ILA client.

The following are examples of various configuration settings, and Set and Get operations required on an optical ILA.

Configuration Settings Performed Using the CLI

- Saving configuration
- Restoring configuration
- Resetting the OS

- Starting the firmware upgrade
- Restoring EDFA defaults
- Resetting the EDFA

Set Parameters for SNMP

- Temperature threshold parameters
- Addition and deletion of SNMP users
- Mode configuration (auto or debug)
- EDFA parameters (such as mode, gain, tilt, and LOS action)
- Optical power parameters (input and output LOS thresholds, and LOS hysteresis)
- OSC parameters (enable, add or drop power value, thresholds, and LOS hysteresis)

Get Parameters for SNMP

- Optical ILA part number, serial number, and uptime
- Temperature
- Fan speed
- Firmware upgrade status
- SNMP user information
- Mode EDFA (module type, part number, working status, gain, and temperature)
- Optical power (input power and output power)
- VOA attenuation
- OSC (index)

Alarms

- Viewing active alarms
- Viewing historical alarms

Related Documentation

- [Communication of SNMP Traps Between Optical ILA and NMS Systems on page 1478](#)
- [Communication of SNMPv2 and SNMPv3 Commands over OSC Between an Optical ILA and NMS on page 1478](#)
- [IPLC Specifications on page 1481](#)
- [Understanding the Performance Monitors and TCAs for IPLCs on page 1482](#)

IPLC Specifications

The Integrated Photonic Line Card (IPLC) is designed to be installed in a PTX3000 router chassis. Architecturally, this card can be plugged into either the FPC or the PIC slot. For control and management purposes, the card behaves exactly similar to an FPC in the PTX3000 router. IPLC uses the same Processor Mezzanine Board (PMB) as the PTX Series router FPCs, although not as a daughter card. Due to mechanical and physical considerations, the PMB is designed onto the card directly. The card supports 100G wavelengths, and contains 32 ports on the faceplate. The IPLC uses an extension card to support an additional 32 ports. The IPLC might also have external DCMs to compensate for incoming dispersion on 10G wavelengths.

The IPLC also supports an OSC channel. This is an in-band channel used to communicate with ILAs and other optical nodes in the line system that are not directly accessible over the Data Communications Network (DCN). DCN is an ITU terminology for a device that provides network telemetry to remote network elements for the purpose of operations and network element management. OSC framing logic is implemented in the FPGA. Performance monitoring of analog data and alarms is supported.

You can set an explicit configuration to associate an IPLC with an expansion card, to increase the number of ports from 32 to 64. You can add an expansion card to the residing on the same chassis. There can be only one association between one IPLC and one expansion card. For example, the IPLC in slot 0 can be associated with expansion card in slot 2. After IPLC slot 0 is associated with expansion card in slot, you cannot create another association between IPLC slot 0 and expansion card in slot 4. This setting is disallowed at the CLI configuration level itself. A corresponding alarm is triggered and an SNMP trap generated on a failure condition.

With only the specification of the configuration settings, it is not guaranteed that the express-in association are added to an optical IPLC. Junos OS needs to validate if the express-in port on the optical IPLC has been connected to the express-in port of the valid IPLC's express-in port, and the express-in ports are UP on both the IPLCs. Only after the validation is successful, express-in ports are moved to the UP state on the optical IPLC. A corresponding alarm is triggered and an SNMP trap is generated on a failure condition.

Related Documentation

- [Communication of SNMP Traps Between Optical ILA and NMS Systems on page 1478](#)
- [Communication of SNMPv2 and SNMPv3 Commands over OSC Between an Optical ILA and NMS on page 1478](#)
- [Overview of Configuring and Managing Optical ILAs from Connectivity Services Director Using DMI on page 1479](#)

Understanding the Performance Monitors and TCAs for IPLCs

Performance monitors enable you to examine and diagnose the health, working capacity, operational efficiency, and the traffic-handling condition of the integrated photonic line cards modules (IPLCs) at various points on the optical IPLC hardware. You can enable configure threshold-crossing alarms (TCA) for the optical IPLC performance monitors. TCAs are alarms that are activated when a certain configurable threshold—near-end measurement threshold or far-end measurement threshold—is crossed and remains so for 15 minutes

The IPLC supports the optical performance monitors listed in [Table 231 on page 1482](#).

Table 231: IPLC Optical Performance Monitors

Performance Monitor	15 Min Bin	24 Hr Bin	TCA High	TCA Low
OSC TX power	Yes	Yes	Yes	Yes
OSC RX power	Yes	Yes	Yes	Yes
OSC/FPGA estimated fiber loss	Yes	Yes	No	No
Line OUT VOA attenuation	Yes	Yes	Yes	Yes
EDFA Input power (for both EDFAs)	Yes	Yes	Yes	Yes
EDFA Output power (for both EDFAs)	Yes	Yes	Yes	Yes
EDFA Signal output power (for both EDFAs)	Yes	Yes	Yes	Yes
EDFA Pump current (for both EDFAs)	Yes	Yes	Yes	Yes
EDFA Pump temperature (for both EDFAs)	Yes	Yes	Yes	Yes
OCM power readings (96 channels x 1 monitoring points)	Yes	Yes	Yes	Yes
Power monitor at ADD port	Yes	Yes	Yes	Yes
Power monitor at EXPRESS IN port	Yes	Yes	Yes	Yes

Each performance monitor supports:

- 15-minute and 24-hour binning
- Low and high threshold levels as described in [Table 232 on page 1483](#).

Table 232: IPLC Threshold Crossing Alert Minimum and Maximum Values

TCA	Description	Granularity	Range Minimum/Maximum Default and Recommended Value
erbium-doped fiber amplifier (EDFA) Input Power (for Both EDFAs)			
edfa1-awg-high-tca	Ingress EDFA pump AWG high TCA	5s	390/440 mW 400 mW
edfa1-awg-low-tca	Ingress EDFA pump AWG low TCA		5/15 mW 5 mW
edfa1-express-high-tca	Ingress EDFA pump express high TCA		390/440 mW 400 mW
edfa1-express-low-tca	Ingress EDFA pump express low TCA		5/15 mW 5 mW
edfa1-in-power-high-tca	Ingress EDFA input power high TCA	0.5s	10/12 dBm 11 dBm
edfa1-in-power-low-tca	Ingress EDFA input power low TCA		−38/−34 dBm −35 dBm
edfa1-out-power-high-tca	Ingress EDFA output power high TCA		20/21 dBm 20.5 dBm
edfa1-out-power-low-tca	Ingress EDFA output power low TCA		−1/0.5 dBm
edfa1-pump-current-high-tca	Ingress EDFA pump current high TCA	1s	10/300 mA
edfa1-pump-current-low-tca	Ingress EDFA pump current low TCA		
edfa1-pump-temp-high-tca	Ingress EDFA pump temperature high TCA	0.1s	20°/25° C
edfa1-pump-temp-low-tca	Ingress EDFA pump temperature low TCA		
edfa1-sig-power-high-tca	Ingress EDFA signal power high TCA	0.5s	10/12 dBm 11 dBm
edfa1-sig-power-low-tca	Ingress EDFA signal power low TCA >		−39/−35 dBm −36 dBm

Table 232: IPLC Threshold Crossing Alert Minimum and Maximum Values (continued)

TCA	Description	Granularity	Range Minimum/Maximum Default and Recommended Value
erbium-doped fiber amplifier (EDFA) Input Power (for Both EDFAs)			
erbium-doped fiber amplifier (EDFA) Output Power (for Both EDFAs)			
edfa2-awg-high-tca	Egress EDFA pump AWG high TCA	5s	390/440 mW 400 mW
edfa2-awg-low-tca	Egress EDFA pump AWG low TCA		5/15 mW 5 mW
edfa2-express-high-tca	Egress EDFA pump express high TCA		390/440 mW 400 mW
edfa2-express-low-tca	Egress EDFA pump express low TCA		5/15 mW 5 mW
edfa2-in-power-high-tca	Egress EDFA input power high TCA	0.5s	10/12 dBm 11 dBm
edfa2-in-power-low-tca	Egress EDFA input power low TCA		−38/−34 dBm −35 dBm
edfa2-out-power-high-tca	Egress EDFA output power high TCA		20/21 dBm 20.5 dBm
edfa2-out-power-low-tca	Egress EDFA output power low TCA		−1/0.5 dBm −0.5 dBm
edfa2-pump-current-high-tca	Egress EDFA pump current high TCA	1s	10/300 mA
edfa2-pump-current-low-tca	Egress EDFA pump current low TCA		
edfa2-pump-temp-high-tca	Egress EDFA pump temperature high TCA	0.1s	20°/25° C
edfa2-pump-temp-low-tca	Egress EDFA pump temperature low TCA		

Table 232: IPLC Threshold Crossing Alert Minimum and Maximum Values (continued)

TCA	Description	Granularity	Range Minimum/Maximum Default and Recommended Value
erbium-doped fiber amplifier (EDFA) Input Power (for Both EDFAs)			
edfa2-sig-power-high-tca	Egress EDFA signal power high TCA	0.5s	10/12 dBm 11 dBm
edfa2-sig-power-low-tca	Egress EDFA signal power low TCA		−39/−35 dBm −36 dBm
Line OUT Variable Optical Attenuation (VOA)			
lout-voa-high-tca	LOUT VOA high TCA	0.5	16/25 dBm 17 dBm
lout-voa-low-tca	LOUT VOA low TCA	N/A	N/A
Optical Channel Monitor (OCM) Power Readings (96 channels x 1 Monitoring Points)			
ocm-power-high-line-out-tca	OCM Power Line Out high TCA	0.5 dBm	1/2 dBm per channel 1.5 dBm per channel <i>NOTE:</i> Assumes VOA setting =0
ocm-power-low-line-out-tca	OCM Power Line Out low TCA		−2/−1 dBm per channel −1.5 dBm per channel <i>NOTE:</i> Assumes VOA setting =0
Optical Supervisory Channel (OSC) Estimated Fiber Loss			
osc-fiber-loss-high-tca	OSC fiber loss high TCA	0.5 dB	36/39 dB 37 dB
osc-fiber-loss-low-tca	OSC fiber loss low TCA	N/A	N/A
Optical Supervisory Channel (OSC) RX Power			
osc-rx-power-high-tca	OSC RX power high TCA	0.5 dBm	5/7 dBm 6 dBm
osc-rx-power-low-tca	OSC RX power low TCA		−47/−46 dBm −46 dBm

Table 232: IPLC Threshold Crossing Alert Minimum and Maximum Values (continued)

TCA	Description	Granularity	Range Minimum/Maximum Default and Recommended Value
erbium-doped fiber amplifier (EDFA) Input Power (for Both EDFAs)			
Optical Supervisory Channel (OSC) TX Power			
osc-tx-power-high-tca	OSC TX power high TCA	0.5 dBm	5.5/7 dBm 6 dBm
osc-tx-power-low-tca	OSC TX power low TCA		−2/−0.5 dBm −1 dBm

**Related
Documentation**

- [Communication of SNMP Traps Between Optical ILA and NMS Systems on page 1478](#)
- [Communication of SNMPv2 and SNMPv3 Commands over OSC Between an Optical ILA and NMS on page 1478](#)
- [Overview of Configuring and Managing Optical ILAs from Connectivity Services Director Using DMI on page 1479](#)

CHAPTER 53

Configuring and Monitoring Optical Interfaces, OTUs, and ODUs

- [Viewing a Graphical Image of the Optical Interface Components on page 1487](#)
- [Configuring and Managing OTN Port Details of MX Series and PTX Series Routers for Easy Administration on page 1497](#)
- [Configuring and Managing OTU Details of MX Series and PTX Series Routers for Simplified Management on page 1505](#)
- [Configuring and Managing ODU Details of MX Series and PTX Series Routers for Simplified Management on page 1512](#)
- [Configuring and Managing Optical PIC Details for Effective Provisioning on page 1517](#)
- [Configuring Threshold-Crossing Alarms for OTN Ports for Monitoring Link Performance on page 1519](#)
- [Configuring Threshold-Crossing Alarms for OTUs for Monitoring Link Performance on page 1523](#)
- [Configuring Threshold-Crossing Alarms for ODUs for Monitoring Link Performance on page 1527](#)
- [Viewing Performance Monitoring Details of OTN Ports for Detecting and Diagnosing Faults on page 1530](#)
- [Viewing Performance Monitoring Details of OTUs for Detecting and Diagnosing Faults on page 1541](#)
- [Viewing Performance Monitoring Details of ODUs for Detecting and Diagnosing Faults on page 1549](#)
- [Viewing a Graphical Image of the Chassis of PTX Series Routers on page 1556](#)
- [Diagnosing, Examining, and Correcting Optical Interface Problems on page 1561](#)
- [Changing Alarm Settings for the Optics and OTN Interfaces on page 1565](#)

Viewing a Graphical Image of the Optical Interface Components

The Chassis View provides a pictorial representation of the optical interface, optical channel data unit (ODU), optical channel transport unit (ODU) of an MX Series and PTX Series router, and the modules or components that are installed in it, such as the line cards, interfaces, and other hardware elements.

The purpose of this view is to try and provide a comprehensive monitoring view of the health and status of deployed devices across the network. In this view all the managed devices are shown with their appropriate status and health based on the services and device settings applied. This view helps the operator to know the health and status across the network, it provides with the operator to quickly see the macro level information, which allows the operator to further analyze the information provided and quickly navigate to individual devices and take any further corrective measure required. It provides a cohesive tool for the operator to quickly see the micro-level information and take any further remediation action required.

To view a graphical image of the optical interfaces, OTUs, and ODUs of MX Series and PTX Series routers, and its associated components:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the device for which you want to define the optical port settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. Click a particular component or interface to display the associated details in the lower portion of the page. The Rotate and Perspective buttons enable you to view the images in required orientation.

6. Click the View Back (arrows in a square symbol) icon to cause the device image to rotate along the x-axis and display the rear view of the device. Alternatively, click the View Front icon to view the front plane of the device. The View Back and View Front icons are toggle options.

7. Click the Perspective (cube symbol) icon to display the device image in three-dimensional format. It is a toggle button, which causes the device image to be shown in either three-dimensional or one-dimensional format.

8. Select the level of magnification of the image by clicking the Zoom (magnifying glass) icon. The image is expanded and displayed.

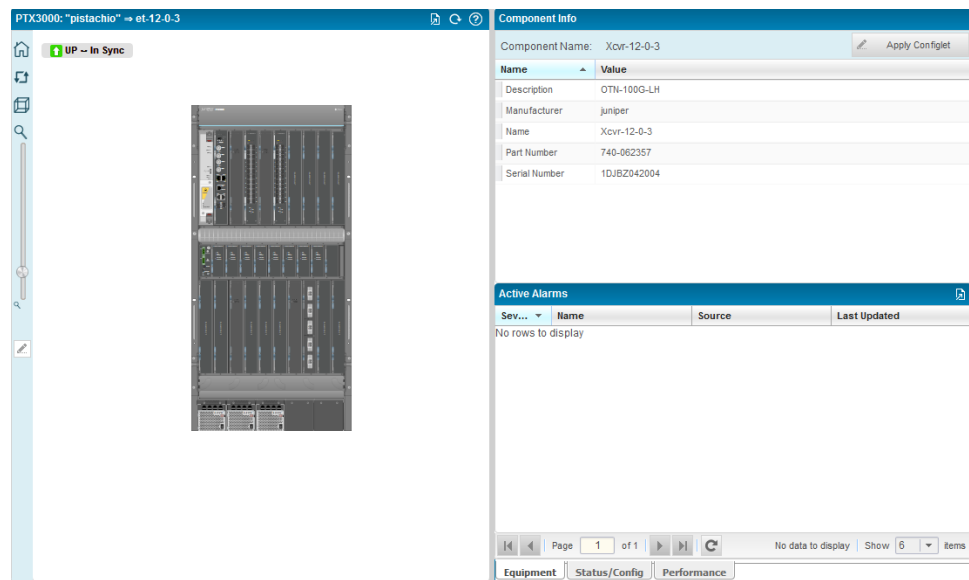
Alternatively, use the slider control beneath the Zoom icon to change the level of magnification.

9. Click the home icon to return to the front view of the chassis.

The selected interface is surrounded with a colored outline based on the operational status. An interface that is operationally up is denoted in green and an interface that is operationally down is represented in red. The components are depicted as small colored icons at the top-left corner of the front view of the equipment image.

In the graphical image of the device displayed as shown in [Figure 88 on page 1489](#), you can mouse over the different parts of the device, such as the interfaces, line cards, and slots. When you mouse over the different modules, their corresponding details are displayed as tooltips. On clicking the device components, the corresponding description for the selected component is displayed by default in the Component Info pane and the Equipment tab with the following values.

Figure 88: Chassis View of a PTX Series Router with an OTN MIC



- Manufacturer—Name of the company that built and shipped the device.
- Part number—Part number of the chassis component.
- Serial number—Serial number of the chassis component. The serial number of the backplane is also the serial number of the router or switch chassis. Use this serial number when you need to contact Juniper Networks Customer Support about the router or switch chassis.

When you select any physical interface configured on the DPCs or PICs or MICs provisioned, the following fields are displayed for the corresponding component for each interface. The interface is surrounded by a colored box to show the Operational Status.

The Component Info pane and the Active Alarms monitor are displayed in the lower portion of the page.

The Active Alarms monitor shows any active alarm that has not yet been cleared. You can view the alarm name, the unique identifier assigned to the alarm, the person to which the alarm is assigned for corrective action, and the severity of the alarm. Click the **Launch Alarm Mgmt** icon (right upward-slanting arrow enclosed in a square) to navigate to the Fault mode and view the four standard alarm monitors available in Fault mode.

Active Alarms for the respective components are displayed when the component is clicked in the image of the chassis displayed. The components for which the alarms are displayed are Flexible Port Concentrator (FPC), Dense Port Concentrator (DPC), Physical Interface Card (PIC), Modular Interface Card (MIC), Routing Engine, Control Boards, fan trays, Switch Interface Board (SIB), and power supply module (PSM).

The following fields are displayed in the Active Alarms pane:

Table 233: Active Alarms Monitor

Table Column	Description
Severity	The severity of the alarm. Severity levels are: <ul style="list-style-type: none"> • Critical—A critical condition exists; immediate action is necessary. • Major—A major error has occurred; escalate or notify as necessary. • Minor—A minor error has occurred; notify or monitor the condition. • Info—An informational message; no action is necessary.
Name	The alarm name.
Source	The IP address of the device or network element that generated the alarm. The SNMP agent is located at the source IP. In most cases, the source IP is the IP address of the switch or controller.
Last Updated	The date and time that the information for the alarm was last modified.

The following fields are displayed in the Component Info pane:

Table 234: Fields for Physical Interfaces in the Component Info Pane

Field	Description
Host Name	Hostname of the device
Physical Interface Name	Name of the physical interface
IP Address	IP address configured on the interface
Encapsulation	Encapsulation configured on the logical interface
Hardware Address	MAC address configured on the interface

Table 234: Fields for Physical Interfaces in the Component Info Pane (continued)

Field	Description
Operation Status	Operational status of the physical interface: Up, Down.
Admin Status	Administrative state of the interface: Enabled or Disabled. If the interface is disabled, it can provide network connectivity, but it cannot provide power to connected devices.
Link Level Type	Encapsulation type configured on the interface
Link Type	Data transmission type
Speed	Speed at which the interface is running
MTU	Maximum transmission unit size on the physical interface
Loopback	Specifies whether the loopback status is enabled or disabled. If loopback is enabled, the type of loopback—Local or Remote—is displayed.
Description	Configured textual description of the interface

A redundant Ethernet interface is a pseudointerface that includes at minimum one physical interface from each node of the cluster. A redundant Ethernet interface must contain, at minimum, a pair of Fast Ethernet interfaces or a pair of Gigabit Ethernet interfaces that are referred to as child interfaces of the redundant Ethernet interface (the redundant parent). If two or more child interfaces from each node are assigned to the redundant Ethernet interface, a redundant Ethernet interface link aggregation group must be formed.

A pseudowire subscriber logical interface terminates an MPLS pseudowire tunnel from an access node to the MX Series router that hosts subscriber management, and enables you to perform subscriber management services at the interface. Subscriber management supports the creation of subscriber interfaces over point-to-point MPLS pseudowires. The pseudowire subscriber interface capability enables service providers to extend an MPLS domain from the access-aggregation network to the service edge, where subscriber management is performed. Service providers can take advantage of MPLS capabilities such as failover, rerouting, and uniform MPLS label provisioning, while using a single pseudowire to service a large number of DHCP and PPPoE subscribers in the service network.



NOTE: The pseudowire is a tunnel that is either an MPLS-based Layer 2 VPN or Layer 2 circuit. The pseudowire tunnel transports Ethernet encapsulated traffic from an access node (for example, a DSLAM or other aggregation device) to the MX Series router that hosts the subscriber management services. The termination of the pseudowire tunnel on the MX Series router is similar to a physical Ethernet termination, and is the point at which subscriber management functions are performed. A service provider can configure multiple pseudowires on a per-DSLAM basis and then provision support for a large number of subscribers on a specific pseudowire. Figure 1 shows an MPLS network that provides subscriber management support.

The following table describes the fields displayed in the Pseudo Interfaces pane.

Table 235: Pseudo Interfaces Columns

Field	Description
Pseudo Interface Name	Name of the pseudowire subscriber logical interface.
Type	Signaling type for the pseudowire interface. You can use either Layer 2 circuit signaling or Layer 2 VPN signaling. The two signaling types are mutually exclusive for a given pseudowire.
Operation Status	Operational status of the physical interface: Up, Down.
Admin Status	Administrative state of the interface: Enabled or Disabled. If the interface is disabled, it can provide network connectivity, but it cannot provide power to connected devices.

The logical interfaces configured on each interface are also shown along with the physical interface description in tabular format. The following table describes the details displayed for logical interfaces.

Table 236: Logical Interfaces Columns

Field	Description
Device Name	The device configuration name.
Interface Name	Standard information about the interface, in the format type-/fpc/pic/port/logical interface, where type is the media type that identifies the network device; for example, ge-0/0/6.135.
IP Address	The IP address for the logical interface.
Encapsulation	The encapsulation type used on the logical interface.
Vlan	The VLAN ID for the logical interface.

Table 236: Logical Interfaces Columns (continued)

Field	Description
Description	An optional description configured for the interface. It can be any text string of 512 or fewer characters. Any longer string is truncated. If there is no information, the column entry is blank.

From the Chassis View window, click the **Details** icon (arrow enclosed in a square) at the top-right corner of the window to open the Chassis View Details page that lists the configured devices and their parameters in the form of a table.

The following fields are displayed on the right pane, depending on the component or element of the chassis you selected from the chassis image displayed.

Table 237: Fields in the Chassis View Details Page

Field	Description
Module	Name of the SDG and the platform type, such as MX240 or MX480. Click the plus sign (+) to expand the tree to display the components of the device, such as chassis, PIC, CPU, and PIC parameters. Information about the chassis, midplane, craft interface (FPM), power midplane (PMP), Power Supply Modules (PSMs), Power Distribution Modules (PDMs), Routing Engines, Control Boards (CBs) and Switch Processor Mezzanine Boards (SPMBs), Switch Fabric Boards (SFBs), Flexible PIC Concentrators (FPCs), PICs, adapter cards (ADCs) and fan trays is displayed.
Model Number	Model number of the FRU hardware component.
Model	Model of the FRU component.
Part Number	Part number of the chassis component.
Serial Number	Serial number of the chassis component. The serial number of the backplane is also the serial number of the router chassis. Use this serial number when you need to contact Juniper Networks Customer Support about the router or switch chassis.

Table 237: Fields in the Chassis View Details Page (continued)

Field	Description
Description	

Table 237: Fields in the Chassis View Details Page (continued)

Field	Description
	<p>Brief description of the hardware item:</p> <ul style="list-style-type: none"> Type of power supply. Type of PIC. If the PIC type is not supported on the current software release, the output states Hardware Not Supported. Type of FPC: FPC Type 1, FPC Type 2, FPC Type 3, FPC Type 4, or FPC Type OC192. On EX Series switches, a brief description of the FPC. On the J Series routers, the FPC type corresponds to the Physical Interface Module (PIM). The following list shows the PIM abbreviation in the output and the corresponding PIM name. <ul style="list-style-type: none"> 2x FE—Either two built-in Fast Ethernet interfaces (fixed PIM) or dual-port Fast Ethernet PIM 4x FE—4-port Fast Ethernet ePIM 1x GE Copper—Copper Gigabit Ethernet ePIM (one 10-Mbps, 100-Mbps, or 1000-Mbps port) 1x GE SFP—SFP Gigabit Ethernet ePIM (one fiber port) 4x GE Base PIC—Four built-in Gigabit Ethernet ports on a J4350 or J6350 chassis (fixed PIM) 2x Serial—Dual-port serial PIM 2x T1—Dual-port T1 PIM 2x E1—Dual-port E1 PIM 2x CTIE1—Dual-port channelized T1/E1 PIM 1x T3—T3 PIM (one port) 1x E3—E3 PIM (one port) 4x BRI S/T—4-port ISDN BRI S/T PIM 4x BRI U—4-port ISDN BRI U PIM 1x ADSL Annex A—ADSL 2/2+ Annex A PIM (one port, for POTS) 1x ADSL Annex B—ADSL 2/2+ Annex B PIM (one port, for ISDN) 2x SHDSL (ATM)—G SHDSL PIM (2-port two-wire module or 1-port four-wire module) 1x TGM550—TGM550 Telephony Gateway Module (Avaya VoIP gateway module with one console port, two analog LINE ports, and two analog TRUNK ports) 1x DS1 TIM510—TIM510 E1/T1 Telephony Interface Module (Avaya VoIP media module with one E1 or T1 trunk termination port and ISDN PRI backup) 4x FXS, 4x FXO, TIM514—TIM514 Analog Telephony Interface Module (Avaya VoIP media module with four analog LINE ports and four analog TRUNK ports) 4x BRI TIM521—TIM521 BRI Telephony Interface Module (Avaya VoIP media module with four ISDN BRI ports) Crypto Accelerator Module—For enhanced performance of cryptographic algorithms used in IP Security (IPsec) services MPC M 16x 10GE—16-port 10-Gigabit Module Port Concentrator that supports SFP+ optical transceivers. (Not on EX Series switches.) For hosts, the Routing Engine type. For small form-factor pluggable transceiver (SFP) modules, the type of fiber: LX, SX, LH, or T. LCD description for EX Series switches (except EX2200 switches).

Table 237: Fields in the Chassis View Details Page (continued)

Field	Description
	<ul style="list-style-type: none"> • MPC2—1-port MPC2 that supports two separate slots for MICs. • MPC3E—1-port MPC3E that supports two separate slots for MICs (MIC-3D-1X100GE-CFP and MIC-3D-20GE-SFP) on MX960, MX480, and MX240 routers. The MPC3E maps one MIC to one PIC (1 MIC, 1 PIC), which differs from the mapping of legacy MPCs. • 100GBASE-LR4, pluggable CFP optics • Supports the Enhanced MX Switch Control Board with fabric redundancy and existing SCBs without fabric redundancy. • Interoperates with existing MX Series line cards, including Flexible Port Concentrators (FPC), Dense Port Concentrators (DPCs), and Modular Port Concentrators (MPCs). • MPC4E—Fixed configuration MPC4E that is available in two flavors: MPC4E-3D-32XGE-SFP and MPC4E-3D-2CGE-8XGE on MX2020, MX960, MX480, and MX240 routers. • LCD description for MX Series routers

Click the **Apply Configlet** button (pencil icon displayed beside the button) and use the links shown on the components in Chassis View to select the context and apply configlets.

- Related Documentation**
- [Deleting Devices from Chassis View on page 1345](#)
 - [Rebooting Devices After Examining the Status in Chassis View on page 1346](#)
 - [About Chassis View on page 1335](#)

Configuring and Managing OTN Port Details of MX Series and PTX Series Routers for Easy Administration

Instead of using Junos OS CLI statements and operational commands to configure the OTN port settings and view the configured parameters, you can view an image of the OTN port using Connectivity Services Director to obtain an intuitive and high-level understanding of the settings and alarms. This view enables you to modify the OTN port settings to suit your network deployment needs in a simplified and optimal manner. Because the important OTN port settings can be configured alongside the visual representation of the entire chassis that is displayed, this method of managing the OTN port settings provides a consolidated and cohesive interface for easy administration of the network.

You can perform the following tasks in this dialog box:

- View the optical interface specifications that are currently applied on the device, such as wavelength and power
- Modify the existing parameters of the optical port to suit your network needs or resolve any alarms caused by certain interface settings

To configure the full C-band International Telecommunication Union (ITU)-Grid tunable optics for 10-Gigabit Ethernet or 100-Gigabit Ethernet dense wavelength-division multiplexing (DWDM) interfaces:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the device for which you want to define the optical port settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device and associated hardware components is displayed on the right pane.

5. In the image of the device, select an OTN port or interface—for example, a 100-Gigabit Ethernet OTN PIC installed in a PTX Series router.

The Optical Port dialog box is displayed. At the lower part of the dialog box, the Optical Port Section pane is expanded and displayed.

6. Click the **Status/Config** tab at the bottom of the dialog box.

The configuration settings that pertain to the optical interface are displayed as shown in [Figure 89 on page 1498](#).

Figure 89: Optical Port Dialog Box

The screenshot shows the 'Optical Port' dialog box with three main sections: Port State, Loopbacks, and Config. The Port State section shows OperState as Fault, AdminState as IS, and Status as PRESENT. The Loopbacks section shows both Local Loopback and Line Loopback as Disabled. The Config section shows Wavelength as Ch:6/1565.5nm/191.5THz, Modulation as DP-QPSK, Laser Enable as Enabled, Tx Power as 0 dBm, Rx Power as 0 dBm, and PM Collection as Enabled. At the bottom, there are tabs for OTU Section, ODU Path, Equipment, Status/Config (selected), and Performance.

Optical Port	
<div> <div>Update</div> <div>Cancel</div> </div>	
<div> <div>Port State</div> <div> <div>OperState: Fault</div> <div>AdminState: IS</div> <div>Status: PRESENT</div> </div> </div>	
<div> <div>Loopbacks</div> <div> <div>Local Loopback: Disabled</div> <div>Line Loopback: Disabled</div> </div> </div>	
<div> <div>Config</div> <div> <div>Wavelength: Ch:6/1565.5nm/191.5THz</div> <div>Modulation: DP-QPSK</div> <div>Laser Enable: Enabled</div> <div>Tx Power: 0 dBm</div> <div>Rx Power: 0 dBm</div> <div>PM Collection: Enabled</div> </div> </div>	
<div> <div>OTU Section</div> <div>ODU Path</div> <div> <div>Equipment</div> <div>Status/Config</div> <div>Performance</div> </div> </div>	

7. In the Port State section, do the following:
 - a. The OperStatus field displays the operational status of the optical interface. Possible values are **Fault** or **Normal**.
 - b. From the AdminState list, specify the administrative status of the interface as enabled or disabled, and click **Update** at the top of the dialog box to save the changes. Possible values are:

- **IS**—In-service with masked alarms disabled
- **IS-MA**—In-service with masked alarms enabled
- **OOS**—Out-of-service with masked alarms disabled
- **OOS-MA**—Out-of-service with masked alarms enabled

c. The Status field displays any of the following values:

- **LOS** (loss of signal)
- **LOF** (loss of frame)
- **LOM** (loss of multiframe)
- **SSF** (server signal failure)
- **TSF** (trail signal fail)

8. In the Loopbacks section, do the following:

- a. From the Line Loopback list, specify whether line-loopback needs to be enabled or disabled, and click **Update** at the top of the dialog box to save the changes. When configured in line loopback mode, the router never receives data from the network. A line loopback places an interface in external loopback state.

Instead of transmitting the signal toward the far-end device, the line loopback sends the signal back to the originating router. If the originating router receives back its own data link layer packets, you have verified that the problem is beyond the originating router. Next, configure a line loopback farther away from the local router. If this originating router does not receive its own data link layer packets, you can assume the problem is on one of the segments between the local router and the remote router's interface card. In this case, the next troubleshooting step is to configure a line loopback closer to the local router to find the source of the problem.

- b. From the Local Loopback list, specify whether local-loopback needs to be enabled or disabled, and click **Update** at the top of the dialog box to save the changes. When you create a local loopback, you create an internal loop on the interface being tested. A local loopback loops the traffic internally on that PIC. A local loopback tests the interconnection of the PIC but does not test the transmit and receive ports. A local loopback enables you to configure a loop without physically connecting the transmit port to the receive port.

Local loopback is useful for troubleshooting physical PIC errors. Configuring local loopback on an interface allows transmission of packets to the channel service unit (CSU) and then to the circuit toward the far-end device. The interface receives its own transmission, which includes data and timing information, on the local router's PIC. The data received from the CSU is ignored.

9. In the Config section, do the following:

- a. From the Laser Enable field, specify whether the laser on the OTN interface must be enabled or disabled, and click **Update** at the top of the dialog box to save the changes.
- b. The laser is disabled by default for all OTN interfaces. The Modulation field displays the type of modulation as Dual polarization quadrature phase shift keying (DP-QPSK) modulation.
- c. From the Wavelength list, select the wavelength value, which can be one of the following, and click **Update** at the top of the dialog box to save the changes. All values are displayed. However, if you configure a value that is not supported by the device, an error message is displayed and the device is not tuned to the specified wavelength.
 - **1528.38**—1528.38 nanometers (nm), corresponds to a 50-GHz grid
 - **1528.77**—1528.77 nm, corresponds to 50-GHz and 100-GHz grids
 - **1529.16**—1529.16 nm, corresponds to a 50-GHz grid
 - **1529.55**—1529.55 nm, corresponds to 50-GHz and 100-GHz grids
 - **1529.94**—1529.94 nm, corresponds to a 50-GHz grid
 - **1530.33**—1530.33 nm, corresponds to 50-GHz and 100-GHz grids
 - **1530.72**—1530.72 nm, corresponds to a 50-GHz grid
 - **1531.12**—1531.12 nm, corresponds to 50-GHz and 100-GHz grids
 - **1531.51**—1531.51 nm, corresponds to a 50-GHz grid
 - **1531.90**—1531.90 nm, corresponds to 50-GHz and 100-GHz grids
 - **1532.29**—1532.29 nm, corresponds to a 50-GHz grid
 - **1532.68**—1532.68 nm, corresponds to 50-GHz and 100-GHz grids
 - **1533.07**—1533.07 nm, corresponds to a 50-GHz grid
 - **1533.47**—1533.47 nm, corresponds to 50-GHz and 100-GHz grids
 - **1533.86**—1533.86 nm, corresponds to a 50-GHz grid
 - **1534.25**—1534.25 nm, corresponds to 50-GHz and 100-GHz grids
 - **1534.64**—1534.64 nm, corresponds to a 50-GHz grid
 - **1535.04**—1535.04 nm, corresponds to 50-GHz and 100-GHz grids
 - **1535.43**—1535.43 nm, corresponds to a 50-GHz grid
 - **1535.82**—1535.82 nm, corresponds to 50-GHz and 100-GHz grids
 - **1536.22**—1536.22 nm, corresponds to a 50-GHz grid
 - **1536.61**—1536.61 nm, corresponds to 50-GHz and 100-GHz grids
 - **1537.00**—1537.00 nm, corresponds to a 50-GHz grid
 - **1537.40**—1537.40 nm, corresponds to 50-GHz and 100-GHz grids
 - **1537.79**—1537.79 nm, corresponds to a 50-GHz grid

- **1538.19**—1538.19 nm, corresponds to 50-GHz and 100-GHz grids
- **1538.58**—1538.58 nm, corresponds to a 50-GHz grid
- **1538.98**—1538.98 nm, corresponds to 50-GHz and 100-GHz grids
- **1539.37**—1539.37 nm, corresponds to a 50-GHz grid
- **1539.77**—1539.77 nm, corresponds to 50-GHz and 100-GHz grids
- **1540.16**—1540.16 nm, corresponds to a 50-GHz grid
- **1540.56**—1540.56 nm, corresponds to 50-GHz and 100-GHz grids
- **1540.95**—1540.95 nm, corresponds to a 50-GHz grid
- **1541.35**—1541.35 nm, corresponds to 50-GHz and 100-GHz grids
- **1541.75**—1541.75 nm, corresponds to a 50-GHz grid
- **1542.14**—1542.14 nm, corresponds to 50-GHz and 100-GHz grids
- **1542.54**—1542.54 nm, corresponds to a 50-GHz grid
- **1542.94**—1542.94 nm, corresponds to 50-GHz and 100-GHz grids
- **1543.33**—1543.33 nm, corresponds to a 50-GHz grid
- **1543.73**—1543.73 nm, corresponds to 50-GHz and 100-GHz grids
- **1544.13**—1544.13 nm, corresponds to a 50-GHz grid
- **1544.53**—1544.53 nm, corresponds to 50-GHz and 100-GHz grids
- **1544.92**—1544.92 nm, corresponds to a 50-GHz grid
- **1545.32**—1545.32 nm, corresponds to 50-GHz and 100-GHz grids
- **1545.72**—1545.72 nm, corresponds to a 50-GHz grid
- **1546.12**—1546.12 nm, corresponds to 50-GHz and 100-GHz grids
- **1546.52**—1546.52 nm, corresponds to a 50-GHz grid
- **1546.92**—1546.92 nm, corresponds to 50-GHz and 100-GHz grids
- **1547.32**—1547.32 nm, corresponds to a 50-GHz grid
- **1547.72**—1547.72 nm, corresponds to 50-GHz and 100-GHz grids
- **1548.11**—1548.11 nm, corresponds to a 50-GHz grid
- **1548.51**—1548.51 nm, corresponds to 50-GHz and 100-GHz grids
- **1548.91**—1548.91 nm, corresponds to a 50-GHz grid
- **1549.32**—1549.32 nm, corresponds to 50-GHz and 100-GHz grids
- **1549.72**—1549.72 nm, corresponds to a 50-GHz grid
- **1550.12**—1550.12 nm, corresponds to 50-GHz and 100-GHz grids
- **1550.52**—1550.52 nm, corresponds to a 50-GHz grid
- **1550.92**—1550.92 nm, corresponds to 50-GHz and 100-GHz grids

- **1551.32**—1551.32 nm, corresponds to a 50-GHz grid
- **1551.72**—1551.72 nm, corresponds to 50-GHz and 100-GHz grids
- **1552.12**—1552.12 nm, corresponds to a 50-GHz grid
- **1552.52**—1552.52 nm, corresponds to 50-GHz and 100-GHz grids
- **1552.93**—1552.93 nm, corresponds to a 50-GHz grid
- **1553.33**—1554.33 nm, corresponds to 50-GHz and 100-GHz grids
- **1553.73**—1554.73 nm, corresponds to a 50-GHz grid
- **1554.13**—1554.13 nm, corresponds to 50-GHz and 100-GHz grids
- **1554.54**—1554.54 nm, corresponds to a 50-GHz grid
- **1554.94**—1554.94 nm, corresponds to 50-GHz and 100-GHz grids
- **1555.34**—1555.34 nm, corresponds to a 50-GHz grid
- **1555.75**—1555.75 nm, corresponds to 50-GHz and 100-GHz grids
- **1556.15**—1556.15 nm, corresponds to a 50-GHz grid
- **1556.55**—1556.55 nm, corresponds to 50-GHz and 100-GHz grids
- **1556.96**—1556.96 nm, corresponds to a 50-GHz grid
- **1557.36**—1557.36 nm, corresponds to 50-GHz and 100-GHz grids
- **1557.77**—1557.77 nm, corresponds to a 50-GHz grid
- **1558.17**—1558.17 nm, corresponds to 50-GHz and 100-GHz grids
- **1558.58**—1558.58 nm, corresponds to a 50-GHz grid
- **1558.98**—1558.98 nm, corresponds to 50-GHz and 100-GHz grids
- **1559.39**—1559.39 nm, corresponds to a 50-GHz grid
- **1559.79**—1559.79 nm, corresponds to 50-GHz and 100-GHz grids
- **1560.20**—1560.20 nm, corresponds to a 50-GHz grid
- **1560.61**—1560.61 nm, corresponds to 50-GHz and 100-GHz grids
- **1561.01**—1561.01 nm, corresponds to a 50-GHz grid
- **1561.42**—1561.42 nm, corresponds to 50-GHz and 100-GHz grids
- **1561.83**—1561.83 nm, corresponds to a 50-GHz grid
- **1562.23**—1562.23 nm, corresponds to 50-GHz and 100-GHz grids
- **1562.64**—1562.64 nm, corresponds to a 50-GHz grid
- **1563.05**—1563.05 nm, corresponds to 50-GHz and 100-GHz grids
- **1563.45**—1563.45 nm, corresponds to a 50-GHz grid
- **1563.86**—1563.86 nm, corresponds to 50-GHz and 100-GHz grids
- **1564.27**—1564.27 nm, corresponds to a 50-GHz grid

- **1564.68**—1564.68 nm, corresponds to 50-GHz and 100-GHz grids
- **1565.09**—1565.09 nm, corresponds to a 50-GHz grid
- **1565.50**—1565.50 nm, corresponds to 50-GHz and 100-GHz grids
- **1565.90**—1565.90 nm, corresponds to a 50-GHz grid
- **1566.31**—1566.31 nm, corresponds to 50-GHz and 100-GHz grids
- **1566.72**—1566.72 nm, corresponds to a 50-GHz grid
- **1567.13**—1567.13 nm, corresponds to 50-GHz and 100-GHz grids
- **1567.54**—1567.54 nm, corresponds to a 50-GHz grid
- **1567.95**—1567.95 nm, corresponds to 50-GHz and 100-GHz grids
- **1568.36**—1568.36 nm, corresponds to a 50-GHz grid
- **1568.77**—1568.77 nm, corresponds to 50-GHz and 100-GHz grids

Table 220 on page 1442 shows configurable wavelengths and the corresponding frequency for each configurable wavelength.

Table 238: Wavelength-to-Frequency Conversion Matrix

Wavelength (nm)	Frequency (THz)	Wavelength (nm)	Frequency (THz)	Wavelength (nm)	Frequency (THz)
1528.38	196.15	1542.14	194.40	1556.15	192.65
1528.77	196.10	1542.54	194.35	1556.55	192.60
1529.16	196.05	1542.94	194.30	1556.96	192.55
1529.55	196.00	1543.33	194.25	1557.36	192.50
1529.94	195.95	1543.73	194.20	1557.77	192.45
1530.33	195.90	1544.13	194.15	1558.17	192.40
1530.72	195.85	1544.53	194.10	1558.58	192.35
1531.12	195.80	1544.92	194.05	1558.98	192.30
1531.51	195.75	1545.32	194.00	1559.39	192.25
1531.90	195.70	1545.72	193.95	1559.79	192.20
1532.29	195.65	1546.12	193.90	1560.20	192.15
1532.68	195.60	1546.52	193.85	1560.61	192.10
1533.07	195.55	1546.92	193.80	1561.01	192.05

Table 238: Wavelength-to-Frequency Conversion Matrix (continued)

Wavelength (nm)	Frequency (THz)	Wavelength (nm)	Frequency (THz)	Wavelength (nm)	Frequency (THz)
1533.47	195.50	1547.32	193.75	1561.42	192.00
1533.86	195.45	1547.72	193.70	1561.83	191.95
1534.25	195.40	1548.11	193.65	1562.23	191.90
1534.64	195.35	1548.51	193.60	1562.64	191.85
1535.04	195.30	1548.91	193.55	1563.05	191.80
1535.43	195.25	1549.32	193.50	1563.45	191.75
1535.82	195.20	1549.72	193.45	1563.86	191.70
1536.22	195.15	1550.12	193.40	1564.27	191.65
1536.61	195.10	1550.52	193.35	1564.68	191.60
1537.00	195.05	1550.92	193.30	1565.09	191.55
1537.40	195.00	1551.32	193.25	1565.50	191.50
1537.79	194.95	1551.72	193.20	1565.90	191.45
1538.19	194.90	1552.12	193.15	1566.31	191.40
1538.58	194.85	1552.52	193.10	1566.72	191.35
1538.98	194.80	1552.93	193.05	1567.13	191.30
1539.37	194.75	1553.33	193.00	1567.54	191.25
1539.77	194.70	1553.73	192.95	1567.95	191.20
1540.16	194.65	1554.13	192.90	1568.36	191.15
1540.56	194.60	1554.54	192.85	1568.77	191.10
1540.95	194.55	1554.94	192.80		
1541.35	194.50	1555.34	192.75		
1541.75	194.45	1555.75	192.70		

- d. The Tx Power field displays the transmit laser output power (dBm). If you did not specify a value, the default transmit laser output power is –2 dBm.
 - e. The Rx Power field displays the laser received optical power, in mW and dBm.
10. From the PM collection list, specify whether the retrieval and computation of performance management statistics by polling the device must be enabled or not, and click **Update** to save the changes. If you do not enable the collection of performance monitoring counters and values, you might not be able to measure the performance and the operational status of the services running in your network.

You can click the **Refresh** (rotating arrow icon) button at the top of the dialog box to enable the latest settings be retrieved from the device and displayed.

**Related
Documentation**

- [Configuring and Managing OTU Details of MX Series and PTX Series Routers for Simplified Management on page 1505](#)
- [Configuring and Managing ODU Details of MX Series and PTX Series Routers for Simplified Management on page 1512](#)
- [Configuring and Managing Optical PIC Details for Effective Provisioning on page 1517](#)

Configuring and Managing OTU Details of MX Series and PTX Series Routers for Simplified Management

Instead of using Junos OS CLI statements and operational commands to configure OTU settings and view the configured parameters, you can view an image of the OTN port using Connectivity Services Director to obtain an intuitive and high-level understanding of the settings and alarms. This view enables you to modify the OTU settings to suit your network deployment needs in a simplified and optimal manner. Because the important OTU settings can be configured alongside the visual representation of the entire chassis that is displayed, this method of managing the OTU settings provides a consolidated and cohesive interface for easy administration of the network.

You can perform the following tasks in the OTU Section pane:

- View the optical channel transport unit (OTU) specifications that are currently applied on the device, such as wavelength and power
- Modify the existing parameters of the optical port to suit your network needs or resolve any alarms caused by certain interface settings

To configure the OTN parameters for 10-Gigabit Ethernet or 100-Gigabit Ethernet dense wavelength-division multiplexing (DWDM) interfaces:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the device for which you want to define the optical port settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. In the image of the device, select an OTN port or interface—for example, a 100-Gigabit Ethernet OTN PIC installed in a PTX Series router.

The Optical Port dialog box is displayed. At the lower part of the dialog box, the OTU Section and ODU Section panes are displayed in a collapsed form.

6. Click the **OTU Section** header at the bottom of the dialog box.

The OTU Section pane is expanded and displayed.

7. Click the **Status/Config** tab at the bottom of the dialog box.

The configuration settings that pertain to the OTU are displayed as shown in [Figure 90 on page 1507](#).

Figure 90: OTU Section Dialog Box

OTU Section

Update Cancel

Status

OTU Status:

Config

OTU Rate: OTU4 (120.5Gbps)

FEC Mode: SDFEC

Backward FRR: Disabled

Signal Degrad Monitor: Disabled

TTI - DAPI

Tx Trace: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Rx Trace:

Tx Trace Config:

Rx Trace Config:

TTI - SAPI

Tx Trace: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Rx Trace: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Tx Trace Config:

ODU Path

Equipment Status/Config Performance

8. In the Status section, the OTU Status field is displayed. The OTU Status field displays the status of the OTU. Possible values are:
- OTU-FEC-DEG (forward error correction degraded)
 - OTU-FEC-EXE (excessive errors, FEC_FAIL from the transponder)
 - OTU-AIS (alarm indication signal or all ones signal)
 - OTU-BDI (backward defect identification)
 - OTU-IAE (incoming alignment error)
 - OTU-BIAE (backward incoming alignment error)

- **OTU-TTIM** (destination access point identifier [DAPI], source access point identifier [SAPI], or both mismatch from expected to received)
- **OTU-DEG** (OTU degraded)

9. In the Config section, do the following:

- The Rate field displays the line rate or speed of the OTN signals. One of the following values is displayed, if you have previously configured the OTN mode:
 - **fixed-stuff-bytes**—Fixed stuff bytes 11.0957 Gbps.
 - **no-fixed-stuff-bytes**—No fixed stuff bytes 11.0491 Gbps.
 - **pass-through**—Enable OTN passthrough mode.
 - **no-pass-through**—Do not enable OTN passthrough mode

Select a different line rate if needed from the Rate list.

- The FEC Mode field displays the forward error correction (FEC) mode. One of the following values is displayed, if you have previously configured the FEC mode:
 - **EFEC**—G.975.11.4 enhanced forward error correction (EFEC) is configured to detect and correct bit errors.
 - **GFEC**—G.709 generic forward error correction (GFEC) mode is configured to detect and correct bit errors.
 - **GFEC-SDFEC**—GFEC and soft-decision forward error correction (SD-FEC) modes are configured to detect and correct bit errors.
 - **NONE**—FEC mode is not configured.
 - **UFEC**—Ultra Forward Error Correction (UFEC) mode is configured to detect and correct bit errors.

Select a different FEC mode if needed from the FEC Mode list.

- From the Backward FRR list, specify whether you want to enable or disable preemptive fast reroute (FRR) insertion. By default, FRR ODU backward FRR insertion is disabled.
- From the Signal Degrade Monitor list, specify whether you want to enable or disable preemptive fast reroute (FRR) signal degrade monitoring. By default, FRR signal degrade monitoring is disabled. If you do not configure the signal-degrade parameter, the default threshold values are used.
- From the Signal Degrade Interval selector, use the up and down arrows to specify the time interval in milliseconds (ms). This is the interval for which the BER must stay above the signal degradation threshold—as configured in the Ber Threshold Signal Degrade field—for the alarm to be raised. After an alarm is raised, if the BER returns below the clear threshold—as configured in the Ber Threshold Clear field—for the specified interval, the alarm is cleared.

The default value is 100 ms. The range is from 1 ms through 100 ms.



NOTE: For the P1-PTX-2-100G-WDM PIC, the BER must stay above the signal degradation threshold for ten consecutive intervals for the alarm to be raised and the BER must stay below the clear threshold for ten consecutive intervals for the alarm to be cleared. For example, if the interval is configured as 10 ms, then the BER must stay above the signal degradation threshold for 100 ms (10 ms * 10 intervals) for the alarm to be raised, or below the clear threshold for 100 ms for the alarm to be cleared.



NOTE: For P1-PTX-24-10G-W-SFPP PIC and P2-100GE-OTN PIC, when the router cannot configure BER with the given interval, it selects an optimum interval that is supported for the given BER configuration. If the router is still not able to support the configuration (for example, with a wider gap between the degrade set and clear values), the default values are used and a log is generated.

For the P2-10G-40G-QSFPP PIC, the time interval is supported in multiples of 100 ms. For example, when you configure the interval as 10 ms, then it is rounded off to the nearest multiple of 100 ms.

Configuring a high BER threshold for signal degradation and a long interval might cause the internal counter register to be saturated. Such a configuration is ignored by the router, and the default values are used instead. A system log message is logged for this error.

- In the Ber Threshold Clear field, specify the bit error rate (BER) threshold to clear the interface alarm for signal degradation. You must specify the BER threshold for signal degradation in scientific notation. Both the mantissa and exponent are configurable. Enter the value in the format $x\text{E}-n$, where x is the mantissa and n is the exponent. For example, $4.5\text{E}-3$.

The mantissa must be a decimal number. There is no limit on the number of digits before or after the decimal point. The exponent must be an integer from 0 through 9.

You can configure the BER clear threshold to customize the BER that will clear an interface alarm when signal degrade monitoring is enabled.

[Table 239 on page 1509](#) shows the default values for pre-FEC BER and ODU BER signal degrade threshold values for different PICs. If the BER signal degrade threshold is not configured, the default value is used.

Table 239: Default Clear Threshold Values

PIC	Default Pre-FEC BER Clear Threshold Value	Default ODU BER Clear Threshold Value
P1-PTX-2-100G-WDM	$3.0\text{E}-3$	Not supported

Table 239: Default Clear Threshold Values (continued)

PIC	Default Pre-FEC BER Clear Threshold Value	Default ODU BER Clear Threshold Value
P2-100GE-OTN	3.0E-3	1.0E-9
P1-PTX-24-10G-W-SFPP	3.0E-3	Not supported

- In the Ber Threshold Degrade field, specify the BER threshold is used to raise an interface alarm for signal degradation. You can configure the BER signal degrade threshold to customize the BER that will raise an interface alarm when signal degrade monitoring is enabled. You must specify the BER threshold for signal degradation in scientific notation. Both the mantissa and exponent are configurable. Enter the value in the format $x\text{E}-n$, where x is the mantissa and n is the exponent. For example, 4.5E-3.

The mantissa must be a decimal number. There is no limit on the number of digits before or after the decimal point. The exponent must be an integer from 0 through 9.



NOTE: Configuring a high BER threshold for signal degradation and a long interval might cause the internal bit error counter register to get saturated. For example, for the P1-PTX-2-100G-WDM PIC, the internal bit error counter gets saturated when the error count reaches 2E+29. Therefore, the value of `ber-threshold-signal-degrade * line rate / interval` must be less than 2E+29 to avoid saturation. Assuming a fixed PIC line rate of 1.27E+11 bits per second and an interval of 1000 ms, the `ber-threshold-signal-degrade` value must be less than 4.22E-3.

If the value of the `ber-threshold-signal-degrade * line rate / interval` exceeds the saturation limit, the configuration is ignored by the router, and the default values are used instead. A system log message is logged for this error.

Table 240 on page 1510 shows the default values for pre-FEC BER and ODU BER signal degrade threshold values for different PICs. If the BER signal degrade threshold is not configured, the default value is used.

Table 240: Default Signal Degrade Threshold Values

PIC	Default Pre-FEC BER Signal Degrade Threshold Value	Default ODU BER Signal Degrade Threshold Value
P1-PTX-2-100G-WDM	7.5E-3	Not supported
P2-100GE-OTN	7.5E-3	1.0E-6
P1-PTX-24-10G-W-SFPP	7.5E-3	Not supported

10. Depending on the configured trace identifier (TTI), any of the following TTI sections are displayed in the OTU Section pane:
 - **odu-dapi**—ODU Destination Access Point Identifier.
 - **odu-expected-receive-dapi**—ODU Expected Receive Destination Access Point Identifier.
 - **odu-expected-receive-sapi**—ODU Expected Receive Source Access Point Identifier.
 - **odu-sapi**—ODU Source Access Point Identifier.
 - **out-dapi**—OTU Destination Access Point Identifier.
 - **out-expected-receive-dapi**—OTU Expected Receive Destination Access Point Identifier.
 - **out-expected-receive-sapi**—OTU Expected Receive Source Access Point Identifier.
 - **out-sapi**—OTU Source Access Point Identifier
11. In the TTI-DAPI section, do the following:
 - The Tx Trace and Rx Trace fields display the transmitted and received path trace values. A path trace identifier is a text string that identifies the circuit. The text string that identifies the circuit. SONET/SDH interfaces allow path trace bytes to be sent inband across the SONET/SDH link. Juniper Networks and other router manufacturers use these bytes to help diagnose misconfigurations and network errors by setting the transmitted path trace message so that it contains the system hostname and name of the physical interface. The received path trace value is the message received from the routing device at the other end of the fiber. The transmitted path trace value is the message that this routing device transmits.
 - In the Tx Trace config field, specify the propagated path trace identifier. A common convention is to use the circuit identifier as the path trace identifier.
 - In the Rx Trace Config field, specify the received path trace identifier. A common convention is to use the circuit identifier as the path trace identifier.
12. In the TTI-DAPI section, do the following:
 - The Tx Trace and Rx Trace fields display the transmitted and received path trace values. A path trace identifier is a text string that identifies the circuit. The text string that identifies the circuit. SONET/SDH interfaces allow path trace bytes to be sent inband across the SONET/SDH link. Juniper Networks and other router manufacturers use these bytes to help diagnose misconfigurations and network errors by setting the transmitted path trace message so that it contains the system hostname and name of the physical interface. The received path trace value is the message received from the routing device at the other end of the fiber. The transmitted path trace value is the message that this routing device transmits.
 - In the Tx Trace config field, specify the propagated path trace identifier. A common convention is to use the circuit identifier as the path trace identifier.
 - In the Rx Trace Config field, specify the received path trace identifier. A common convention is to use the circuit identifier as the path trace identifier.
13. Click **Update** at the top of the dialog box to save the modified OTU settings.

The settings are saved in the Connectivity Services Director database.

You can click the **Refresh** (rotating arrow icon) button at the top of the dialog box to enable the latest settings be retrieved from the device and displayed.

**Related
Documentation**

- [Configuring and Managing OTN Port Details of MX Series and PTX Series Routers for Easy Administration on page 1497](#)
- [Configuring and Managing ODU Details of MX Series and PTX Series Routers for Simplified Management on page 1512](#)
- [Configuring and Managing Optical PIC Details for Effective Provisioning on page 1517](#)

Configuring and Managing ODU Details of MX Series and PTX Series Routers for Simplified Management

Instead of using Junos OS CLI statements and operational commands to configure ODU settings and view the configured parameters, you can view an image of the OTN port using Connectivity Services Director to obtain an intuitive and high-level understanding of the settings and alarms. This view enables you to modify the ODU settings to suit your network deployment needs in a simplified and optimal manner. Because the important ODU settings can be configured alongside the visual representation of the entire chassis that is displayed, this method of managing the ODU settings provides a consolidated and cohesive interface for easy administration of the network.

You can perform the following tasks in the ODU Path pane:

- View the optical channel data unit (ODU) specifications that are currently applied on the device, such as wavelength and power
- Modify the existing parameters of the optical port to suit your network needs or resolve any alarms caused by certain interface settings

To configure the ODU parameters for 10-Gigabit Ethernet or 100-Gigabit Ethernet dense wavelength-division multiplexing (DWDM) interfaces:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the device for which you want to define the optical port settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. In the image of the device, select an OTN port or interface—for example, a 100-Gigabit Ethernet OTN PIC installed in a PTX Series router.

The Optical Port dialog box is displayed. At the lower part of the dialog box, the OTU Section and ODU Path panes are displayed in a collapsed form.

6. Click the **ODU Path** header at the bottom of the dialog box.

The ODU Path pane is expanded and displayed.

7. Click the **Status/Config** tab at the bottom of the dialog box.

The configuration settings that pertain to the ODU are displayed as shown in [Figure 91 on page 1514](#).

Figure 91: ODU Path Dialog Box

Optical Port

OTU Section

ODU Path

Update Cancel

Status

ODU Status:

Config

ODU Backward FRR: Disabled

ODU Signal Degrade Monitor: Disabled

TTI - DAPI

Tx Trace: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Rx Trace: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Tx Trace Config:

Rx Trace Config:

TTI - SAPI

Tx Trace: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Rx Trace: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Tx Trace Config:

Rx Trace Config:

Equipment Status/Config Performance

8. In the Status section, the ODU Status field is displayed.

The ODU Status field displays the status of the ODU (optical channel data unit). Possible values are:

- CSF (client signal failure)
- ODU-DM-TIMEOUT (DM timeout)
- ODU-LCK (ODU lock triggers for PM [path monitoring] and TCM levels 1 through 6)
- ODU-AIS (alarm indication signal or all ones signal)
- ODU-OCI (open connection error)

- **ODU-BDI** (backward defect indication)
 - **ODU-DEG** (ODU degraded)
 - **ODU-IAE** (incoming alignment error)
 - **ODU-DAPI-TTIM** (DAPI or DAPI/SAPI mismatch from expected to receive)
 - **ODU-SAPI-TTIM** (SAPI or DAPI/SAPI mismatch from expected to receive)
 - **ODU-BEI** (backward error indication)
 - **ODU-BEI-ERR** (backward error indication error)
 - **ODU-BIP8-ERR** (bit interleaved parity 8 error)
 - **ODU-SSF** (server signal fail)
 - **ODU-TSF** (trail signal fail)
 - **ODU-SD** (signal degrade)
9. In the Config section, do the following:
- From the ODU Backward FRR list, specify whether you want to enable or disable backward fast reroute (FRR) insertion. You can insert the ODU status into the transmitted OTN frames and monitor the received OTN frames for the ODU BER status. By default, FRR ODU backward FRR insertion is disabled.
 - From the ODU Signal Degrade Monitor list, specify whether you want to enable or disable monitoring of signal degradation of ODU BER in the received OTN frames. By default, FRR signal degrade monitoring disabled.
10. Depending on the configured trace identifier (TTI), any of the following TTI sections are displayed in the OTU Section pane:
- **odu-dapi**—ODU Destination Access Point Identifier.
 - **odu-expected-receive-dapi**—ODU Expected Receive Destination Access Point Identifier.
 - **odu-expected-receive-sapi**—ODU Expected Receive Source Access Point Identifier.
 - **odu-sapi**—ODU Source Access Point Identifier.
 - **out-dapi**—OTU Destination Access Point Identifier.
 - **out-expected-receive-dapi**—OTU Expected Receive Destination Access Point Identifier.
 - **out-expected-receive-sapi**—OTU Expected Receive Source Access Point Identifier.
 - **out-sapi**—OTU Source Access Point Identifier
11. In the TTI-DAPI section, do the following:
- The Tx Trace and Rx Trace fields display the transmitted and received path trace values. A path trace identifier is a text string that identifies the circuit. The text string that identifies the circuit. SONET/SDH interfaces allow path trace bytes to be sent inband across the SONET/SDH link. Juniper Networks and other router manufacturers use these bytes to help diagnose misconfigurations and network errors by setting

the transmitted path trace message so that it contains the system hostname and name of the physical interface. The received path trace value is the message received from the routing device at the other end of the fiber. The transmitted path trace value is the message that this routing device transmits.

- In the Tx Trace config field, specify the propagated path trace identifier. A common convention is to use the circuit identifier as the path trace identifier.
- In the Rx Trace Config field, specify the received path trace identifier. A common convention is to use the circuit identifier as the path trace identifier.

12. In the TTI-DAPI section, do the following:

- The Tx Trace and Rx Trace fields display the transmitted and received path trace values. A path trace identifier is a text string that identifies the circuit. The text string that identifies the circuit. SONET/SDH interfaces allow path trace bytes to be sent inband across the SONET/SDH link. Juniper Networks and other router manufacturers use these bytes to help diagnose misconfigurations and network errors by setting the transmitted path trace message so that it contains the system hostname and name of the physical interface. The received path trace value is the message received from the routing device at the other end of the fiber. The transmitted path trace value is the message that this routing device transmits.
- In the Tx Trace config field, specify the propagated path trace identifier. A common convention is to use the circuit identifier as the path trace identifier.
- In the Rx Trace Config field, specify the received path trace identifier. A common convention is to use the circuit identifier as the path trace identifier.

13. Click **Update** at the top of the dialog box to save the modified ODU settings.

You can click the **Refresh** (rotating arrow icon) button at the top of the dialog box to enable the latest settings be retrieved from the device and displayed.

You can collapse the contents of a particular section by clicking the minus sign (-) beside the header and expand the contents of a section by clicking the plus sign (+) beside the header.

Related Documentation

- [Configuring and Managing OTN Port Details of MX Series and PTX Series Routers for Easy Administration on page 1497](#)
- [Configuring and Managing OTU Details of MX Series and PTX Series Routers for Simplified Management on page 1505](#)
- [Configuring and Managing Optical PIC Details for Effective Provisioning on page 1517](#)

Configuring and Managing Optical PIC Details for Effective Provisioning

Instead of using Junos OS CLI statements and operational commands to configure OTN PIC settings and view the configured parameters, you can view an image of the OTN PIC using Connectivity Services Director to obtain an intuitive and high-level understanding of the settings and alarms. This view enables you to modify the OTN PIC settings to suit your network deployment needs in a simplified and optimal manner. Because the important OTN PIC settings can be configured alongside the visual representation of the entire chassis that is displayed, this method of managing the OTN PIC settings provides a consolidated and cohesive interface for easy administration of the network.

You can perform the following tasks in this dialog box:

- View the optical interface specifications that are currently applied on the device, such as the PIC state and PIC type
- Modify the existing parameters of the optical port to suit your network needs or resolve any alarms caused by certain interface settings

To configure the full C-band International Telecommunication Union (ITU)-Grid tunable optics for 10-Gigabit Ethernet or 100-Gigabit Ethernet dense wavelength-division multiplexing (DWDM) OTN PICs:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the device for which you want to define the optical port settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

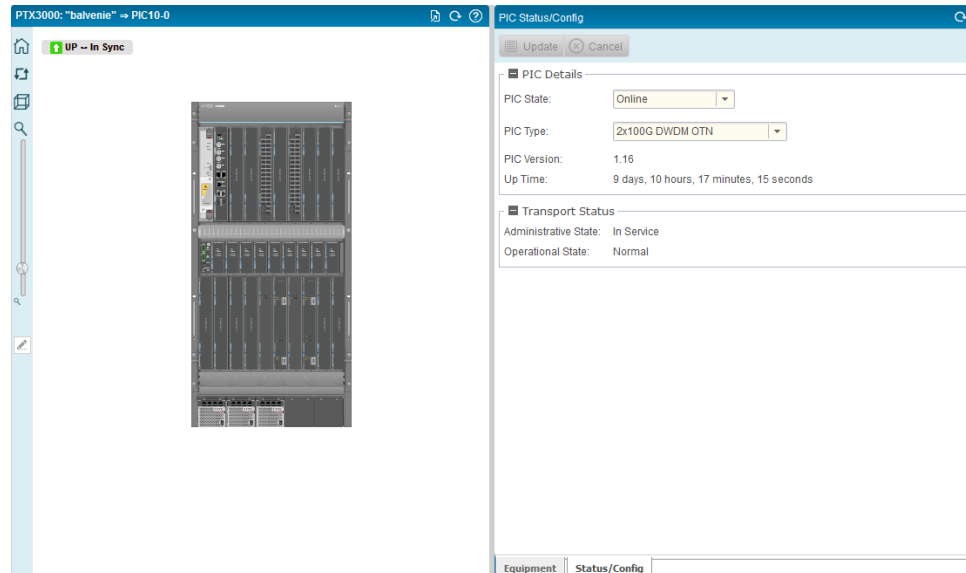
5. In the image of the device, select an OTN PIC, such as a 2-port 100-Gigabit Ethernet OTN PIC or a 100-Gigabit Ethernet PIC installed in a PTX Series router.

The Component Info dialog box is displayed on the right pane with the PIC specifications.

6. Click the **Status/Config** tab at the bottom of the dialog box.

The configuration settings that pertain to the optical interface are displayed in the PIC Status/Config dialog box as shown in [Figure 92 on page 1518](#).

Figure 92: PIC Status/Config Dialog Box



7. In the PIC Details section, do the following:
 - a. From the PIC State list, select **On Line** to turn on the PIC so that the PIC is running or **Off Line** to turn off the PIC so that the PIC is powered down. State is displayed only when a PIC resides in the slot.
 - b. From the PIC Type list, select the type of PIC, such as 2X100GE CFP2 OTN, 24X10GE SFPP OTN, 2x100G DWDM OTN, or 2x100GE CFP.
 - c. In the PIC version field, the PIC hardware version is displayed.
 - d. In the Uptime field, the number of days, hours, minutes, and seconds for which the PIC has been online is displayed.
8. In the Transport State section, the following fields are displayed:
 - Admin State—The administrative state of the port—In Service or Out of Service.
 - Operational State—The operational status of the port—link up (UP) or link down (DOWN).
9. Click **Update** to save the configured settings. Alternatively, click **Cancel** to discard the modified settings.

You can click the **Refresh** (rotating arrow icon) button at the top of the dialog box to enable the latest settings be retrieved from the device and displayed.

Related Documentation

- [Configuring and Managing OTN Port Details of MX Series and PTX Series Routers for Easy Administration on page 1497](#)

- [Configuring and Managing OTU Details of MX Series and PTX Series Routers for Simplified Management on page 1505](#)
- [Configuring and Managing ODU Details of MX Series and PTX Series Routers for Simplified Management on page 1512](#)

Configuring Threshold-Crossing Alarms for OTN Ports for Monitoring Link Performance

By monitoring the performance of links, you ensure that an end-to-end Ethernet service is always available over any path for a single link or multiple links spanning networks composed of multiple LANs. Link performance metrics enable operators to offer binding service-level agreements (SLAs) and generate new revenues from rate- and performance-guaranteed service packages that are customized to meet specific needs of their customers. To monitor link performance, you need to configure threshold-crossing alarms (TCAs) for optical transport network (OTN) ports.

TCAs are alarms that are activated when a certain configurable threshold—near-end measurement threshold or far-end measurement threshold—is crossed and remains so until the end of the 15-minute interval and the 24-hour interval for parameters such as optical channel transport unit (OTU) and optical data unit (ODU). A near-end measurement is associated with ingress data frames and a far-end measurement is associated with egress data frames.

You can configure TCAs for both the minimum and maximum values for gauges and the maximum values for counters. A gauge represents a non-negative integer, which may increase or decrease, but never exceeds a maximum value. A gauge has its maximum value whenever the information being modeled is greater than or equal to the maximum value. If the TCA parameter subsequently goes below the maximum value, the gauge also decreases. A counter represents a non-negative integer that monotonically increases until it reaches a maximum value of $2^{32}-1$.

The timely detection of TCAs is essential to proactively manage an interface. TCAs are not an indication of a fault, but rather an indication that the entity may be close to a fault. You can enable the TCA that you want monitor. You can keep the default threshold settings or change the settings.

To configure TCAs for OTN port interface parameters:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the device for which you want to define the OTN interface settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. In the image of the device, select an OTN interface or port—for example, a 100-Gigabit Ethernet OTN MIC installed in a PTX Series router.

The Optical Port dialog box is displayed. At the lower part of the dialog box, the OTU Section and ODU Section panes are displayed in a collapsed form.

6. Click the **Optical Port Section** header at the bottom of the dialog box.

The Optical Port Section pane is expanded and displayed. This pane contains the Equipment, Status/Config, and Performance tabs.


7. Click the **Performance** tab at the bottom of the pane.

The Optics PMs dialog box is displayed with the performance monitoring gauges and counters that pertain to the selected OTN port. This dialog box contains the Perf Mon and TCA Config tabs.


8. Click the **TCA Config** tab to configure TCAs for the various attributes.





The dialog box is refreshed to display the performance monitoring parameters shown in [Figure 93 on page 1521](#). Only a portion of the fields displayed in the dialog box are illustrated in the [Figure 93 on page 1521](#). These parameters can be edited inline.


Figure 93: TCA Config Tab of the Optics PMs Dialog Box


Optics PMs (last updated: 02:13:23 PM, March 14, 2016) 

Perf Mon | **TCA Config** | 15 Mins CFO ▾ | 24 Hours CD ▾

 Update  Cancel

PM Type/Group	Threshold-15Min	Threshold-24Hr	Enable
 Carrier Frequency Offset (MHz)			
CFO	--	--	--
CFO-Min	-5000	-5000	<input type="checkbox"/>
CFO-Max	5000	5000	<input type="checkbox"/>
CFO-Avg	--	--	--
 Chromatic Dispersion			
CD	--	--	--
CD-Min	--	--	--
CD-Max	--	--	--
CD-Avg	--	--	--
 Differential Group Delay			
DGD	--	--	--
DGD-Min	--	--	--
DGD-Max	--	--	--
DGD-Avg	--	--	--
 Module Temperature (°C)			
MT	--	--	--
MT-Min	-5	-5	<input type="checkbox"/>
MT-Max	75	75	<input type="checkbox"/>
MT-Avg	--	--	--

OTU PMs (last updated: 02:13:14 PM, March 14, 2016) 

ODU PMs (last updated: 02:12:19 PM, March 14, 2016) 

Equipment | **Status/Config** | Performance

Inline editing enables you to modify previously defined settings easily and quickly. Embedded editing is also enabled, which causes the grids showing the devices and interfaces to become modifiable directly; you do not need to highlight, edit, and save the changes every time.

A gray triangle in the upper-right corner of a field denotes that the value of that field or attribute has been modified.

- For the parameters under each performance monitoring category for which you want to modify the TCA value, click the value in the Threshold-15Min or Threshold-24Hr

columns. You can also select or clear the check box in the Enable column to enable or disable the TCA value for the specified parameter, respectively.

10. Click **Update** to save the configured threshold settings. Alternatively, click **Cancel** to discard the configuration.

**Related
Documentation**

- [Configuring Threshold-Crossing Alarms for OTUs for Monitoring Link Performance on page 1523](#)
- [Configuring Threshold-Crossing Alarms for ODUs for Monitoring Link Performance on page 1527](#)
- [Viewing Performance Monitoring Details of OTN Ports for Detecting and Diagnosing Faults on page 1530](#)
- [Viewing Performance Monitoring Details of OTUs for Detecting and Diagnosing Faults on page 1541](#)
- [Viewing Performance Monitoring Details of ODUs for Detecting and Diagnosing Faults on page 1549](#)

Configuring Threshold-Crossing Alarms for OTUs for Monitoring Link Performance

By monitoring the performance of links, you ensure that an end-to-end Ethernet service is always available over any path for a single link or multiple links spanning networks composed of multiple LANs. Link performance metrics enable operators to offer binding service-level agreements (SLAs) and generate new revenues from rate- and performance-guaranteed service packages that are customized to meet specific needs of their customers. To monitor link performance, you need to configure threshold-crossing alarms (TCAs) for optical channel transport unit (OTU) and optical data unit (ODU) of optical transport network (OTN) ports.

TCAs are alarms that are activated when a certain configurable threshold—near-end measurement threshold or far-end measurement threshold—is crossed and remains so until the end of the 15-minute interval and the 24-hour interval for parameters such as OTU and ODU. A near-end measurement is associated with ingress data frames and a far-end measurement is associated with egress data frames.

You can configure TCAs for both the minimum and maximum values for gauges and the maximum values for counters. A gauge represents a non-negative integer, which may increase or decrease, but never exceeds a maximum value. A gauge has its maximum value whenever the information being modeled is greater than or equal to the maximum value. If the TCA parameter subsequently goes below the maximum value, the gauge also decreases. A counter represents a non-negative integer that monotonically increases until it reaches a maximum value of $2^{32}-1$.

The timely detection of TCAs is essential to proactively manage an interface. TCAs are not an indication of a fault, but rather an indication that the entity may be close to a fault. You can enable the TCA that you want monitor. You can keep the default threshold settings or change the settings.

To configure TCAs for OTU parameters:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the device for which you want to define the optical port settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. In the the image of the device, select an OTN interface or port—for example, a 100-Gigabit Ethernet optical transport network (OTN) MIC installed in a PTX Series router.

The Optical Port dialog box is displayed. At the lower part of the dialog box, the OTU Section and ODU Section panes are displayed in a collapsed form.

6. Click the **OTU Section** header at the bottom of the dialog box.

The OTU Section pane is expanded and displayed. This pane contains the Equipment, Status/Config, and Performance tabs.

7. Click the **Performance** tab at the bottom of the pane.

The OTU PMs dialog box is displayed with the performance monitoring counters and metrics that pertain to the OTU. This dialog box contains the Perf Mon and TCA Config tabs. At the top-left corner of the PMs dialog box, the TCA Config tab (green right arrow enclosed in a square) is displayed.

8. Click the **TCA Config** tab to configure the TCAs for the different optical interface, OTU, or ODU attributes. The dialog box is refreshed to display the different performance monitoring parameters shown in [Figure 94 on page 1525](#). These parameters can be edited inline.

Figure 94: TCA Config Tab of the OTU PMs Dialog Box

OTU PMs (last updated: 02:14:34 PM, March 14, 2016)

Perf Mon
TCA Config
15 Mins OTU
24 Hours FEC

Update
Cancel

PM Type/Group	Threshold-15Min	Threshold-24Hr	Enable
OTU NE			
BBE	800	960	<input type="checkbox"/>
ES	135	162	<input type="checkbox"/>
SES	90	108	<input type="checkbox"/>
UAS	90	108	<input type="checkbox"/>
OTU FE			
BBE	800	960	<input type="checkbox"/>
ES	135	162	<input type="checkbox"/>
SES	90	108	<input type="checkbox"/>
UAS	90	108	<input type="checkbox"/>
FEC NE			
FEC-CorrectedErr	--	--	--
FEC-UncorrectedWords	--	--	--
BER NE			
BER-Max	--	--	--
BER-Min	0.01	0.01	<input type="checkbox"/>
BER-Avg	--	--	--

ODU PMs (last updated: 02:12:19 PM, March 14, 2016)

Equipment
Status/Config
Performance

Inline editing enables you to modify previously defined settings easily and quickly. Embedded editing is also enabled, which causes the grids showing the devices and interfaces to become modifiable directly; you do not need to highlight, edit, and save the changes every time.

A gray triangle in the upper-right corner of a field denotes that the value of that field or attribute has been modified.

- For the parameters under each performance monitoring category for which you want to modify the TCA value, click the value in the Threshold-15Min or Threshold-24Hr columns to set the TCA value for the 15-minute interval or 24-hour interval. You can

also select or clear the check box in the Enable column to enable or disable the TCA value for the specified parameter, respectively.

10. Click **Update** to save the configured threshold settings. Alternatively, click **Cancel** to discard the configuration.

**Related
Documentation**

- [Configuring Threshold-Crossing Alarms for OTN Ports for Monitoring Link Performance on page 1519](#)
- [Configuring Threshold-Crossing Alarms for ODUs for Monitoring Link Performance on page 1527](#)
- [Viewing Performance Monitoring Details of OTN Ports for Detecting and Diagnosing Faults on page 1530](#)
- [Viewing Performance Monitoring Details of OTUs for Detecting and Diagnosing Faults on page 1541](#)
- [Viewing Performance Monitoring Details of ODUs for Detecting and Diagnosing Faults on page 1549](#)

Configuring Threshold-Crossing Alarms for ODUs for Monitoring Link Performance

By monitoring the performance of links, you ensure that an end-to-end Ethernet service is always available over any path for a single link or multiple links spanning networks composed of multiple LANs. Link performance metrics enable operators to offer binding service-level agreements (SLAs) and generate new revenues from rate- and performance-guaranteed service packages that are customized to meet specific needs of their customers. To monitor link performance, you need to configure threshold-crossing alarms (TCAs) for optical channel transport unit (OTU) and optical data unit (ODU) of optical transport network (OTN) ports.

TCAs are alarms that are activated when a certain configurable threshold—near-end measurement threshold or far-end measurement threshold—is crossed and remains so until the end of the 15-minute interval and the 24-hour interval for parameters such as OTU and ODU. A near-end measurement is associated with ingress data frames and a far-end measurement is associated with egress data frames.

You can configure TCAs for both the minimum and maximum values for gauges and the maximum values for counters. A gauge represents a non-negative integer, which may increase or decrease, but never exceeds a maximum value. A gauge has its maximum value whenever the information being modeled is greater than or equal to the maximum value. If the TCA parameter subsequently goes below the maximum value, the gauge also decreases. A counter represents a non-negative integer that monotonically increases until it reaches a maximum value of $2^{32}-1$.

The timely detection of TCAs is essential to proactively manage an interface. TCAs are not an indication of a fault, but rather an indication that the entity may be close to a fault. You can enable the TCA that you want monitor. You can keep the default threshold settings or change the settings.

To configure TCAs for ODU parameters:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the device for which you want to define the optical port settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. In the the image of the device, select an OTN interface or port—for example, a 100-Gigabit Ethernet optical transport network (OTN) MIC installed in a PTX Series router.

The Optical Port dialog box is displayed. At the lower part of the dialog box, the OTU Section and ODU Section panes are displayed in a collapsed form.

6. Click the **ODU Path** header at the bottom of the dialog box.

The ODU Path pane is expanded and displayed. This pane contains the Equipment, Status/Config, and Performance tabs.

7. Click the **Performance** tab at the bottom of the pane.

The ODU PMs dialog box is displayed with the performance monitoring counters and metrics that pertain to the ODU. This dialog box contains the Perf Mon and TCA Config tabs.

8. Click the **TCA Config** tab to configure the TCAs for the different optical interface, OTU, or ODU attributes. The dialog box is refreshed to display the different performance monitoring parameters shown in [Figure 95 on page 1529](#). These parameters can be edited inline.

Figure 95: TCA Config Tab of the ODU PMs Dialog Box

Optics PMs (last updated: 02:13:23 PM, March 14, 2016)
OTU PMs (last updated: 02:14:34 PM, March 14, 2016)
ODU PMs (last updated: 02:15:37 PM, March 14, 2016)

Perf Mon
TCA Config
15 Mins ODU
24 Hours ODU

Update
Cancel

PM Type/Group	Threshold-15Min	Threshold-24Hr	Enable
ODU NE			
BBE	800	960	<input type="checkbox"/>
ES	135	162	<input type="checkbox"/>
SES	90	108	<input type="checkbox"/>
UAS	90	108	<input type="checkbox"/>
ODU FE			
BBE	800	960	<input type="checkbox"/>
ES	135	162	<input type="checkbox"/>
SES	90	108	<input type="checkbox"/>
UAS	90	108	<input type="checkbox"/>

Equipment
Status/Config
Performance

Inline editing enables you to modify previously defined settings easily and quickly. Embedded editing is enabled, which causes the grids showing the devices and interfaces to become modifiable directly; you do not need to highlight, edit, and save the changes every time.

A gray triangle in the upper-right corner of a field denotes that the value of that field or attribute has been modified.

- For the parameters under each performance monitoring category for which you want to modify the TCA value, click the value in the Threshold-15Min or Threshold-24Hr columns to set the TCA value for the 15-minute interval or 24-hour interval. You can

also select or clear the check box in the Enable column to enable or disable the TCA value for the specified parameter, respectively.

10. Click **Update** to save the configured threshold settings. Alternatively, click **Cancel** to discard the configuration.

**Related
Documentation**

- [Configuring Threshold-Crossing Alarms for OTN Ports for Monitoring Link Performance on page 1519](#)
- [Configuring Threshold-Crossing Alarms for OTUs for Monitoring Link Performance on page 1523](#)
- [Viewing Performance Monitoring Details of OTN Ports for Detecting and Diagnosing Faults on page 1530](#)
- [Viewing Performance Monitoring Details of OTUs for Detecting and Diagnosing Faults on page 1541](#)
- [Viewing Performance Monitoring Details of ODUs for Detecting and Diagnosing Faults on page 1549](#)

Viewing Performance Monitoring Details of OTN Ports for Detecting and Diagnosing Faults

To analyze and resolve any faults associated with optical transport network (OTN) ports, it is essential to view the diagnostic data, warnings, and alarms for transport performance monitoring. The different types of parameters related to performance monitoring that are retrieved from the OTN ports enable you to ensure service availability and monitor the performance of individual services and the network.

The performance monitoring capability of Connectivity Services Director helps you identify problems with the equipment, pinpoint security attacks, and analyze trends and categories of errors. This capability uses charts and grids to provide important and cohesive information about system conditions, discrepancies and malfunctioning, and protocols or components that need to be examined and debugged for better efficiency and working capacity. You can assess the performance of your network, not only at a point in time, but also over a period of time.

To view performance monitoring details of OTN interfaces:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the device for which you want to define the optical port settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. In the image of the device, select an OTN interface or port—for example, a 100-Gigabit Ethernet optical transport network (OTN) MIC installed in a PTX Series router.

The Optical Port dialog box is displayed. At the lower part of the dialog box, the OTU Section and ODU Section panes are displayed in a collapsed form.

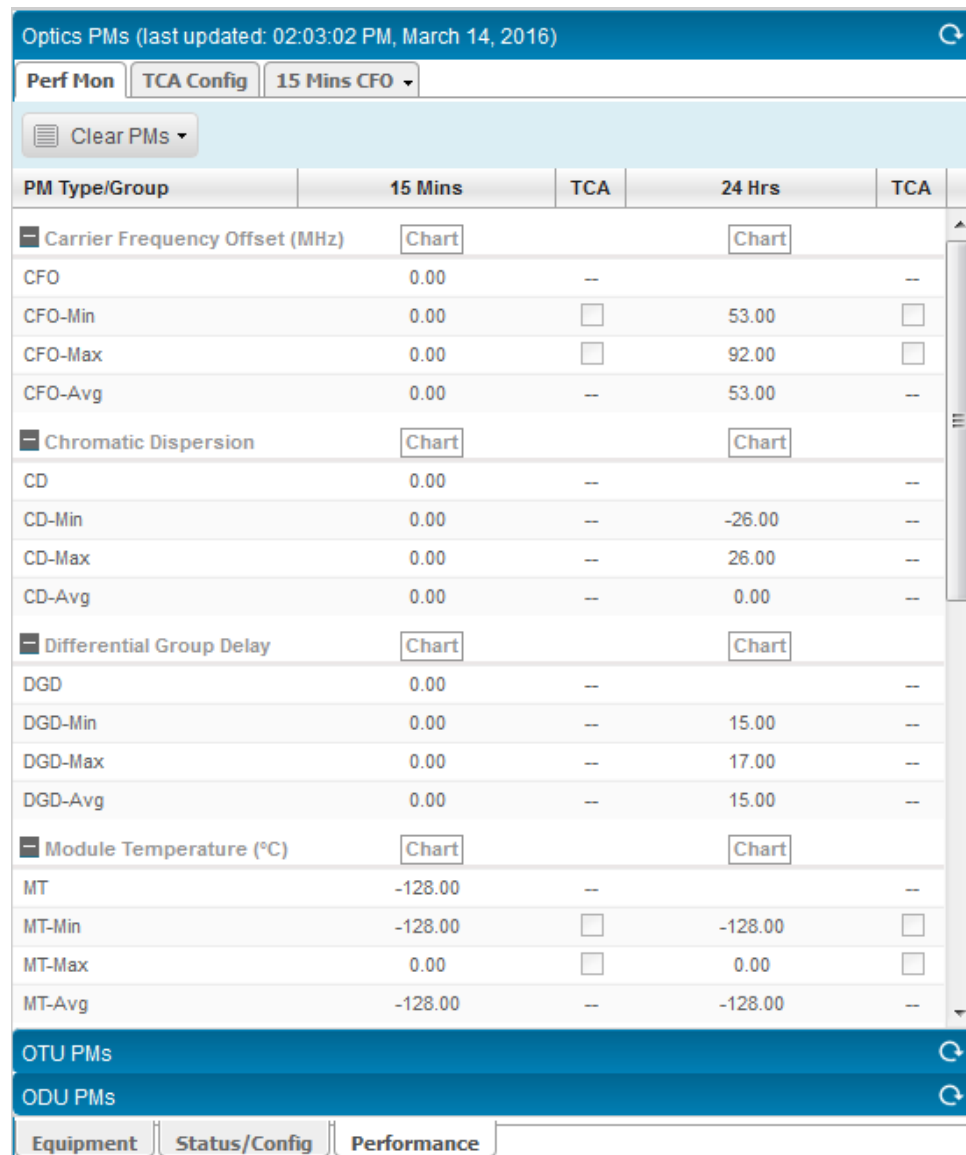
6. Click the **Optical Port Section** header at the bottom of the dialog box.

The Optical Port Section pane is expanded and displayed. This pane contains the Equipment, Status/Config, and Performance tabs.

7. Click the **Performance** tab at the bottom of the pane.

This pane contains the Perf Mon and TCA Config tabs. The Perf Mon tab of the Optics PMs dialog box is displayed as shown in [Figure 96 on page 1532](#). Only a portion of the fields displayed in the dialog box are illustrated in the figure.

Figure 96: Perf Mon Tab of the Optics PMs Dialog Box



The following fields are displayed in the Perf Mon tab of the Optics PMs dialog box. The date and time at which the dialog box was last refreshed is shown.

- Carrier Frequency Offset (MHz)—Carrier frequency offset in megahertz (mHz), which denotes the difference between the carriers (frequency shift in the receive spectrum) between the expected Rx carrier frequency and the actual carrier frequency

CFO—Threshold values for carrier frequency offset

CFO-Min—Low threshold setting trigger when the carrier frequency offset falls below this minimum value

CFO-Avg—Average threshold setting trigger when the carrier frequency offset crosses this average value

CFO-Max—High threshold setting trigger when the carrier frequency offset rises above this maximum value

- Chromatic Dispersion—Lane or residual chromatic dispersion measured at the Rx transceiver port, which denotes the spreading of the signal in time resulting from the different speeds of light rays

CD—Threshold values for chromatic dispersion

CD-Min—Minimum value of the residual chromatic dispersion measured at the Rx transceiver port

CD-Avg—Average value of the residual chromatic dispersion measured at the Rx transceiver port

CD-Max—Maximum value of the residual chromatic dispersion measured at the Rx transceiver port

- Differential Group Delay—Lane differential group delay, which denotes the time difference between the fractions of a pulse that are transmitted in the two principal states of polarization of an optical signal. For distances greater than several kilometers, and assuming random (strong) polarization mode coupling, DGD in a fiber can be statistically modeled as having a Maxwellian distribution.

DGD—Threshold values for differential group delay

DGD-Min—Minimum value of the differential group delay below which a TC is triggered

DGD-Avg—Average value of the differential group delay at which TCA is triggered

DGD-Max—Maximum value of the differential group delay above which a TCA is triggered

- Module Temperature (°C)—Module temperature, which denotes the laser temperature in Celsius

MT—Threshold values for module temperature

MT-Min—High laser temperature in Celsius below which a TCA is sent

MT-Avg—Average laser temperature in Celsius at which a TCA is sent

MT-Max—Maximum laser temperature in Celsius above which a TCA is sent

- Optical Lane Q2 Factor—Quality (Q or Q2) factor value estimated at the Rx transceiver port

Lane Q2 factor—Threshold values for the quality factor

Lane Q2 factor-Min—Minimum value of the quality factor estimated at the Rx transceiver port below which a TCA is sent

Lane Q2 factor-Avg—Average value of the quality factor estimated at the Rx transceiver port at which a TCA is sent

Lane Q2 factor-Max—Maximum value of the quality factor estimated at the Rx transceiver port above which a TCA is sent

- Signal to Noise Ratio—Signal-to-noise ratio estimated at the Rx transceiver port

SNR—Threshold values for signal-to-noise ratio

SNR-Min—Minimum value of the signal-to-noise ratio estimated at the Rx transceiver port below which a TCA is sent

SNR-Avg—Average value of the signal-to-noise ratio estimated at the Rx transceiver port

SNR-Max—Maximum value of the signal-to-noise ratio estimated at the Rx transceiver port above which a TCA is sent

- Optical Tx Output Power—Transmitted laser optical output power in dBm

Tx-Pwr—Threshold values for transmitted laser output power

TxPwr-Min—Minimum value of the transmitted laser output power in dBm below which a TCA is sent

TxPwr-Avg—Average value of the transmitted laser output power in dBm at which a TCA is sent

TxPwr-Max—Maximum value of the transmitted laser output power above which a TCA is sent

- Optical Rx Input Power—Received laser optical input power in dBm

Rx-Pwr—Threshold values for received laser input power

RxPwr-Min—Minimum value of the received laser input power in dBm below which a TCA is sent

RxPwr-Avg—Average value of the received laser power in dBm at which a TCA is sent

RxPwr-Max—Maximum value of the received input power in dBm above which a TCA is sent

On the Perf Mon tab, for the TCA column, either a minus sign (–) is displayed that denotes that an alarm for threshold-exceed is not configured or a check mark is displayed and grayed out that indicates that the TCA for the particular attribute is configured.

8. In the 15 Mins column, click the **Chart** button for the performance monitoring parameter set for which you want to view the statistics for the last 15 minutes. This option enables you to view the statistics in a chart form. Performance monitoring information for the

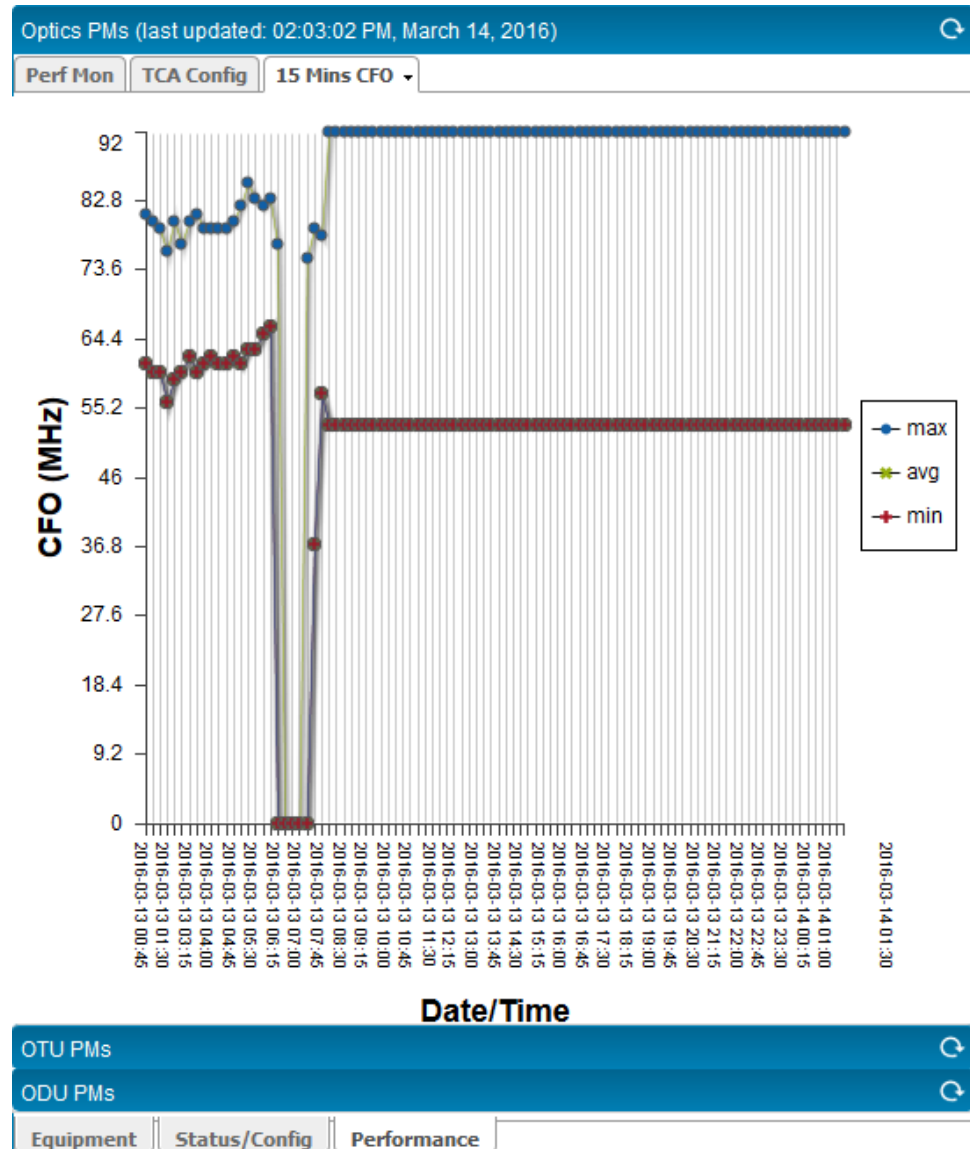
different parameters are displayed for the current 15-minute interval. By default, 96 records of 15-minute intervals are displayed.

A 15-Min *parameter-name* tab is displayed beside the TCA Config tab at the top-left corner of the Optics PMs dialog box. A graphical format of the statistics for the specified parameter is displayed on this tab.

9. Click the **15 Mins *parameter name*** tab.
 - a. Select one of the following options from the drop-down menu:

- Select **View Chart** or the graphical icon (elliptical curve symbol) to display the chart of performance monitoring statistical metrics. A line graph is displayed with date and time along the horizontal axis and the parameter along the vertical axis as shown in [Figure 97 on page 1536](#). A color-coding format is used to display the different lines, and legends reference the parameter names corresponding to the lines displayed. Mouse over the points in the line graph to expand and show the value of the performance monitoring counters at a particular time.

Figure 97: 15 Mins Parameter-Name Tab of the Optics PMs Dialog Box



- Select **View Grid** to switch over to the tabular format of display of performance monitoring statistics.

The records are displayed in tabular format. A serial number of the count of entries, the day, month, and year at which the entry was collected, and the time

at which the entry was collected are displayed. The timestamp is the UTC time in the database that is mapped to the local time zone of the client computer.

- Select **Save Chart**, when you view the performance monitoring statistics in graphical format, to save the graph to a Microsoft Excel file, as a .png image. Click the pin icon on the upper-left corner to revert the tab to the original container panel.
- Select **Popout Tab** or the light blue triangle icon to view the dialog box as a separate window.

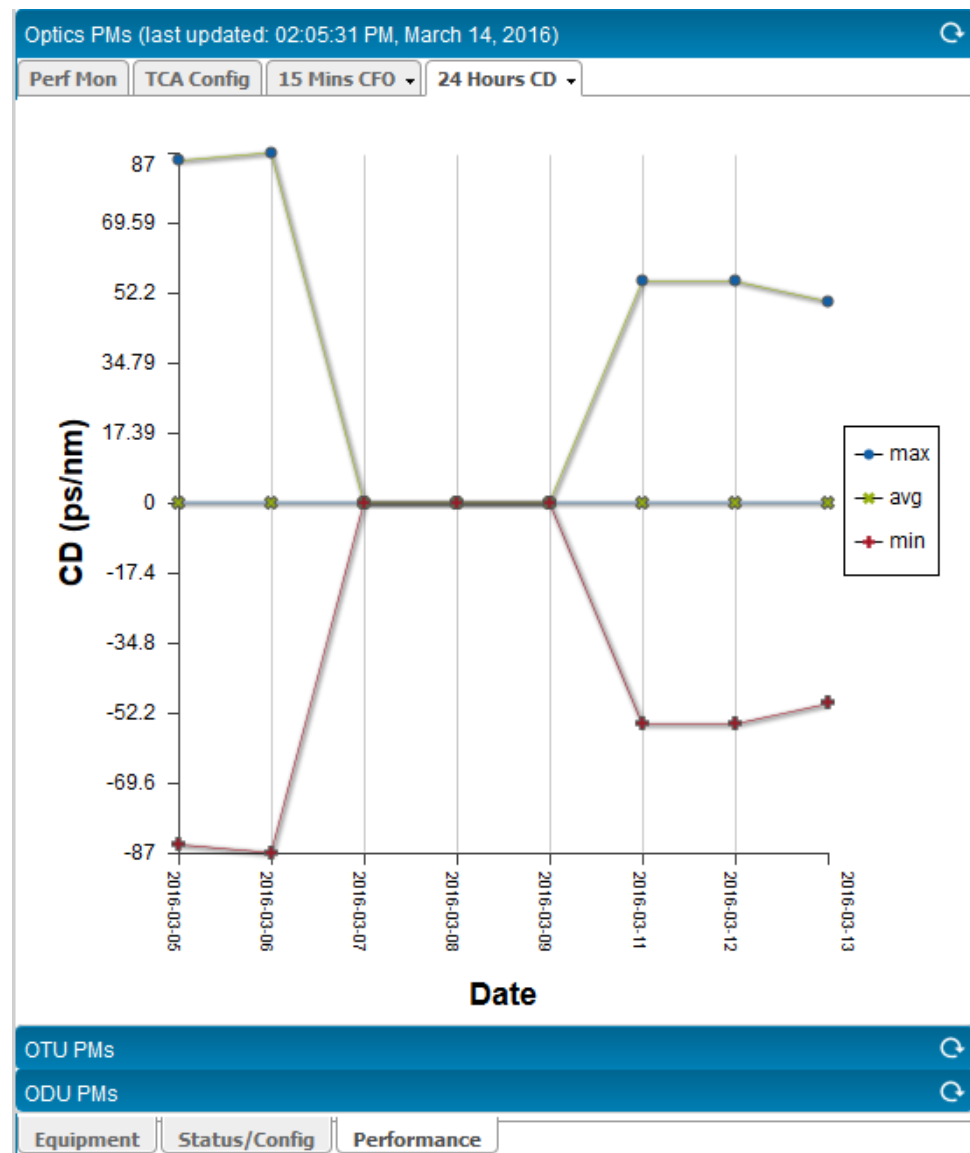
In the pop-up dialog box, you can do one of the following:

- In the From Date field, pull down the calendar and select the start date of the search. In the To Date field, pull down the calendar and select the end date of the search.
- Click **Reload** to refresh the contents and display the updated information for the specified time period.
- Click **Export Data** to transfer the data in graphical or statistical format to a spreadsheet or other business applications for future reference and archival. The comma-separated value (CSV) format takes the raw data from the report and delineates the fields with commas so that the data is imported into popular spreadsheet programs.
- Click the **View Chart** button at the top-left corner of the dialog box to view the statistics in graphical format. Alternatively, click the **View Grid** button at the top-left corner of the dialog box to view the statistics in tabular format. The View Chart/Grid button is a toggle button.
- Click **OK** to close the pop-up dialog box. Alternatively, press Esc to close the dialog box after you complete viewing the statistical details.
- Click **Close** to close the 15-Min *parameter-name* tab.

10. In the 24-Hrs column, click the **Chart** button for the performance monitoring parameter set for which you want to view the statistics for the previous day. This option enables you to view the statistics in a chart form. Performance monitoring information for the different parameters are displayed for the current 24-hour interval. By default, records pertaining to the last 30 days are displayed when you view the performance monitoring counters for the 24-hour duration.

A 24 Hours *parameter-name* tab is displayed beside the TCA Config tab at the top-left corner of the Optics PMs dialog box as shown in [Figure 98 on page 1538](#). A graphical format of the statistics for the specified parameter is displayed on this tab.

Figure 98: 24 Hours Parameter-Name Tab of the Optics PMs Dialog Box



11. Click the **24 Hours parameter name** tab.
 - a. Select one of the following options from the drop-down menu:

- Select **View Chart** or the graphical icon (elliptical curve symbol) to display the chart of performance monitoring statistical metrics. A line graph is displayed with date along the horizontal axis and the parameter along the vertical axis. A color-coding format is used to display the different lines, and legends reference the parameter names corresponding to the lines displayed. Mouse over the points in the line graph to expand and show the value of the performance monitoring counters at a particular time.
- Select **View Grid** to switch over to the tabular format of display of performance monitoring statistics.
- Select **Save Chart**, when you view the performance monitoring statistics in graphical format, to save the graph to a Microsoft Excel file, as a .png image. Click the pin icon on the upper-left corner to revert the tab to the original container panel.
- Select **Popout Tab** or the light blue triangle icon to view the dialog box as a separate window.

In the pop-up dialog box, you can do one of the following:

- In the From Date field, pull down the calendar and select the start date of the search. In the To Date field, pull down the calendar and select the end date of the search. Click **Reload** to refresh the contents and display the updated information for the specified time period.
 - Click **Export Data** to transfer the data in graphical or statistical format to a spreadsheet or other business applications for future reference and archival. The comma-separated value (CSV) format takes the raw data from the report and delineates the fields with commas so that the data is imported into popular spreadsheet programs.
 - Click the **View Chart** button at the top-left corner of the dialog box to view the statistics in graphical format. Alternatively, click the **View Grid** button at the top-left corner of the dialog box to view the statistics in tabular format. The View Chart/Grid button is a toggle button.
 - Click **OK** to close the pop-up dialog box. Alternatively, press Esc to close the dialog box after you complete viewing the statistical details.
 - Click **Close** to close the 24 Hours *parameter-name* tab.
12. Click the **Clear PMs** button at the top of the Optics PMs dialog box, and select one of the following values from the drop-down menu to clear optics information from the transport performance monitoring data.
- **Current**—Clear the optics information for the current interval, such as 15-minute interval or 24-hour interval, for which monitoring data is being collected.
 - **Current Day**—Clear the optics information for the current 24 hours.
 - **All Intervals**—Clear the optics information for the current 15-minute interval, the 96 records of 15-minute intervals, the current day, and the previous day

After you select one of the intervals for which monitoring data must be deleted, a Clear Optics PMs dialog box is displayed to indicate that a job is triggered to delete the monitoring information from the module on the device. The job ID, start and end times of the job, percentage of completion, and status of the job are displayed.

13. Click **Close** to close the job dialog box; alternatively, click **Refresh** to update the job status and view.

You can use the Jobs Management page (by clicking the System icon on the banner and selecting Manage Jobs) to track the status of this job.

You can click the **Refresh** (rotating arrow icon) button at the top of the Optics PMs dialog box to enable the latest performance monitoring statistics to be polled and displayed.

**Related
Documentation**

- [Configuring Threshold-Crossing Alarms for OTN Ports for Monitoring Link Performance on page 1519](#)
- [Configuring Threshold-Crossing Alarms for OTUs for Monitoring Link Performance on page 1523](#)
- [Configuring Threshold-Crossing Alarms for ODUs for Monitoring Link Performance on page 1527](#)
- [Viewing Performance Monitoring Details of OTUs for Detecting and Diagnosing Faults on page 1541](#)
- [Viewing Performance Monitoring Details of ODUs for Detecting and Diagnosing Faults on page 1549](#)

Viewing Performance Monitoring Details of OTUs for Detecting and Diagnosing Faults

The performance monitoring capability in Connectivity Services Director displays information about the health of your network and changing conditions of your optical channel transport units (OTUs). Use this diagnosis and detection mechanism to identify problems with the equipment, pinpoint security attacks, or to analyze trends and categories of errors. This feature includes fault-monitoring details in the dashboard, in monitoring pages, and on a dedicated page that displays alarms, events, and system log messages that are generated. Performance monitoring parameters can be viewed in both chart and statistical formats. These charts and statistical details provide essential and cohesive information about system conditions, any discrepancies and malfunctioning, and protocols or components that need to be examined and debugged for better efficiency and working capacity. You can assess the performance of your network, not only at a point in time, but also over a period of time. This feature enables you to determine trending and network-health parameters; for example, whether service-level agreements (SLAs) have been violated.

To view performance monitoring details of OTUs:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the device for which you want to define the optical port settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. In the image of the device, select an OTN interface or port—for example, a 100-Gigabit Ethernet optical transport network (OTN) MIC installed in a PTX Series router.

The Optical Port dialog box is displayed. At the lower part of the dialog box, the OTU Section and ODU Section panes are displayed in a collapsed form.

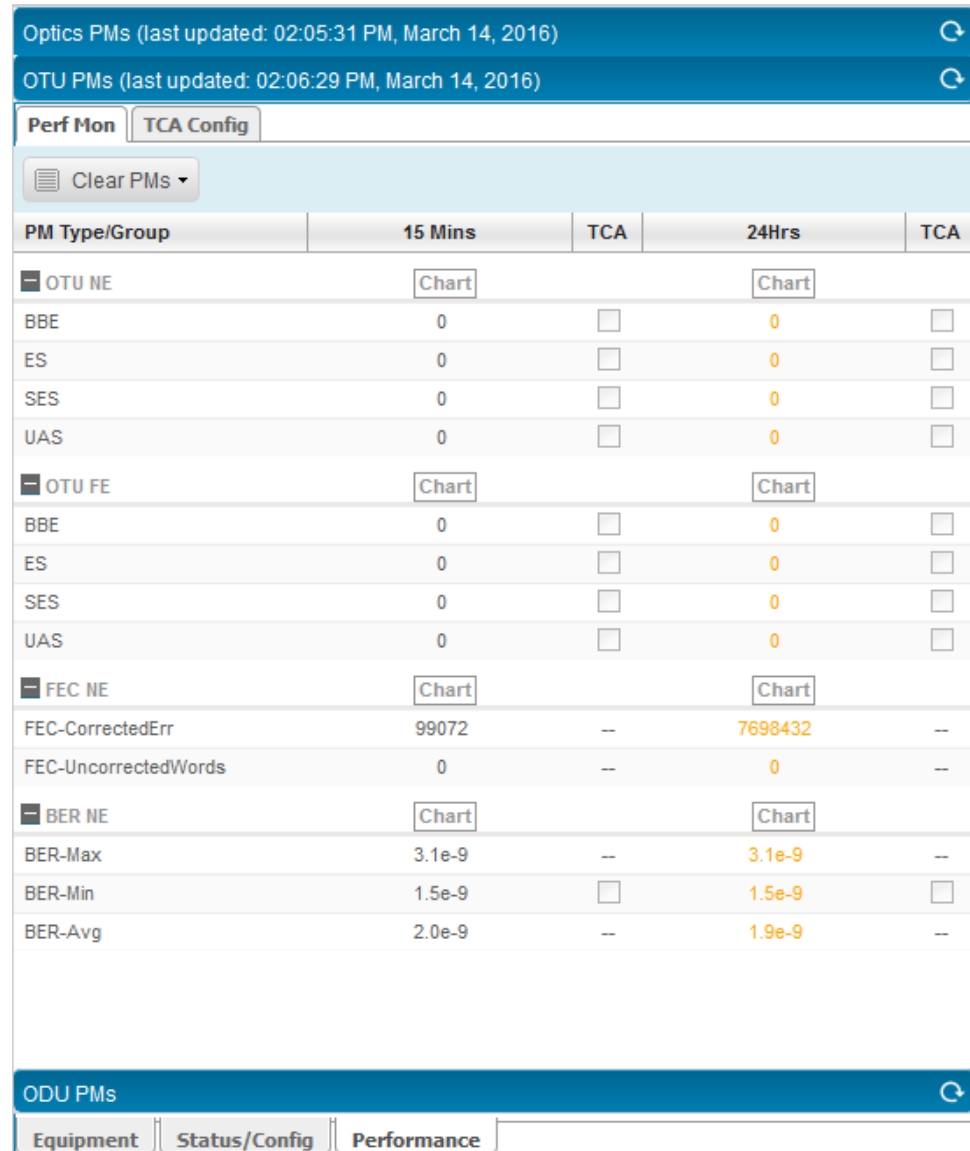
6. Click the **OTU Section** header at the bottom of the dialog box.

The OTU Section pane is expanded and displayed. This pane contains the Equipment, Status/Config, and Performance tabs.

- Click the **Performance** tab at the bottom of the pane.

This pane contains the Perf Mon and TCA Config tabs. The Perf Mon tab of the OTU PMs dialog box is expanded and displayed as shown in [Figure 99 on page 1542](#). Only a portion of the parameters displayed in this dialog box are illustrated in this figure.

Figure 99: Perf Mon Tab of the OTU PMs Dialog Box



The following fields are displayed in the Perf Mon tab of the OTU PMs dialog box. The date and time at which the dialog box was last refreshed is shown.

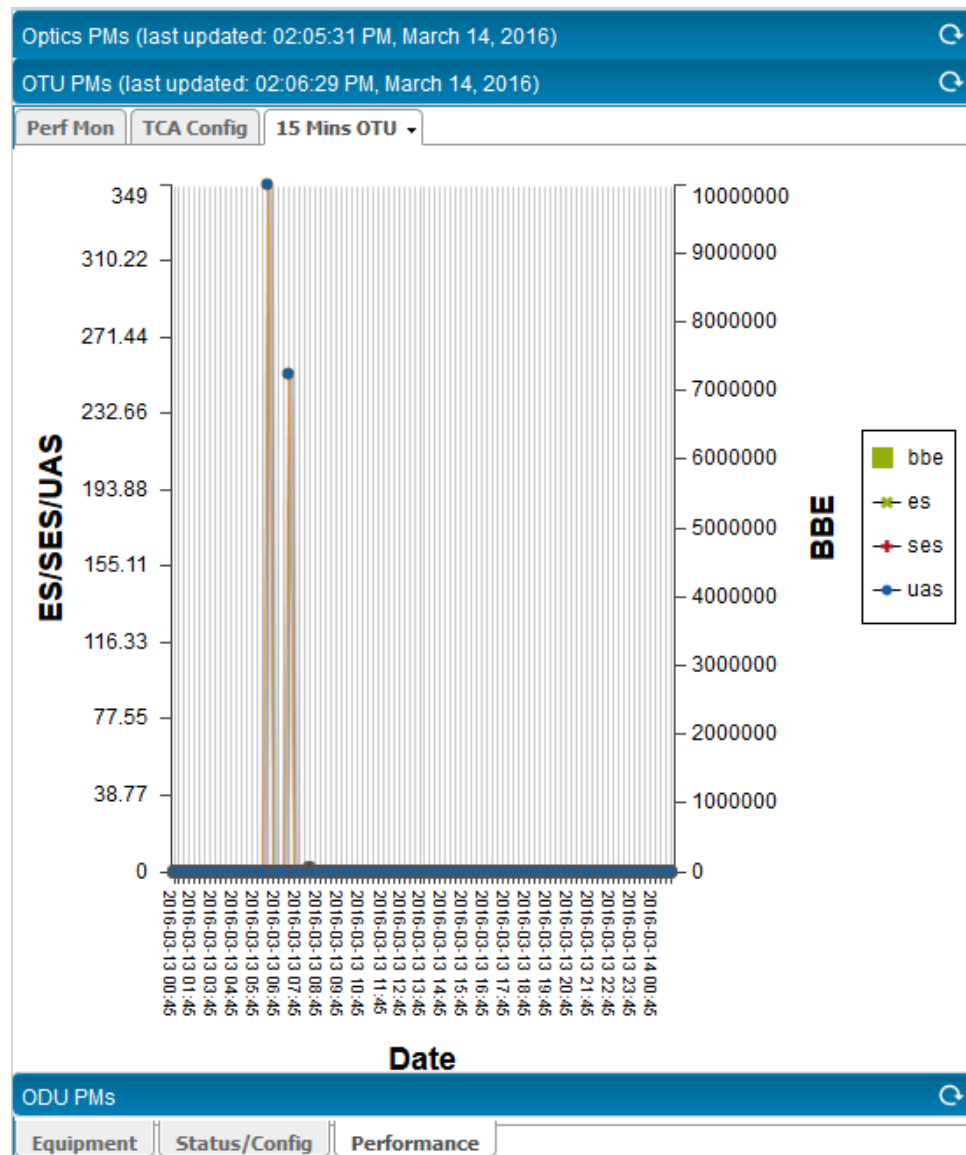
- OTU FE—OTU far-end measurement threshold
 - BBE—Background block error threshold-crossing defect trigger for OTU far-end
 - ES—Errored seconds threshold-crossing defect trigger for OTU far-end
 - SES—Severely errored seconds threshold-crossing defect trigger for OTU far-end
 - UAS—Unavailable seconds threshold-crossing defect trigger for OTU far-end
- OTU NE—OTU near-end measurement threshold for OTU near-end
 - BBE—Background block error threshold-crossing defect trigger for OTU near-end
 - ES—Errored seconds threshold-crossing defect trigger for OTU near-end
 - SES—Severely errored seconds threshold-crossing defect trigger for OTU near-end
 - UAS—Unavailable seconds threshold-crossing defect trigger for OTU near-end
- FEC NE (OTU only)—Near-end forward error correction threshold-crossing defect trigger
 - FEC-CorrectedErrMin—Forward error correction Corrected Errors counter
 - FEC-UncorrectedWords—Forward error correction Uncorrected Words counter
 - FECMax—Maximum forward error correction
- BER NE (OTU only)—Near-end bit error rate threshold-crossing defect trigger
 - BER-Min—Minimum bit error rate for OTU near-end
 - BER-Avg—Average bit error rate for OTU near-end
 - BERMax—Maximum bit error rate for OTU near-end

On the Perf Mon tab, for the TCA column, either a minus sign (–) is displayed that denotes that an alarm for threshold-exceed is not configured or a check mark is displayed and grayed out that indicates that the TCA for the particular attribute is configured.

In the 15 Mins column, click the **Chart** button for the performance monitoring parameter set for which you want to view the statistics for the last 15 minutes. This option enables you to view the statistics in a chart form. Performance monitoring information for the different parameters are displayed for the current 15-minute interval. By default, 96 records of 15-minute intervals are displayed.

A 15-Min *parameter-name* tab is displayed beside the TCA Config tab at the top-left corner of the Optics PMs dialog box as shown in [Figure 100 on page 1544](#). A graphical format of the statistics for the specified parameter is displayed on this tab.

Figure 100: 15 Mins Parameter-Name Tab of the OTU PMs Dialog Box



8. Click the **15 Mins parameter name** tab.
 - a. Select one of the following options from the drop-down menu:

- Select **View Chart** or the graphical icon (elliptical curve symbol) to display the chart of performance monitoring statistical metrics. A line graph is displayed with date and time along the horizontal axis and the parameter along the vertical axis. A color-coding format is used to display the different lines, and legends reference the parameter names corresponding to the lines displayed. Mouse over the points in the line graph to expand and show the value of the performance monitoring counters at a particular time.
- Select **View Grid** to switch over to the tabular format of display of performance monitoring statistics.

The records are displayed in tabular format. A serial number of the count of entries, the day, month, and year at which the entry was collected, and the time at which the entry was collected are displayed. The timestamp is the UTC time in the database that is mapped to the local time zone of the client computer.

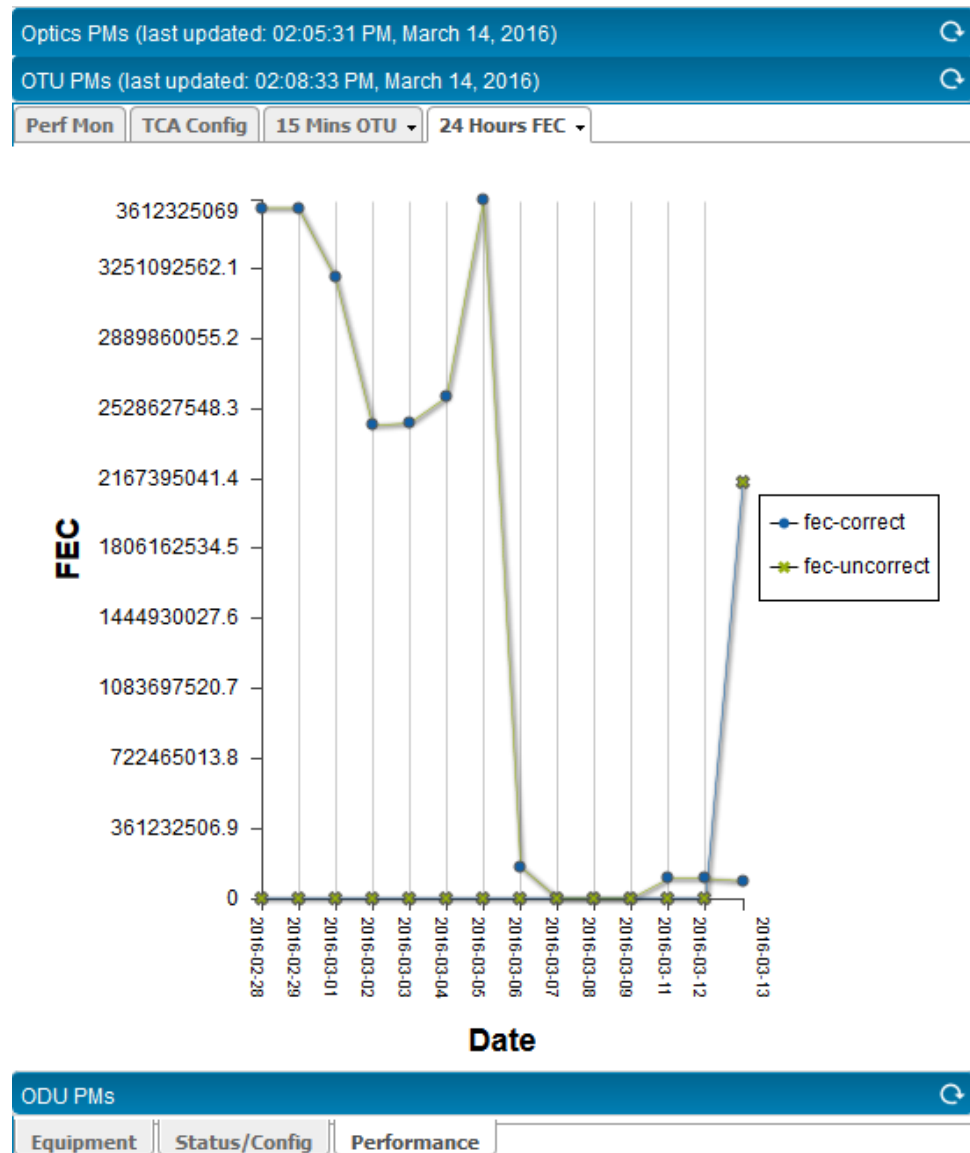
- Select **Save Chart**, when you view the performance monitoring statistics in graphical format, to save the graph to a Microsoft Excel file, as a .png image. Click the pin icon on the upper-left corner to revert the tab to the original container panel.
- Select **Popout Tab** or the light blue triangle icon to view the dialog box as a separate window.

In the pop-up dialog box, you can do one of the following:

- In the From Date field, pull down the calendar and select the start date of the search. In the To Date field, pull down the calendar and select the end date of the search.
 - Click **Reload** to refresh the contents and display the updated information for the specified time period.
 - Click **Export Data** to transfer the data in graphical or statistical format to a spreadsheet or other business applications for future reference and archival. The comma-separated value (CSV) format takes the raw data from the report and delineates the fields with commas so that the data is imported into popular spreadsheet programs.
 - Click the **View Chart** button at the top-left corner of the dialog box to view the statistics in graphical format. Alternatively, click the **View Grid** button at the top-left corner of the dialog box to view the statistics in tabular format. The View Chart/Grid button is a toggle button.
 - Click **OK** to close the pop-up dialog box. Alternatively, press Esc to close the dialog box after you complete viewing the statistical details.
 - Click **Close** to close the 15-Min *parameter-name* tab.
9. In the 24-Hrs column, click the **Chart** button for the performance monitoring parameter set for which you want to view the statistics for the previous day. This option enables you to view the statistics in a chart form. By default, records pertaining to the last 30 days are displayed when you view the performance monitoring counters for the 24-hour duration.

A 24 Hours *parameter-name* tab is displayed beside the TCA Config tab at the top-left corner of the Optics PMs dialog box as shown in [Figure 101 on page 1546](#). A graphical format of the statistics for the specified parameter is displayed on this tab.

Figure 101: 24 Hours Parameter-Name Tab of the OTU PMs Dialog Box



10. Click the **24 Hours *parameter name*** tab.

a. Select one of the following options from the drop-down menu:

- Select **View Chart** or the graphical icon (elliptical curve symbol) to display the chart of performance monitoring statistical metrics. A line graph is displayed with date along the horizontal axis and the parameter along the vertical axis. A color-coding format is used to display the different lines, and legends reference the parameter names corresponding to the lines displayed. Mouse over the points in the line graph to expand and show the value of the performance monitoring counters at a particular time.
- Select **View Grid** to switch over to the tabular format of display of performance monitoring statistics.
- Select **Save Chart**, when you view the performance monitoring statistics in graphical format, to save the graph to a Microsoft Excel file, as a .png image. Click the pin icon on the upper-left corner to revert the tab to the original container panel.
- Select **Popout Tab** or the light blue triangle icon to view the dialog box as a separate window.

In the pop-up dialog box, you can do one of the following:

- In the From Date field, pull down the calendar and select the start date of the search. In the To Date field, pull down the calendar and select the end date of the search. Click **Reload** to refresh the contents and display the updated information for the specified time period.
 - Click **Export Data** to transfer the data in graphical or statistical format to a spreadsheet or other business applications for future reference and archival. The comma-separated value (CSV) format takes the raw data from the report and delineates the fields with commas so that the data is imported into popular spreadsheet programs.
 - Click the **View Chart** button at the top-left corner of the dialog box to view the statistics in graphical format. Alternatively, click the **View Grid** button at the top-left corner of the dialog box to view the statistics in tabular format. The View Chart/Grid button is a toggle button.
 - Click **OK** to close the pop-up dialog box. Alternatively, press Esc to close the dialog box after you complete viewing the statistical details.
 - Click **Close** to close the 24 Hours *parameter-name* tab.
11. Click the **Clear PMs** button at the top of the dialog box, and select one of the following values from the drop-down menu to clear OTU information from the transport performance monitoring data.
 - **Current**—Clear the OTU information for the current interval, such as 15-minute interval or 24-hour interval, for which monitoring data is being collected.
 - **Current Day**—Clear the OTU information for the current 24 hours.
 - **All Intervals**—Clear the OTU information for the current 15-minute interval, the 96 records of 15-minute intervals, the current day, and the previous day

After you select one of the intervals for which monitoring data must be deleted, a Clear Optics PMs dialog box is displayed to indicate that a job is triggered to delete the monitoring information from the module on the device. The job ID, start and end times of the job, percentage of completion, and status of the job are displayed.

12. Click **Close** to close the job dialog box; alternatively, click **Refresh** to update the job status and view.

You can use the Jobs Management page (by clicking the System icon on the banner and selecting Manage Jobs) to track the status of this job.

You can click the **Refresh** (rotating arrow icon) button at the top of the dialog box to enable the latest performance monitoring statistics to be polled and displayed.

**Related
Documentation**

- [Configuring Threshold-Crossing Alarms for OTN Ports for Monitoring Link Performance on page 1519](#)
- [Configuring Threshold-Crossing Alarms for OTUs for Monitoring Link Performance on page 1523](#)
- [Configuring Threshold-Crossing Alarms for ODUs for Monitoring Link Performance on page 1527](#)
- [Viewing Performance Monitoring Details of OTN Ports for Detecting and Diagnosing Faults on page 1530](#)
- [Viewing Performance Monitoring Details of ODUs for Detecting and Diagnosing Faults on page 1549](#)

Viewing Performance Monitoring Details of ODUs for Detecting and Diagnosing Faults

To analyze and resolve any faults associated with optical channel data units (ODUs) of OTN ports, it is essential to view the diagnostic data, warnings, and alarms for transport performance monitoring. The different types of parameters related to performance monitoring that are retrieved from the ODUs enable you to ensure service availability and verify or monitor individual services and the service network performance.

The performance monitoring capability in Connectivity Services Director displays information about the health of your network and changing conditions of the OTUs of OTN ports. Use this diagnosis and detection mechanism to identify problems with the equipment, pinpoint security attacks, or to analyze trends and categories of errors. This feature includes fault-monitoring details in the dashboard, in monitoring pages, and on a dedicated page that displays alarms, events, and system log messages that are generated. Performance monitoring parameters can be viewed in both chart and statistical formats. These charts and statistical details provide essential and cohesive information about system conditions, any discrepancies and malfunctioning, and protocols or components that need to be examined and debugged for better efficiency and working capacity. You can assess the performance of your network, not only at a point in time, but also over a period of time. This feature enables you to determine trending and network-health parameters; for example, whether service-level agreements (SLAs) have been violated.

To view performance monitoring details of ODUs:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the device for which you want to define the optical port settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. Select an optical interface in the image of the device.

The Optical Port dialog box is displayed on the right pane.











6. Click the **ODU Path** header at the bottom of the dialog box.

The ODU Path pane is expanded and displayed. This pane contains the Equipment, Status/Config, and Performance tabs.

- Click the **Performance** tab at the bottom of the pane.

This pane contains the Perf Mon and TCA Config tabs. The Perf Mon tab of the ODU PMs dialog box is displayed as shown in [Figure 102 on page 1550](#).

Figure 102: Perf Mon Tab of the ODU PMs Dialog Box

Optics PMs (last updated: 02:05:31 PM, March 14, 2016) 				
OTU PMs (last updated: 02:08:33 PM, March 14, 2016) 				
ODU PMs (last updated: 02:10:06 PM, March 14, 2016) 				
Perf Mon TCA Config				
 Clear PMs ▾				
PM Type/Group	15 Mins	TCA	24 Hrs	TCA
 ODU NE  				
BBE	0	<input type="checkbox"/>	0	<input type="checkbox"/>
ES	0	<input type="checkbox"/>	0	<input type="checkbox"/>
SES	0	<input type="checkbox"/>	0	<input type="checkbox"/>
UAS	0	<input type="checkbox"/>	0	<input type="checkbox"/>
 ODU FE  				
BBE	0	<input type="checkbox"/>	0	<input type="checkbox"/>
ES	0	<input type="checkbox"/>	0	<input type="checkbox"/>
SES	0	<input type="checkbox"/>	0	<input type="checkbox"/>
UAS	0	<input type="checkbox"/>	0	<input type="checkbox"/>

Equipment	Status/Config	Performance
------------------	----------------------	--------------------

The following fields are displayed in the Perf Mon tab of the ODU PMs dialog box. The date and time at which the dialog box was last refreshed is shown.

- ODU FE—ODU far-end measurement threshold
- BBE—Background block error threshold-crossing defect trigger for ODU far-end

ES—Errored seconds threshold-crossing defect trigger for ODU far-end

SES—Severely errored seconds threshold-crossing defect trigger for ODU far-end

UAS—Unavailable seconds threshold-crossing defect trigger for ODU far-end

- ODU NE—ODU near-end measurement threshold for ODU near-end

BBE—Background block error threshold-crossing defect trigger for ODU near-end

ES—Errored seconds threshold-crossing defect trigger for ODU near-end

SES—Severely errored seconds threshold-crossing defect trigger for ODU near-end

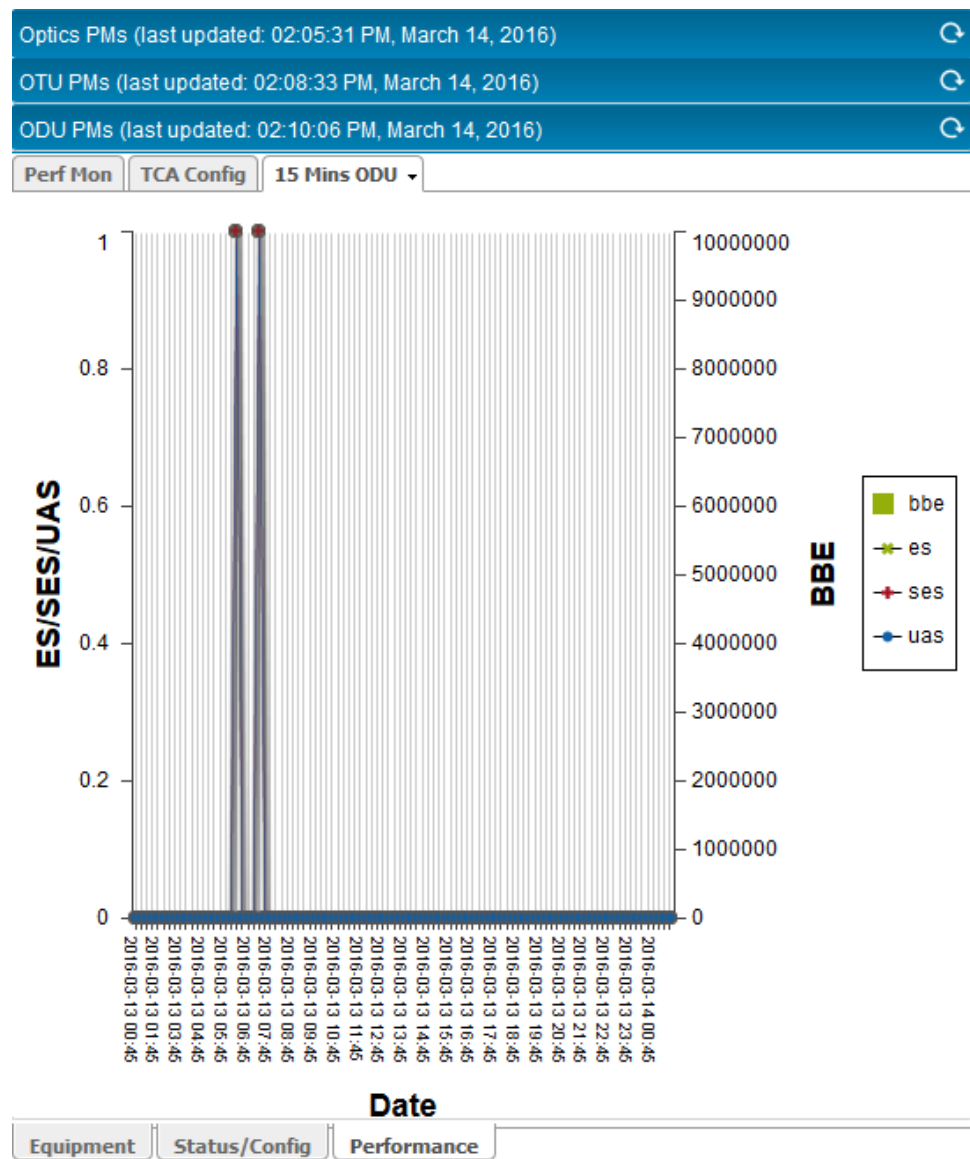
UAS—Unavailable seconds threshold-crossing defect trigger for ODU near-end

On the Perf Mon tab, for the TCA column, either a minus sign (–) is displayed that denotes that an alarm for threshold-exceed is not configured or a check mark is displayed and grayed out that indicates that the TCA for the particular attribute is configured.

8. In the 15 Mins column, click the **Chart** button for the performance monitoring parameter set for which you want to view the statistics for the last 15 minutes. This option enables you to view the statistics in a chart form. By default, 96 records of 15-minute intervals are displayed.

A 15-Min *parameter-name* tab is displayed beside the TCA Config tab at the top-left corner of the Optics PMs dialog box as shown in [Figure 103 on page 1552](#). A graphical format of the statistics for the specified parameter is displayed on this tab.

Figure 103: 15 Mins Parameter-Name Tab of the ODU PMs Dialog Box



9. Click the **15 Mins parameter name** tab.
 - a. Select one of the following options from the drop-down menu:

- Select **View Chart** or the graphical icon (elliptical curve symbol) to display the chart of performance monitoring statistical metrics. A line graph is displayed with date and time along the horizontal axis and the parameter along the vertical axis. A color-coding format is used to display the different lines, and legends reference the parameter names corresponding to the lines displayed. Mouse over the points in the line graph to expand and show the value of the performance monitoring counters at a particular time.
- Select **View Grid** to switch over to the tabular format of display of performance monitoring statistics.

The records are displayed in tabular format. A serial number of the count of entries, the day, month, and year at which the entry was collected, and the time at which the entry was collected are displayed. The timestamp is the UTC time in the database that is mapped to the local time zone of the client computer.

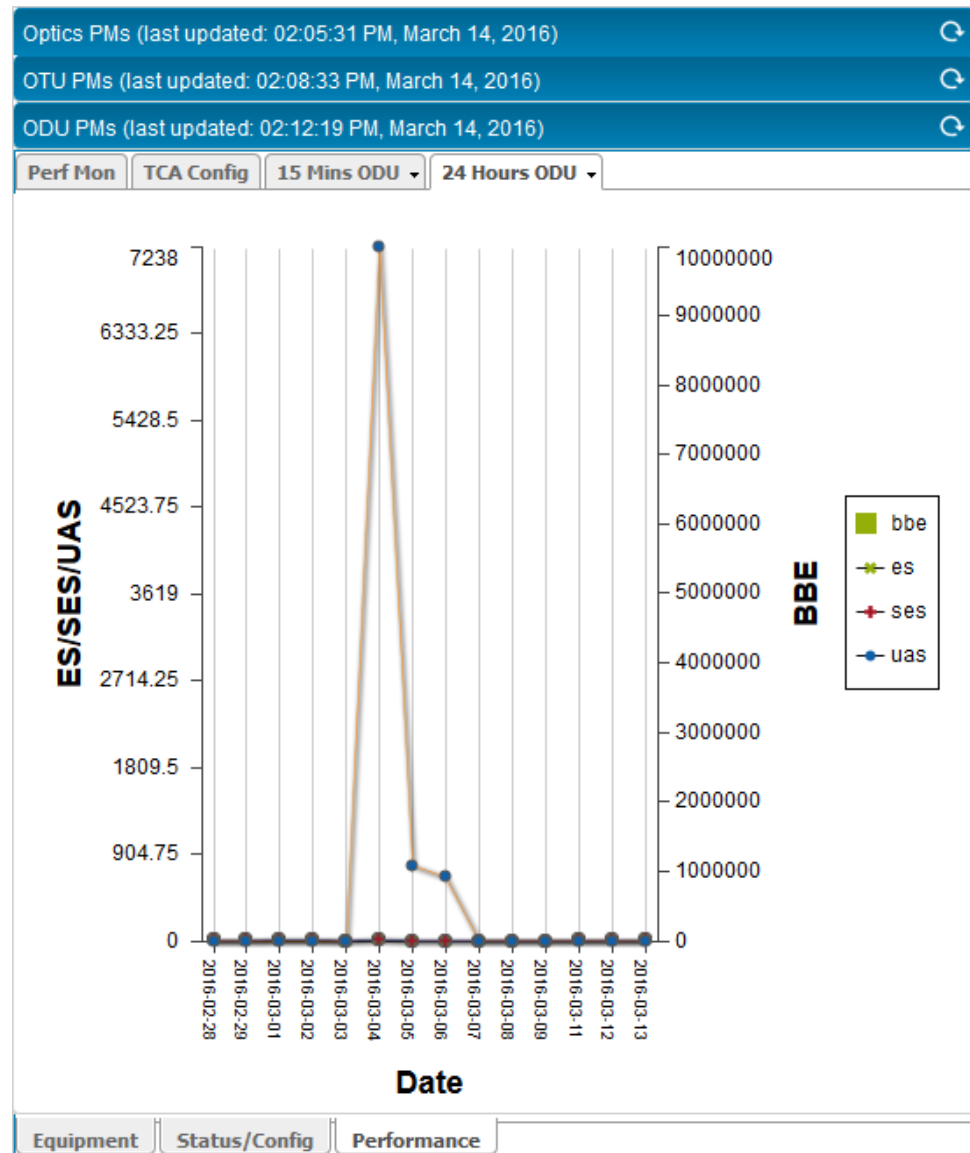
- Select **Save Chart**, when you view the performance monitoring statistics in graphical format, to save the graph to a Microsoft Excel file, as a .png image. Click the pin icon on the upper-left corner to revert the tab to the original container panel.
- Select **Popout Tab** or the light blue triangle icon to view the dialog box as a separate window.

In the pop-up dialog box, you can do one of the following:

- In the From Date field, pull down the calendar and select the start date of the search. In the To Date field, pull down the calendar and select the end date of the search.
 - Click **Reload** to refresh the contents and display the updated information for the specified time period.
 - Click **Export Data** to transfer the data in graphical or statistical format to a spreadsheet or other business applications for future reference and archival. The comma-separated value (CSV) format takes the raw data from the report and delineates the fields with commas so that the data is imported into popular spreadsheet programs.
 - Click the **View Chart** button at the top-left corner of the dialog box to view the statistics in graphical format. Alternatively, click the **View Grid** button at the top-left corner of the dialog box to view the statistics in tabular format. The View Chart/Grid button is a toggle button.
 - Click **OK** to close the pop-up dialog box. Alternatively, press Esc to close the dialog box after you complete viewing the statistical details.
 - Click **Close** to close the 15-Min *parameter-name* tab.
10. In the 24-Hrs column, click the **Chart** button for the performance monitoring parameter set for which you want to view the statistics for the previous day. This option enables you to view the statistics in a chart form. Performance monitoring information for the different parameters are displayed for the current 24-hour interval. By default, records pertaining to the last 30 days are displayed when you view the performance monitoring counters for the 24-hour duration.

A 24 Hours *parameter-name* tab is displayed beside the TCA Config tab at the top-left corner of the Optics PMs dialog box as shown in [Figure 104 on page 1554](#). A graphical format of the statistics for the specified parameter is displayed on this tab.

Figure 104: 24 Hours Parameter-Name Tab of the ODU PMs Dialog Box



11. Click the **24 Hours *parameter name*** tab.
 - a. Select one of the following options from the drop-down menu:

- Select **View Chart** or the graphical icon (elliptical curve symbol) to display the chart of performance monitoring statistical metrics. A line graph is displayed with date along the horizontal axis and the parameter along the vertical axis. A color-coding format is used to display the different lines, and legends reference the parameter names corresponding to the lines displayed. Mouse over the points in the line graph to expand and show the value of the performance monitoring counters at a particular time.
- Select **View Grid** to switch over to the tabular format of display of performance monitoring statistics.
- Select **Save Chart**, when you view the performance monitoring statistics in graphical format, to save the graph to a Microsoft Excel file, as a .png image. Click the pin icon on the upper-left corner to revert the tab to the original container panel.
- Select **Popout Tab** or the light blue triangle icon to view the dialog box as a separate window.

In the pop-up dialog box, you can do one of the following:

- In the From Date field, pull down the calendar and select the start date of the search. In the To Date field, pull down the calendar and select the end date of the search. Click **Reload** to refresh the contents and display the updated information for the specified time period.
 - Click **Export Data** to transfer the data in graphical or statistical format to a spreadsheet or other business applications for future reference and archival. The comma-separated value (CSV) format takes the raw data from the report and delineates the fields with commas so that the data is imported into popular spreadsheet programs.
 - Click the **View Chart** button at the top-left corner of the dialog box to view the statistics in graphical format. Alternatively, click the **View Grid** button at the top-left corner of the dialog box to view the statistics in tabular format. The View Chart/Grid button is a toggle button.
 - Click **OK** to close the pop-up dialog box. Alternatively, press Esc to close the dialog box after you complete viewing the statistical details.
 - Click **Close** to close the 24 Hours *parameter-name* tab.
12. Click the **Clear PMs** button at the top of the dialog box, and select one of the following values from the drop-down menu to clear ODU information from the transport performance monitoring data.
- **Current**—Clear the optics and OTN information for the current interval, such as 15-minute interval or 24-hour interval, for which monitoring data is being collected.
 - **Current Day**—Clear the ODU information for the current 24 hours.
 - **All Intervals**—Clear the ODU information for the current 15-minute interval, the 96 records of 15-minute intervals, the current day, and the previous day

After you select one of the intervals for which monitoring data must be deleted, a Clear Optics PMs dialog box is displayed to indicate that a job is triggered to delete the monitoring information from the module on the device. The job ID, start and end times of the job, percentage of completion, and status of the job are displayed.

13. Click **Close** to close the job dialog box; alternatively, click **Refresh** to update the job status and view.

You can use the Jobs Management page (by clicking the System icon on the banner and selecting Manage Jobs) to track the status of this job.

You can click the **Refresh** (rotating arrow icon) button at the top of the dialog box to enable the latest performance monitoring statistics to be polled and displayed.

**Related
Documentation**

- [Configuring Threshold-Crossing Alarms for OTN Ports for Monitoring Link Performance on page 1519](#)
- [Configuring Threshold-Crossing Alarms for OTUs for Monitoring Link Performance on page 1523](#)
- [Configuring Threshold-Crossing Alarms for ODUs for Monitoring Link Performance on page 1527](#)
- [Viewing Performance Monitoring Details of OTN Ports for Detecting and Diagnosing Faults on page 1530](#)
- [Viewing Performance Monitoring Details of OTUs for Detecting and Diagnosing Faults on page 1541](#)

Viewing a Graphical Image of the Chassis of PTX Series Routers

In the Connectivity Services Director GUI, you can view a graphical representation of a device from Build mode of Device View by selecting the **Device Management > View Physical Inventory** option from the Tasks pane. The hardware and line module details are displayed with a pictorial view of the slots of the PTX Series routers and the modules installed in these slots. The Chassis View provides a pictorial representation of the chassis or device, and the modules or components that are installed in it, such as the line cards, interfaces, and other hardware elements.

To view a pictorial representation of a device chassis and the configured components, such as interfaces, line cards, and hardware elements, select a managed device listed on the My Network tree in Device View of Connectivity Services Director, and select **Device Management > View Physical Inventory** from the tasks pane. The right pane displays the device image and the corresponding description of the view selected in a tabular manner. The Chassis View is displayed. The hardware and line module details are displayed with a pictorial view of the slots of the devices and the modules installed in these slots. The device image can be rotated to view the front, rear, top, bottom, right and left planes of the device by clicking the respective arrow buttons on the page.

To view a graphical image of the chassis and its associated components:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

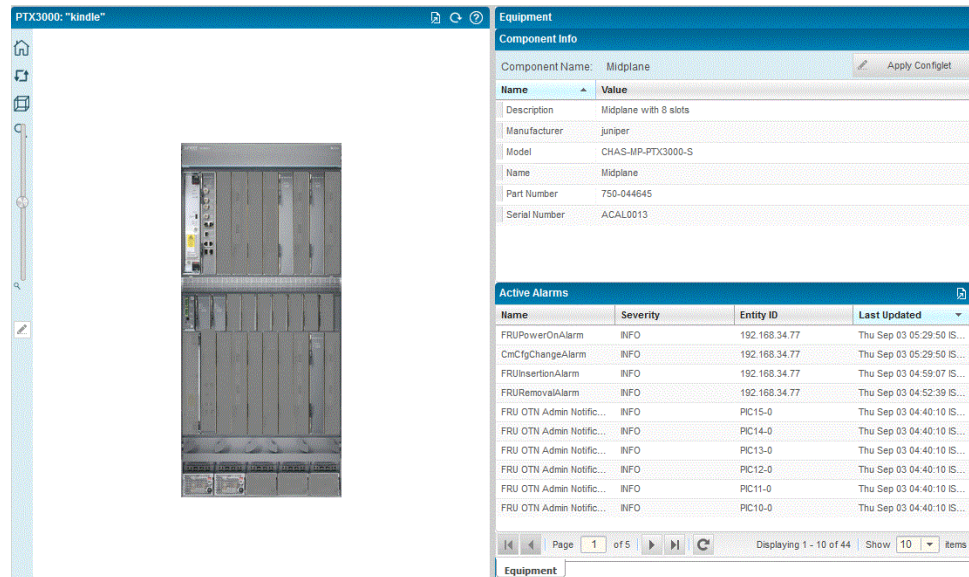
3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the device for which you want to define the optical port settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane as shown in [Figure 105 on page 1557](#).

Figure 105: Chassis View of a PTX Series Router



5. Click a particular component or interface to display the associated details in the lower portion of the page. The Rotate and Perspective buttons enable you to view the images in required orientation.

6. Click the **View Back** (arrows in a square symbol) icon to cause the device image to rotate along the x-axis and display the rear view of the device. Alternatively, click the **View Front** icon to view the front plane of the device. The View Back and View Front icons are toggle options.

7. Click the **Perspective** (cube symbol) icon to display the device image in three-dimensional format. It is a toggle button, which causes the device image to be shown in either three-dimensional or one-dimensional format.
8. Select the level of magnification of the image by clicking the **Zoom** (magnifying glass) icon. The image is expanded and displayed.

Alternatively, use the slider control beneath the Zoom icon to change the level of magnification.

9. Click the home icon to return to the front view of the chassis. The selected interface is surrounded with a colored outline based on the operational status. An interface that is operationally up is denoted in green and an interface that is operationally down is represented in red. The components are depicted as small colored icons at the top-left corner of the front view of the equipment image.

In the graphical image of the device displayed, you can mouse over the different parts of the device, such as the interfaces, line cards, and slots. When you mouse over the different modules, their corresponding details are displayed as tooltips. On clicking the device components, the corresponding description for the selected component is displayed by default in the Component Info pane and the Equipment tab with the following values.

- Description—Brief description of the hardware item:
 - Type of power supply.
 - Type of PIC. If the PIC type is not supported on the current software release, the output states **Hardware Not Supported**.
 - Type of FPC: **FPC Type 1**, **FPC Type 2**, **FPC Type 3**, **FPC Type 4** , or **FPC TypeOC192**.

On EX Series switches, a brief description of the FPC.

On the J Series routers, the FPC type corresponds to the Physical Interface Module (PIM). The following list shows the PIM abbreviation in the output and the corresponding PIM name.

- **2x FE**—Either two built-in Fast Ethernet interfaces (fixed PIM) or dual-port Fast Ethernet PIM
- **4x FE**—4-port Fast Ethernet ePIM
- **1x GE Copper**—Copper Gigabit Ethernet ePIM (one 10-Mbps, 100-Mbps, or 1000-Mbps port)
- **1x GE SFP**—SFP Gigabit Ethernet ePIM (one fiber port)
- **4x GE Base PIC**—Four built-in Gigabit Ethernet ports on a J4350 or J6350 chassis (fixed PIM)
- **2x Serial**—Dual-port serial PIM
- **2x T1**—Dual-port T1 PIM

- **2x E1**—Dual-port E1 PIM
- **2x CTIE1**—Dual-port channelized T1/E1 PIM
- **1x T3**—T3 PIM (one port)
- **1x E3**—E3 PIM (one port)
- **4x BRI S/T**—4-port ISDN BRI S/T PIM
- **4x BRI U**—4-port ISDN BRI U PIM
- **1x ADSL Annex A**—ADSL 2/2+ Annex A PIM (one port, for POTS)
- **1x ADSL Annex B**—ADSL 2/2+ Annex B PIM (one port, for ISDN)
- **2x SHDSL (ATM)**—G SHDSL PIM (2-port two-wire module or 1-port four-wire module)
- **1x TGM550**—TGM550 Telephony Gateway Module (Avaya VoIP gateway module with one console port, two analog **LINE** ports, and two analog **TRUNK** ports)
- **1x DS1 TIM510**—TIM510 E1/T1 Telephony Interface Module (Avaya VoIP media module with one E1 or T1 trunk termination port and ISDN PRI backup)
- **4x FXS, 4x FX0, TIM514**—TIM514 Analog Telephony Interface Module (Avaya VoIP media module with four analog **LINE** ports and four analog **TRUNK** ports)
- **4x BRI TIM521**—TIM521 BRI Telephony Interface Module (Avaya VoIP media module with four ISDN BRI ports)
- **Crypto Accelerator Module**—For enhanced performance of cryptographic algorithms used in IP Security (IPsec) services
- **MPC M 16x 10GE**—16-port 10-Gigabit Module Port Concentrator that supports SFP+ optical transceivers. (Not on EX Series switches.)
- For hosts, the Routing Engine type.
- For small form-factor pluggable transceiver (SFP) modules, the type of fiber: **LX**, **SX**, **LH**, or **T**.
- LCD description for EX Series switches (except EX2200 switches).
- **MPC2**—1-port MPC2 that supports two separate slots for MICs.
- **MPC3E**—1-port MPC3E that supports two separate slots for MICs (MIC-3D-1X100GE-CFP and MIC-3D-20GE-SFP) on MX960, MX480, and MX240 routers. The MPC3E maps one MIC to one PIC (1 MIC, 1 PIC), which differs from the mapping of legacy MPCs.
- 100GBASE-LR4, pluggable CFP optics
- Supports the Enhanced MX Switch Control Board with fabric redundancy and existing SCBs without fabric redundancy.
- Interoperates with existing MX Series line cards, including Flexible Port Concentrators (FPC), Dense Port Concentrators (DPCs), and Modular Port Concentrators (MPCs).

- **MPC4E**—Fixed configuration MPC4E that is available in two flavors:
MPC4E-3D-32XGE-SFPP and MPC4E-3D-2CGE-8XGE on MX2020, MX960, MX480, and MX240 routers.
- LCD description for MX Series routers
- Model—Model number of the FRU component.
- Name—Name of the SDG and the platform type, such as MX240 or MX480. This field displays the components of the device, such as chassis, PIC, CPU, and PIC parameters. Information about the chassis, midplane, craft interface (FPM), power midplane (PMP), Power Supply Modules (PSMs), Power Distribution Modules (PDMs), Routing Engines, Control Boards (CBs) and Switch Processor Mezzanine Boards (SPMBs), Switch Fabric Boards (SFBs), Flexible PIC Concentrators (FPCs), PICs, adapter cards (ADCs) and fan trays is displayed.
- Manufacturer—Name of the company that built and shipped the device.
- Part number—Part number of the chassis component.
- Serial number—Serial number of the chassis component. The serial number of the backplane is also the serial number of the router or switch chassis. Use this serial number when you need to contact Juniper Networks Customer Support about the router or switch chassis.

The Active Alarms monitor shows any active alarm that has not yet been cleared. It is one of the four standard monitors available in Alarm mode. Active Alarms is a table that has four fields and appear by default. However, nine fields are available for selection. View [Table 186 on page 1339](#) for a description of the table.

Table 241: Active Alarms Monitor

ID	A system and sequentially-generated identification number.	No	No
Assigned To	If assigned to an individual, it shows the name of the person assigned; otherwise, it shows System to mark that the alarm is still unassigned.	No	Yes
Severity	<p>The severity of the alarm. Severity levels are:</p> <ul style="list-style-type: none"> • Critical—A critical condition exists; immediate action is necessary. • Major—A major error has occurred; escalate or notify as necessary. • Minor—A minor error has occurred; notify or monitor the condition. • Info—An informational message; no action is necessary. 	Yes	Yes
Entity ID	The identification of the entity responsible for causing this alarm. The Entity ID is the key for correlation of events into an alarm. The Entity ID could be a MAC address of a radio or an IP address of the device.	Yes	Yes

Table 241: Active Alarms Monitor (continued)

Source	The IP address of the device or network element that generated the alarm. The SNMP agent is located at the source IP. In most cases, the source IP is the IP address of the switch or controller.	No	No
Reporting Device	The hostname or IP address of the reporting device.	Yes	Yes
Creation Date	The date and time the alarm was first reported.	No	No
Last Updated	The date and time that the information for the alarm was last modified.	Yes	Yes
Updated By	Either the system or the last user who modified the alarm.	No	No

Related Documentation • [Viewing a Graphical Image of the Optical Interface Components on page 1487](#)

Diagnosing, Examining, and Correcting Optical Interface Problems

Connectivity Services Director enables you to manage the optical functionality provided by 100-Gigabit Ethernet PIC that can be installed in MX Series and PTX Series routers. A topological network view is implemented, which enables you the user to visualize optical sites, links and services and a site view that provides status, configuration, alarms and fault management, and performance monitoring functionalities on the optical interfaces. FCAPS (fault, configuration, accounting, performance, and security) is a categorical model of the working objectives of network management.

The fault management capability in Connectivity Services Director shows you information about the health of your network and changing conditions of your equipment. Use this diagnosis and detection mechanism to identify problems with the equipment, pinpoint security attacks, or to analyze trends and categories of errors. This feature includes fault-monitoring details in the dashboard, monitoring pages, and in a dedicated page that displays the alarms, events, and system logging messages that are generated. These charts and messages provide essential and cohesive information about system conditions, any discrepancies and malfunctioning, and protocols or components that need to be examined and debugged for better efficiency and working capacity.

You can assess the performance of your network, not only at a point in time, but also over a period of time. This feature enables you to determine trending and network-health parameters; for example, whether service-level agreements (SLAs) have been violated. The fault management data includes SNMP traps and syslogs received from PTX Series routers. Junos Space platform is integrated with OpenNMS, which is a network management application platform that provides solutions for enterprises and carriers, to receive SNMP Traps. Connectivity Services Director uses OpenNMS for SNMP trap collection and correlation.

Activity on a network device consists of a series of events. Optical interfaces generate SNMP traps when certain types of events are persistent, or when the condition causing

the event crosses a threshold, SNMP sends a notification, also called a trap to Connectivity Services Director. Connectivity Services Director correlates traps, describing a condition, into an alarm. You can use the Fault Management page monitor to sort alarms, view an alarm in depth, and to assign a disposition to an alarm.

Alarms include Clear and Set alarms. All alarms are listed under OTN category and can be critical, major, or minor severity levels. Three main categories of alarms—Optical, OTU, and ODU—are displayed.

Threshold-crossing alarms (TCAs) are alarms that are activated when a certain configurable threshold—near-end measurement threshold or far-end measurement threshold—is crossed and remains so until the end of the 15-minute interval and the 24-hour interval for parameters such as optical channel transport unit (OTU) and optical data unit (ODU). A near-end measurement is associated with ingress data frames and a far-end measurement is associated with egress data frames. Monitoring the performance of links provides for end-to-end Ethernet service assurance over any path for either a single link or multiple links spanning networks composed of multiple LANs. The link performance metrics enable operators to offer binding service-level agreements (SLAs) and generate new revenues from rate- and performance-guaranteed service packages that are tailored to the specific needs of their customers.

Optical Alarms, 24 Hour Threshold-Crossing Alarms (TCA), and 15 Minute Threshold-Crossing Alarms (TCA)

The following are the different optical alarms that are generated:

- AvgPowerAlarm—Average Power Alarm
- BiasCurrentHighAlarm—Bias Current High Alarm
- BiasCurrentLowAlarm—Bias Current Low Alarm
- ChromaticDispHighWarning—Chromatic Dispersion High Warning
- ChromaticDispLowWarning—Chromatic Dispersion Low Warning
- LOS—Loss Of Signal
- LossofACPowerAlarm—Loss of Alternating Current (AC) Power Alarm
- ModuleTempHighWarning—Module Temperature High Warning
- ModuleTempLowWarning—Module Temperature Low Warning
- OSNRLowWarning—Optical Signal to Noise Ratio (OSNR) Low Warning
- PowerHighAlarm—Power High Alarm
- PowerLowAlarm—Power Low Alarm
- QLowWarning—Q Factor Low Warning
- RxCarrierFreqHigh—Receive Carrier Frequency High
- RxCarrierFreqLow—Receive Carrier Frequency Low
- RxLossAvgPowerAlarm—Receive Loss Average Power Alarm
- RxPLLLockAlarm—Receive Phase Lock Loop Alarm

- RxPowerHighAlarm—Receive Power High Alarm
- RxPowerHighWarning—Receive Power High Warning
- RxPowerLowAlarm—Receive Power Low Alarm
- RxPowerLowWarning—Receive Power Low Warning
- TemperatureHighAlarm—Temperature High Alarm
- TemperatureLowAlarm—Temperature Low Alarm
- TxPLLLockAlarm—Transmit Phase Loop Lock Alarm
- TxPowerHighWarning—Transmit Power High Warning
- TxPowerLowWarning—Transmit Power Low Warning
- WavelengthLockErr—Wavelength Lock Error

The following are the threshold-crossing alarms generated when threshold is exceeded over the last 15 minutes for optical interfaces:

- 24HourModuleTempHighThreshAlert—24 Hour Module Temperature High Threshold Alert
- 24HourModuleTempLowThreshAlert—24 Hour Module Temperature Low Threshold Alert
- 24HourRxPowerHighThreshAlert—24 Hour Receive Power High Threshold Alert
- 24HourRxPowerLowThreshAlert—24 Hour Receive Power Low Threshold Alert
- 24HourTxPowerHighThreshAlert—24 Hour Transmit Power High Threshold Alert
- 24HourTxPowerLowThreshAlert—24 Hour Transmit Power Low Threshold Alert

The following are the threshold-crossing alarms generated when threshold is exceeded over the last 24 hours for optical interfaces:

- RxPowerHighThreshAlert—15 Minute Receive Power High Threshold Alert
- ModuleTempHighThreshAlert—15 Minute Module Temperature High Threshold Alert
- RxPowerLowThreshAlert—15 Minute Receive Power Low Threshold Alert
- TxPowerHighThreshAlert—15 Minute Transmit Power High Threshold Alert
- TxPowerLowThreshAlert—15 Minute Transmit Power Low Threshold Alert
- ModuleTempLowThreshAlert—15 Minute Module Temp Low Threshold Alert

OTU Alarms, 24 Hour Threshold-Crossing Alarms (TCA), and 15 Minute Threshold-Crossing Alarms (TCA)

The following are the different OTU alarms that are generated:

- OtnLofAlarm—Loss of Frame Alarm
- OtnLomAlarm—Loss of Multi-frame Alarm

- OtnLosAlarm—Loss of Signal Alarm
- OtnNoAlarm—OTN No Alarm
- OtuBdiAlarm—OTU Backward Error Indication Alarm
- OtuBiaeAlarm—OTU Backward Incoming Alignment Error Alarm
- OtuDegAlarm—OTU Degradation Alarm
- OtuFecExcessiveErrsAlarm—OTU Forward Error Correction (FEC) Excessive Errors Alarm
- OtuIaeAlarm—OTU Incoming Alignment Error Alarm
- OtuSsfAlarm—OTU Server Signal Fail Alarm
- OtuTimAlarm—OTU Trace Identifier Mismatch Alarm
- OtuTsfAlarm—OTU Trail Signal Fail Alarm

The following are the threshold-crossing alarms generated when threshold is exceeded over the last 15 minutes for OTU attributes:

- 24HourThreshBBETCA—24 Hour Background Block Error Threshold Alert
- 24HourThreshBip8TCA—24 Hour Bit Interleaved Parity (BIP-8) Threshold Alert
- 24HourThreshESTCA—24 Hour Errored Seconds Threshold Alert
- 24HourThreshPreFECBERTCA—24 Hour Pre-Forward Error Correction Threshold Alert
- 24HourThreshSESTCA—24 Hour Severely Errored Seconds Threshold Alert
- 24HourThreshUASTCA—24 Hour Unavailable Second Threshold Alert

The following are the threshold-crossing alarms generated when threshold is exceeded over the last 24 hours for OTU attributes:

- 15MinThreshBBETCA—15 Minute Background Block Error Threshold Alert
- 15MinThreshBip8TCA—15 Minute Bit Interleaved Parity (BIP-8) Threshold Alert
- 15MinThreshESTCA—15 Minute Errored Seconds Threshold Alert
- 15MinThreshPreFECBERTCA—15 Minute Pre-Forward Error Correction Threshold Alert
- 15MinThreshSESTCA—15 Minute Severely Errored Seconds Threshold Alert
- 15MinThreshUASTCA—15 Minute Unavailable Second Threshold Alert
- 15MinThUnCorrectedWordsTCA—15 Minute UnCorrected Codewords Threshold Alert

ODU Alarms, 24 Hour Threshold-Crossing Alarms (TCA), and 15 Minute Threshold-Crossing Alarms (TCA)

The ODU tables cover both the Path and TCM layers but TCM layers are currently not supported. The following are the different ODU alarms that are generated:

- PtmAlarm—Payload Type Mismatch Alarm
- TcmAisAlarm—Alarm Indication Signal Alarm
- TcmBdiAlarm—Backward Error Indication Alarm
- TcmCSFAlarm—CSFAlarm
- TcmDegAlarm—Degradation Alarm
- TcmIaeAlarm—Incoming Alignment Error Alarm
- TcmLckAlarm—Locked Alarm
- TcmLTCAAlarm—Loss of tandem Connection Alarm
- TcmOciAlarm—Open Connection Indication Alarm
- TcmSSfAlarm—Server Signal Fail Alarm
- TcmTimAlarm—Trace Identifier Mismatch Alarm
- TcmTSfAlarm—Trail Signal Fail Alarm
- OdukTcmNoAlarm—OTN No Alarm

The following are the threshold-crossing alarms generated when threshold is exceeded over the last 15 minutes for ODU attributes:

- Tcm15MinThreshBBETCA—15 Minute Background Block Error Threshold Alert
- Tcm15MinThreshBip8TCA—15 Minute Bit Interleaved Parity (BIP-8)
- Threshold Alert Tcm15MinThreshESTCA—15 Minute Errored Seconds Threshold Alert
- Tcm15MinThreshSESTCA—15 Minute Severely Errored Seconds
- Threshold Alert Tcm15MinThreshUASTCA—15 Minute Unavailable Second Threshold Alert

The following are the threshold-crossing alarms generated when threshold is exceeded over the last 24 hours for ODU attributes:

- Tcm24HourThreshBBETCA—24 Hour Background Block Error Threshold Alert
- Tcm24HourThreshBip8TCA—24 Hour Bit Interleaved Parity (BIP-8) Threshold Alert
- Tcm24HourThreshESTCA—24 Hour Errored Seconds Threshold Alert
- Tcm24HourThreshSESTCA—24 Hour Severely Errored Seconds Threshold Alert
- Tcm24HourThreshUASTCA—24 Hour Unavailable Second Threshold Alert

**Related
Documentation**

- [Diagnosing, Examining, and Correcting Optical Interface Problems on page 1561](#)

Changing Alarm Settings for the Optics and OTN Interfaces

You can modify the configuration settings for alarm settings of optical interfaces using the Preferences page of the Connectivity Services Director application. To open the

Preferences page, click the down arrow next to the System button in the Connectivity Services Director banner and select Preferences. The Preferences page opens with User Preferences as the default tab. Click the Fault tab of the Preferences page of the Connectivity Services Director GUI to enable individual alarms, set the retention period for alarms, configure alarm notifications, configure threshold alarms, and to specify the number of events to keep for each alarm. The Fault tab has multiple sections, which you can expand and collapse by clicking the arrow next to the section title:

- Global Settings, for configuring Faults settings such as global alarm notifications and alarm data retention.
- Individual Alarms and Threshold Settings, for configuring settings for individual alarms and threshold alarms.

This section describes the following tasks that you can perform by using the alarm monitors displayed in Fault mode:

- [Alarms for Optical Interfaces on page 1566](#)
- [Alarms for OTN Interfaces on page 1571](#)
- [Configuring Global Alarm Notifications on page 1576](#)
- [Retaining Alarm History on page 1576](#)
- [Specifying Event History on page 1577](#)
- [Enabling Alarms on page 1577](#)
- [Changing the Severity of Individual Alarms on page 1577](#)
- [Configuring Threshold Alarms on page 1577](#)
- [Configuring Individual Alarm Notifications on page 1578](#)

Alarms for Optical Interfaces

The following alarms are applicable for management of the Optics interface.

- `JnxOpticsLocation`—Near end or far end
- `jnxOpticsPerformanceMonitoring`—{ `jnxIfOpticsMib 2` }
- `jnxOpticsAlarm`—{ `jnxIfOpticsMib 3` }
- `jnxOpticsConfigTable`—This table provides information on the optics configuration.
 - `jnxOpticsConfigEntry`—A conceptual row that contains information about the optics configuration Table.
 - `jnxOpticsConfigContainerIndex`—The associated `jnxContentsContainerIndex`, for example, shelf.
 - `jnxOpticsConfigL1Index`—The level one index associated with this subject, for example, slot.
 - `jnxOpticsConfigL2Index`—The level two index associated with this subject, for example, port.
 - `jnxOpticsConfigL3Index`—The level three index associated with this subject, for example, channel.

- `jnxOpticsType`
- `jnxLaserEnable`—The transmit wavelength of the laser.
- `jnxSpacing`—A minimum nominal difference in frequency (GHz) between two adjacent channels.
- `jnxModulation`
- `jnxTxOpticalPower`—Transmit optical power.
- `jnxModuleTempHighThresh`—High module temperature in degree Fahrenheit above which a Threshold Crossing Alert (TCA) should be sent.
- `jnxModuleTempLowThresh`—Low module temperature in degree Fahrenheit above which a Threshold Crossing Alert (TCA) should be sent.
- `jnxTxPowerHighThresh`—Tx power above which a Threshold Crossing Alert (TCA) should be sent.
- `jnxTxPowerLowThresh`—Tx Power below which a Threshold Crossing Alert (TCA) should be sent.
- `jnxRxPowerHighThresh`—Rx power above which a Threshold Crossing Alert (TCA) should be sent.
- `jnxRxPowerLowThresh`—Rx Power below which a Threshold Crossing Alert (TCA) should be sent.
- `jnxOpticsTraceToneCfgTable`—Information about the optics tests.
 - `jnxOpticsTraceToneCfgEntry`—Information about the optics FRUs
 - `jnxOpticsTraceToneCfgContainerIndex`—The associated `jnxContentsContainerIndex`, for example, shelf.
 - `jnxOpticsTraceToneCfgL1Index`—The level one index associated with this subject, for example slot.
 - `jnxOpticsTraceToneCfgL2Index`—The level two index associated with this subject, for example port.
 - `jnxOpticsTraceToneCfgL3Index`—The level three index associated with this subject, for example channel.
 - `jnxOpticsTraceToneCfgTxEnable`—Enable/disable the transmit Trace tone feature.
 - `jnxOpticsTraceToneCfgRxEnable`—Enable/disable the receive Trace tone feature.
 - `jnxOpticsTraceToneCfgDestId`—The destination Id of the link ID/ the chassis and the blade. The transmit messages will also have the src id, which is this chassis id and this port info.
 - `jnxOpticsTraceToneCfgTxMsg`—The transmit data in the tracetone message.
 - `jnxOpticsTraceToneCfgRxMsg`—The received data in the trace tone message.
- `jnxOpticsPMCurrentTable`—A table of current performance monitoring entries.

- `jnxOpticsPMCurrentEntry`—A conceptual row that contains information about the Performance Monitoring Current Table.
- `jnxPMCurChromaticDispersion`—Residual Chromatic Dispersion measured at Rx Transceiver port.
- `jnxPMCurDiffGroupDelay`—Differential group delay.
- `jnxPMCurPolarizationState`—Polarization state.
- `jnxPMCurPolarDepLoss`—The polarization dependent loss (PDL) is the difference (in dB) between the maximum and minimum values of the channel insertion loss (or gain) of the black-link from point SS to RS due to a variation of the state of polarization (SOP) over all SOPs.
- `jnxPMCurQ`—'Q' factor estimated at Rx Transceiver port.
- `jnxPMCurSNR`—SNR—signal-to-noise ratio.
- `jnxPMCurTxOutputPower`—TxOutputPower—transmit output power.
- `jnxPMCurRxInputPower`—RxInputPower—receive output power
- `jnxPMCurMinChromaticDispersion`—Minimum Residual Chromatic Dispersion measured at Rx Transceiver port.
- `jnxPMCurMaxChromaticDispersion`—Maximum Residual Chromatic Dispersion measured at Rx Transceiver port.
- `jnxPMCurAvgChromaticDispersion`—Average Residual Chromatic Dispersion measured at Rx Transceiver port.
- `jnxPMCurMinDiffGroupDelay`—Minimum Differential group delay
- `jnxPMCurMaxDiffGroupDelay`—Maximum Differential group delay
- `jnxPMCurAvgDiffGroupDelay`—Average Differential group delay
- `jnxPMCurMinPolarState`—Minimum Polarization state
- `jnxPMCurMaxPolarState`—Maximum Polarization state
- `jnxPMCurAvgPolarState`—Average Polarization state
- `jnxPMCurMinPolarDepLoss`—Minimum polarization dependent loss (PDL)
- `jnxPMCurMaxPolarDepLoss`—Maximum polarization dependent loss (PDL)
- `jnxPMCurAvgPolarDepLoss`—Average polarization dependent loss (PDL)
- `jnxPMCurMinQ`—Minimum 'Q' factor estimated at Rx Transceiver port.
- `jnxPMCurMaxQ`—Max 'Q' factor estimated at Rx Transceiver port.
- `jnxPMCurAvgQ`—Average 'Q' factor estimated at Rx Transceiver port.
- `jnxPMCurMinSNR`—Minimum SNR—signal-to-noise ratio
- `jnxPMCurMaxSNR`—Maximum SNR—signal-to-noise ratio
- `jnxPMCurAvgSNR`—Average SNR—signal-to-noise ratio
- `jnxPMCurMinTxOutputPower`— Minimum TxOutputPower—transmit output power

- jnxPMCurAvgTxOutputPower—Average TxOutputPower—transmit output power
- jnxPMCurMinRxInputPower—Minimum RxInputPower—receive output power
- jnxPMCurMaxRxInputPower—Maximum RxInputPower—receive output power
- jnxPMCurAvgRxInputPower—Average RxInputPower—receive output power
- jnxPMCurSuspectedFlag—If true, the data in this entry may be unreliable.
- jnxPMCurSuspectReason —If SuspectedFlag is true, the reason for the performance monitoring data being suspect.
- jnxOpticsPMIntervalTable—A table of current performance monitoring entries.
 - jnxOpticsPMIntervalEntry—A conceptual row that contains information about the Performance Monitoring Interval Table.
 - jnxOpticsPMIntervalNumber—This is the 15 minute interval number.
 - jnxPMIntMinChromaticDispersion—Residual Chromatic Dispersion measured at Rx Transceiver port—minimum in the 15 minute interval.
 - jnxPMIntMaxChromaticDispersion—Residual Chromatic Dispersion measured at Rx Transceiver port—maximum in the 15 minute interval.
 - jnxPMIntAvgChromaticDispersion—Residual Chromatic Dispersion measured at Rx Transceiver port—average in the 15 minute interval.
 - jnxPMIntMinDiffGroupDelay—Differential group delay measured at Rx Transceiver port—minimum in the 15 minute interval.
 - jnxPMIntMaxDiffGroupDelay—Differential group delay measured at Rx Transceiver port—maximum in the 15 minute interval
 - jnxPMIntAvgDiffGroupDelay—Differential group delay measured at Rx Transceiver port—average in the 15 minute interval
 - jnxPMIntMinPolarState—Polarization state—minimum in the 15 minute interval
 - jnxPMIntMaxPolarState—Polarization state—max in the 15 minute interval
 - jnxPMIntAvgPolarState—Polarization state—average in the 15 minute interval
 - jnxPMIntMinPolarDependentLoss—Polarization Dependent Loss—minimum in the 15 minute interval
 - jnxPMIntMaxPolarDependentLoss—Polarization Dependent Loss—maximum in the 15 minute interval
 - jnxPMIntMinQ—Q—minimum in the 15 minute interval
 - jnxPMIntMaxQ—Q—maximum in the 15 minute interval
 - jnxPMIntAvgQ—Q—Average in the 15 minute interval
 - jnxPMIntMinSNR—SNR—minimum in the 15 minute interval
 - jnxPMIntMaxSNR—SNR—maximum in the 15 minute interval
 - jnxPMIntAvgSNR—SNR—average in the 15 minute interval

- jnxPMIntMinTxOutputPower—TxOutputPower—minimum in the 15 minute interval
- jnxPMIntMaxTxOutputPower—TxOutputPower—maximum in the 15 minute interval
- jnxPMIntAvgTxOutputPower—TxOutputPower—average in the 15 minute interval
- jnxPMIntMinRxInputPower—RxInputPower—minimum in the 15 minute interval
- jnxPMIntMaxRxInputPower—RxInputPower—maximum in the 15 minute interval
- jnxPMIntAvgRxInputPower—RxInputPower—average in the 15 minute interval
- jnxPMIntTimeStamp—Time stamp performance monitoring interval
- jnxPMIntSuspectedFlag—If true, the data in this entry may be unreliable.
- jnxPMIntSuspectReason—If SuspectedFlag is true, the reason for the performance monitoring data being suspect.
- jnxOpticsPMDayTable—A table of current performance monitoring Day entries.
 - jnxOpticsPMDayEntry—A conceptual row that contains information about the performance monitoring Day Table
 - jnxOpticsPMDayIndex—This is 0 - cur day/ 1- prev day
 - jnxPMDayMinChromaticDispersion—Residual Chromatic Dispersion measured at Rx Transceiver port—minimum in the day
 - jnxPMDayMaxChromaticDispersion—Residual Chromatic Dispersion measured at Rx Transceiver port—maximum in the day
 - jnxPMDayAvgChromaticDispersion—Residual Chromatic Dispersion measured at Rx Transceiver port—average in the day
 - jnxPMDayMinDiffGroupDelay—Differential Group Delay measured at Rx Transceiver port—minimum in the day
 - jnxPMDayMaxDiffGroupDelay—Differential Group Delay measured at Rx Transceiver port—maximum in the day
 - jnxPMDayAvgDiffGroupDelay—Differential Group Delay measured at Rx Transceiver port—average in the day
 - jnxPMDayMinPolarState—Polarization state—minimum in the day
 - jnxPMDayMaxPolarState—Polarization state—maximum in the day
 - jnxPMDayAvgPolarState—Polarization state—average in the day
 - jnxPMDayMinPolarDependentLoss—Polarization Dependent Loss—minimum in the day
 - jnxPMDayMaxPolarDependentLoss—Polarization Dependent Loss—maximum in the day
 - jnxPMDayAvgPolarDependentLoss—Polarization Dependent Loss—average in the day interval
 - jnxPMDayMinQ—Q—minimum in the day
 - jnxPMDayMaxQ—Q—maximum in the day

- jnxPMDayAvgQ—Q—Average in the day
- jnxPMDayMinSNR—SNR—min in the day
- jnxPMDayMaxSNR—SNR—max in the day
- jnxPMDayAvgSNR—SNR—avg in the day
- jnxPMDayMinTxOutputPower—TxOutputPower—minimum in the day
- jnxPMDayMaxTxOutputPower—TxOutputPower—maximum in the day.
- jnxPMDayAvgTxOutputPower—TxOutputPower—average in the day.
- jnxPMDayMinRxInputPower—RxInputPower—minimum in the day.
- jnxPMDayMaxRxInputPower—RxInputPower—maximum in the day.
- jnxPMDayAvgRxInputPower—RxInputPower—average in the day.
- jnxPMDayTimeStamp—Time for the Day.
- jnxPMDaySuspectedFlag—If true, the data in this entry may be unreliable.
- jnxPMDaySuspectReason—If SuspectedFlag is true, the reason for the performance monitoring data being suspect.

Alarms for OTN Interfaces

The following alarms are applicable for management of OTN interface for Juniper products.

- jnxIfAdminStates—Administraion state of the interface.
 - jnxAdminStatInService(1)—In service.
 - jnxAdminStateInServiceMA(2)—In service maintenance, the link is in service, but the alarms are suppressed.
 - jnxAdminStateOutOfService(3)—Out of service due to a fault.
 - jnxAdminStateOutOfServiceMA(4)—Out of service maintenance as configured by the user, may or may not have alarms.
- jnxIfOperStates—Operation states of the interface.
 - jnxOperStateInit(1)—Starting state of the interface.
 - jnxOperStateNormal(2)—The interface is working normally.
 - jnxOperStateFault(3)—There is some traffic affecting fault on the interface, for example, LOS.
 - jnxOperStateDegraded(4)—There is some function affecting the performance on the interface resulting in degradation, for example BER.
- jnxIfOtnRate—Rates for an interface.
- jnxIfOtnFecType—FEC modes of an interface.
- jnxIfOtnLayer—Layer which describes the table.

- jnxIfOtnType—Near end of far end
- jnxIfOtnDirection—Direction for the entities in the table.
- jnxIfOtnSeverity—Severity of the notification.
- jnxIfOtnServiceStateAction—Notification action on the service state.
- jnxIfOtnOtnNotificationId—Identifies specific OTN alarms that may exist on an interface.
 - jnxIfOtnOtnLosAlarm(1)
 - jnxIfOtnOtnLofAlarm(2)
 - jnxIfOtnOtnLomAlarm(3)
 - jnxIfOtnOtnOtuSsfAlarm(4)
 - jnxIfOtnOtnOtuBdiAlarm(5)
 - jnxIfOtnOtnOtuTtimAlarm(6)
 - jnxIfOtnOtnOtuLaeAlarm(7)
 - jnxIfOtnOtuBiaeAlarm(8)
 - jnxIfOtnOtuDegAlarm(9)
 - jnxIfOtnOtuFecExcessiveErrsAlarm(11)
 - jnxIfOtn15MinThreshBBETCA(12)
 - jnxIfOtn15MinThreshESTCA(13)
 - jnxIfOtn15MinThreshSESTCA(14)
 - jnxIfOtn15MinThreshUASTCA(15)
 - jnxIfOtn15MinThreshFcsTCA(16)
 - jnxIfOtn15MinThUnCorrectedWordsTCA(17)
 - jnxIfOtn15MinThreshPreFECBERTCA(18)
- JnxIfOtnOduktcmNotificationId—Alarms from the ODUk and TCM layers.
 - jnxIfOtnOduktcmOciAlarm(1)
 - jnxIfOtnOduktcmLckAlarm(2)
 - jnxIfOtnOduktcmBdiAlarm(3)
 - jnxIfOtnOduktcmTimAlarm(4)
 - jnxIfOtnOduktcmDegAlarm(5)
 - jnxIfOtnOduktcmLaeAlarm(6)
 - jnxIfOtnOduktcmLTCAAlarm(7)
 - jnxIfOtnOduktcmCSfAlarm(8)
 - jnxIfOtnOduktcmSSfAlarm(9)
 - jnxIfOtnOduktcmTSfAlarm(10)

- jnxIfOtnOdukTcm15MinThreshBBETCA(11)
- jnxIfOtnOdukTcm15MinThreshESTCA(12)
- jnxIfOtnOdukTcm15MinThreshSESTCA(13)
- jnxIfOtnOdukTcm15MinThreshUASTCA(14)
- jnxIfOtnOdukTcm15MinThreshFcsTCA(15)
- jnxIfOtnOdukTcmAisAlarm(16)
- jnxIfOtnOChCfgTable—This table provides information on the Otn OCh configuration.
 - jnxIfOtnOChCfgEntry
 - jnxIfOtnOChCfgContainerIndex
 - jnxIfOtnOChCfgL1Index
 - jnxIfOtnOChCfgL3Index
- jnxIfOtnLocalLoopback—Local loopback at the line after the optics.
- jnxIfOtnLineLoopback—Line loopback at the line.
- jnxIfOtnPayloadLoopback—Payload loopback after the optics.
- jnxIfOtnAdminState
- jnxIfOtnOperState—Operation state of the interface.
- jnxIfOtnIndex-IfIndex of the interface.
- jnxIfOtnOChStatus
- jnxIfOtnOChPortMode— Port mode of the interface.
- jnxIfOtnOTUkCfgTable—This table provides information on the Otn OTUk configuration.
 - jnxIfOtnOTUkCfgEntry—A conceptual row that contains the Otn OTUk configuration table.
 - jnxIfOtnOTUkCfgContainerIndex—The associated jnxContentsContainerIndex, for example, shelf.
 - jnxIfOtnOTUkCfgL1Index—The level one index associated with the subject, for example, slot.
 - jnxIfOtnOTUkCfgL2Index—The level two index associated with the subject, for example, port.
 - jnxIfOtnOTUkCfgL3Index— The level three index associated with the subject, for example channel.
 - jnxIfOtnOTUkCfgRate— The rate for the interface, depending on the interface/fru type.
 - jnxIfOtnOTUkCfgFecMode—The FEC type in the OTU frame, the selection depends on the interface/fru type.

- `jnxIfOtnOTUkEnableAutoFrrByteInsert`—Enable or disable the automatic insertion of the frr SF/SD byte in the overhead bytes(RES).
- `jnxIfOtnOTUkEnableBERFrrSupport`—Enable or disable the FRR support for BER.
- `jnxIfOtnOTUkPreFecBERThresholdMantissa`—Sets the BER threshold(mantissa), which when crossed triggers signal degrade.
- `jnxIfOtnOTUkPreFecBERThresholdExponent` —Sets the BER threshold(exponent), which when crossed triggers signal degrade.
- `jnxIfOtnOTUkPreFecBERThresholdTime`—The collection time to calculate the BER.
- `jnxIfOtnOTUkTIMActEnabled`—Indicates whether or not the Trace Identifier Mismatch (TIM) consequent action function is enabled.
- `jnxIfOtnOTUkTxTTI`— The Trace TTI SAPI 0..15, DAPI 16..31 32..63 user defined.
- `jnxIfOtnOTUkRxTTI`— The Receive Trace TTI SAPI 0..15, DAPI 16..31 32..63 user defined.
- `jnxIfOtnOTUkExpectedRxSapi` — Expected receive SAPI.
- `jnxIfOtnOTUkExpectedRxDapi`-Expected receive DAPI.
- `jnxIfOtnOTUkStatus`—The status of the interface.
- `jnxIfOtnOTUkPreFecBERThresholdClearMantissa`—Sets the BER threshold(mantissa) for clear signal degrade condition, which signal degrade condition will be cleared when Pre-FEC error count is below the clear threshold error count.
- `jnxIfOtnOTUkPreFecBERThresholdClearExponent`—Sets the BER threshold(exponent) for clear signal degrade condition, which signal degrade condition will be cleared when Pre-FEC error count is below the clear threshold error count.
- `jnxIfOtnODUkCfgTable`-This table provides information on the Otn ODUk configuration.
 - `jnxIfOtnODUkCfgEntry`—A conceptual row that contains information about the Otn ODUk configuration.
 - `jnxIfOtnODUkCfgContainerIndex`—The associated `jnxContentsContainerIndex`, for example, shelf.
 - `jnxIfOtnODUkCfgL1Index`—The level one index associated with this subject, for example slot.
 - `jnxIfOtnODUkCfgL2Index`—The level two index associated with the subject, for example, port.
 - `jnxIfOtnODUkCfgL3Index`—The level three index associated with the subject, for example channel.
 - `jnxIfOtnODUkAPSPCC0`—Read/Write APS PCC byte 0 for this ODUk only.
 - `jnxIfOtnODUkAPSPCC1`—Read/Write APS PCC byte 1 for this ODUk only.
 - `jnxIfOtnODUkAPSPCC2`—Read/Write APS PCC byte 2 for this ODUk only.

- jnxIfOtnODUkAPSPCC3—Read/Write APS PCC byte 3 for this ODUk only.
- jnxIfOtnODUkPayloadType—Read/Write Payload Type for ODUk only.
- jnxIfOtnODUkTIMActEnabled—Indicates whether or not the Trace Identifier Mismatch (TIM) consequent action function is enabled. The default value of this object is false(2).
- jnxIfOtnODUkTxTTI—The Trace TTI SAPI 0..15, DAPI 16..31 32..63 user defined for this layer.
- jnxIfOtnODUkRxTTI—The Receive Trace TTI SAPI 0..15, DAPI 16..31 32..63 user defined.
- jnxIfOtnODUkExpectedRxSapi—Expected receive SAPI for this layer.
- jnxIfOtnODUkExpectedRxDapi—Expected receive DAPI for this layer.
- jnxIfOtnODUkStatus—The status of the interface. Only some of these alarms are valid for the TCM layer.
- jnxIfOtnODUkRxPayloadType—Receive payload type for ODUk only.
- jnxIfOtnTcmCfgTable—This table provides information on the Otn TCM configuration.
 - jnxIfOtnTcmCfgEntry—A conceptual row that contains information about the Otn Tcm configuration.
 - jnxIfOtnTcmCfgContainerIndex—The associated jnxContentsContainerIndex, for example shelf.
 - jnxIfOtnTcmCfgL1Index—The level one index associated with this subject, for example, slot.
 - jnxIfOtnTcmCfgL2Index—The level one index associated with this subject, for example, port.
 - jnxIfOtnTcmCfgL3Index—The level one index associated with this subject, for example, channel.
 - jnxIfOtnTcmCfgLevel—The TCM level for the table.
 - jnxIfOtnTCMEnable—Enable this TCM layer (only for TCM layers)
 - jnxIfOtnTcmTxTTI—The Trace TTI SAPI 0..15, DAPI 16..31 32 ..63 user defined for this layer.
 - jnxIfOtnTcmRxTTI—The Receive Trace TTI SAPI 0..15, DAPI 16..31 32 ..63 user defined for this layer.
 - jnxIfOtnTcmExpectedRxSapi—Expected receive SAPI for this layer.
 - jnxIfOtnTcmExpectedRxDapi—Expected receive DAPI for this layer.
 - jnxIfOtnTcmStatus—Status of this layer.
- jnxIfOtnODUkTcmTestTable—This table provides information on the Otn ODUk test function.

- `jnxIfOtnODUkTcmTestEntry`—A conceptual row that contains information about the Otn ODUk test function.
- `jnxIfOtnODUkTcmTestLayer`—The OTU/ODU/TCM layer for the alarm.
- `jnxIfOtnODUkTcmTestTCMLevel`—For ODUk will be this will be 0 If layer is TCM then this will give the TCM level 1..6.
- `jnxIfOtnODUkTcmInsertAis`—Insert ODU Ais into OTN stream.
- `jnxIfOtnODUkTcmInsertLck`—Insert ODU Lck into OTN stream.
- `jnxIfOtnODUkTcmInsertOci`—Insert ODU Oci into OTN stream.
- `jnxIfOtnODUkPayloadPRBS`—Insert Payload PRBS, For ODUk layer and TCM level is 0.
- `jnxIfOtnODUkPayloadPRBSResult`—Result of the Payload PRBS.
- `jnxIfOtnODUkTcmDMTable`—Table for OTN ODUk/TCM Delay Measurement configuration table.
- `jnxIfOtnODUkTcmDMEntry`—A conceptual row that contains information about the Delay Measurement (DM) test table.
 - `jnxIfOtnODUkTcmDMLayer`—The layer OTU/ODU/TCM layer for the alarm
 - `jnxIfOtnODUkTcmDMLevel`—For ODUk, this value is 0, if layer is TCM then this gives the TCMlevel 1..6.
- `jnxIfOtnDMConnectionMonitoringEndpoint`—Originate Connection Monitoring Endpoint for the Delay Measurement.
- `jnxIfOtnDMBypass`—Act as tandem, passing DM value through node.
- `jnxIfOtnDMPersistFrames`—Number of consecutive frames required to declare DM Complete.
- `jnxIfOtnDMEnable`—Start/Stop the DM measurement.

Configuring Global Alarm Notifications

You can configure global e-mail notifications to be sent when any alarm with notifications enabled is generated. To configure global e-mail notifications, enter the e-mail addresses to receive global alarm notifications in the Alarm Notifications Destinations field in the Global Settings section. Separate addresses with a comma (,). For information about enabling notification for an alarm, see [“Configuring Individual Alarm Notifications” on page 152](#).

Retaining Alarm History

Use the **No. of days to keep Alarm** field in the Global Settings section to specify the number of days to keep alarm history. The default retention time is 120 days; but you can specify a period of 7 through 1000 days. Specifying a longer retention time consumes more database resources. To change the alarm retention duration, type a new value and click **OK** and **Yes** to confirm the change.

Specifying Event History

Use the **Events/Alarm** field in the Global Settings section to specify the number of event entries that are kept in the alarm history. The default setting for events is 20. To change the setting, type a new value and click **OK** and **Yes** to confirm the change.

Enabling Alarms

Ensure all devices are configured to send traps to Connectivity Services Director. This task is performed for the devices in Deploy mode through Set SNMP Trap Configuration.

Use the Individual Alarms and Threshold Settings section to disable and re-enable individual alarms or all alarms. Alarms appear on both tabs in the section: Alarm Settings and Threshold Settings. Fault alarms are preconfigured and initially enabled. To enable or disable alarms:

1. (Optional) Sort the alarms. By default, the list of alarms is sorted alphabetically within each category. You can also sort by description or alarm severity within a category by clicking a column heading.
2. Review the alarms and either select the check box in the heading to select all of the alarms or select the check box for the individual alarms you want to enable.
3. Click **OK** and **Yes** to confirm the alarm change.

Changing the Severity of Individual Alarms

You can change the severity of the alarms to match your corporate procedures and guidelines. For example, at your company a DoS attack might be considered a critical alarm, while Connectivity Services Director has a default severity for DoS attacks as a major alarm. Alarms appear on both tabs in the Individual Alarms and Threshold Settings section: Alarm Settings and Threshold Settings.

To change the severity of an alarm:

1. Select the current severity in the **Severity** column. A list of the severity levels appear.
2. Select the new severity level for the alarm.
3. Click **OK** and **Yes** to confirm the change to the severity setting.

To configure alarm notifications, see [“Configuring Individual Alarm Notifications” on page 152](#).

Configuring Threshold Alarms

Threshold alarms are alarms that are generated when a monitored value crosses the configured threshold. They provide enhanced visibility into potential issues on the network.

You configure and manage threshold alarms the same way as other alarms. You also have the option of setting the threshold level of individual threshold alarms.

To set threshold alarm thresholds:

1. Select the **Threshold Settings** tab in the Individual Alarms and Threshold settings section of the Fault tab.
2. Click **Edit Settings** in the Threshold Settings column of the alarm threshold you want to edit.
3. Set the threshold in the window that opens.
4. Click **Save** to save the new threshold.

To configure alarm notifications, see [“Configuring Individual Alarm Notifications” on page 152](#).

Configuring Individual Alarm Notifications

You can configure e-mail notifications to be sent when an individual alarm is generated. When you enable notification for an alarm, the notifications are sent to the e-mail addresses configured for the alarm and the addresses configured for global alarm notifications. Alarms appear on both tabs in the Individual Alarms and Threshold Settings section: Alarm Settings and Threshold Settings.

To configure e-mail notification for an alarm name:

1. Select the check box in the alarm's Notification column.
If you later want to disable notification for the alarm, clear the check box.
2. Click **Edit Notification** in the Notification column. The Alarm Notification Details window opens.
3. Enter one or more e-mail addresses in the Notification Email Addresses field. Separate addresses with a comma (,).
You can later edit the addresses to send notifications to different addresses.
4. (Optional) Enter a comment in the Comments field. This comment is included in the e-mail notification message.
5. Click **Save**.

Related Documentation

- [Changing Alarm Settings for the Optics and OTN Interfaces on page 1565](#)

Configuring and Monitoring Optical Inline Amplifiers

- [Viewing a Graphical Image of Optical Inline Amplifier on page 1579](#)
- [Viewing Optical ILA Configuration and Status Details for Simplified Administration on page 1583](#)
- [Viewing Performance Monitoring Details of Optical ILAs for Detecting and Diagnosing Faults on page 1588](#)
- [Configuring Threshold-Crossing Alarms for Optical ILAs for Monitoring Link Performance on page 1597](#)
- [Changing Alarm Settings for the Optical ILAs on page 1599](#)

Viewing a Graphical Image of Optical Inline Amplifier

The Chassis View provides a pictorial representation of the optical inline amplifier (ILA) of a PTX Series router. The optical ILA is used in conjunction with the integrated photonic line card (IPLC) that is installed in the PTX3000 routers. The optical ILA operates with redundant hot-swappable pluggable power supplies, which are either AC or DC.

The purpose of this view is to try and provide a comprehensive monitoring view of the health and status of deployed devices across the network. In this view all the managed devices are shown with their appropriate status and health based on the services and device settings applied. This view helps the operator to know the health and status across the network, it provides with the operator to quickly see the macro level information, which allows the operator to further analyze the information provided and quickly navigate to individual devices and take any further corrective measure required. It provides a cohesive tool for the operator to quickly see the micro-level information and take any further remediation action required.

To view a graphical image of the optical ILA of PTX Series routers, and its associated components:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

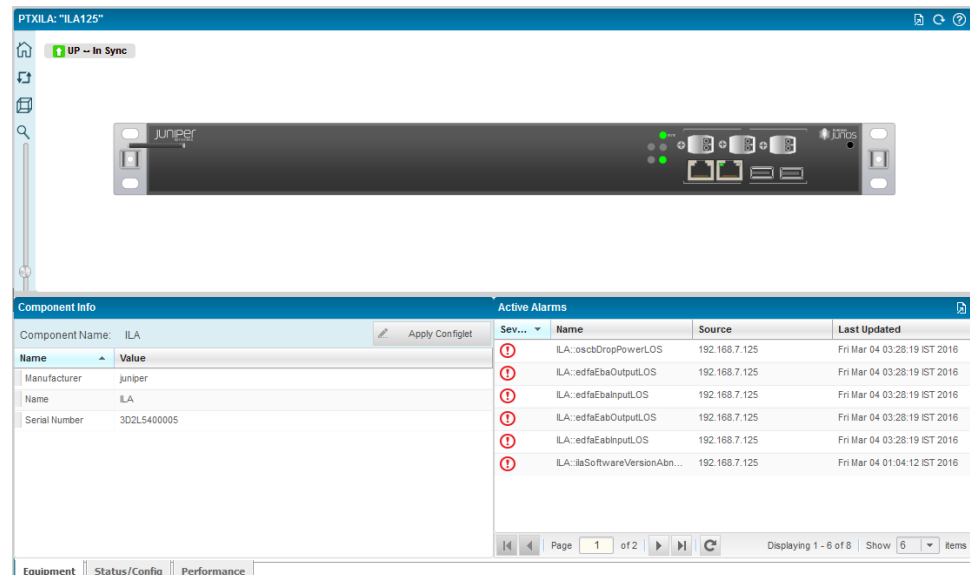
3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the device for which you want to define the optical port settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane as shown in [Figure 106 on page 1580](#).

Figure 106: Chassis View of an Optical ILA



5. Click a particular component or interface to display the associated details in the lower portion of the page. The Rotate and Perspective buttons enable you to view the images in required orientation.
6. Click the View Back (arrows in a square symbol) icon to cause the device image to rotate along the x-axis and display the rear view of the device. Alternatively, click the View Front icon to view the front plane of the device. The View Back and View Front icons are toggle options.

7. Click the Perspective (cube symbol) icon to display the device image in three-dimensional format. It is a toggle button, which causes the device image to be shown in either three-dimensional or one-dimensional format.
8. Select the level of magnification of the image by clicking the Zoom (magnifying glass) icon. The image is expanded and displayed.

Alternatively, use the slider control beneath the Zoom icon to change the level of magnification.

9. Click the home icon to return to the front view of the chassis. The selected interface is surrounded with a colored outline based on the operational status. An interface that is operationally up is denoted in green and an interface that is operationally down is represented in red. The components are depicted as small colored icons at the top-left corner of the front view of the equipment image.

In the graphical image of the device displayed, you can mouse over the different parts of the device, such as the interfaces, line cards, and slots. When you mouse over the different modules, their corresponding details are displayed as tooltips. On clicking the device components, the corresponding description for the selected component is displayed by default in the Component Info pane and the Equipment tab with the following values.

- Description—Configured textual description of the component.
- Manufacturer—Name of the company that built and shipped the device.
- Model—Model of the FRU component.
- Name—Name of the chassis component.
- Part number—Part number of the chassis component.
- Serial number—Serial number of the chassis component. The serial number of the backplane is also the serial number of the router or switch chassis. Use this serial number when you need to contact Juniper Networks Customer Support about the router or switch chassis.

The Component Info pane and the Active Alarms monitor are displayed in the lower portion of the page.

The Active Alarms monitor shows any active alarm that has not yet been cleared. You can view the alarm name, the unique identifier assigned to the alarm, the person to which the alarm is assigned for corrective action, and the severity of the alarm. Click the **Launch Alarm Mgmt** icon (right upward-slanting arrow enclosed in a square) to navigate to the Fault mode and view the four standard alarm monitors available in Fault mode.

Active Alarms for the respective components are displayed when the component is clicked in the image of the chassis displayed. The components for which the alarms are displayed are Flexible Port Concentrator (FPC), Dense Port Concentrator (DPC), Physical Interface Card (PIC), Modular Interface Card (MIC), Routing Engine, Control Boards, fan trays, Switch Interface Board (SIB), and power supply module (PSM).

The following fields are displayed in the Active Alarms pane:

Table 242: Active Alarms Monitor

Table Column	Description
Severity	The severity of the alarm. Severity levels are: <ul style="list-style-type: none">• Critical—A critical condition exists; immediate action is necessary.• Major—A major error has occurred; escalate or notify as necessary.• Minor—A minor error has occurred; notify or monitor the condition.• Info—An informational message; no action is necessary.
Name	The alarm name.
Source	The IP address of the device or network element that generated the alarm. The SNMP agent is located at the source IP. In most cases, the source IP is the IP address of the switch or controller.
Last Updated	The date and time that the information for the alarm was last modified.

From the Chassis View window, click the **Details** icon (arrow enclosed in a square) at the top-right corner of the window to open the Chassis View Details page that lists the configured devices and their parameters in the form of a table.

Click the **Apply Configlet** button (pencil icon displayed beside the button) and use the links shown on the components in Chassis View to select the context and apply configlets.

- Related Documentation**
- [Deleting Devices from Chassis View on page 1345](#)
 - [Rebooting Devices After Examining the Status in Chassis View on page 1346](#)
 - [About Chassis View on page 1335](#)

Viewing Optical ILA Configuration and Status Details for Simplified Administration

Instead of using Junos OS CLI statements and operational commands to view optical ILA parameters, you can view an image of the optical ILA using Connectivity Services Director to obtain an intuitive and high-level understanding of the settings and alarms. This view enables you to modify the optical ILA settings to suit your network deployment needs in a simplified and optimal manner. Because the important optical ILA settings can be viewed alongside the visual representation of the entire chassis that is displayed, this method of managing the optical ILA settings provides a consolidated and cohesive interface for easy administration of the network.

To view the optical ILA configuration and status information:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the device for which you want to view the optical ILA settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. In the image of the device, select an optical ILA.

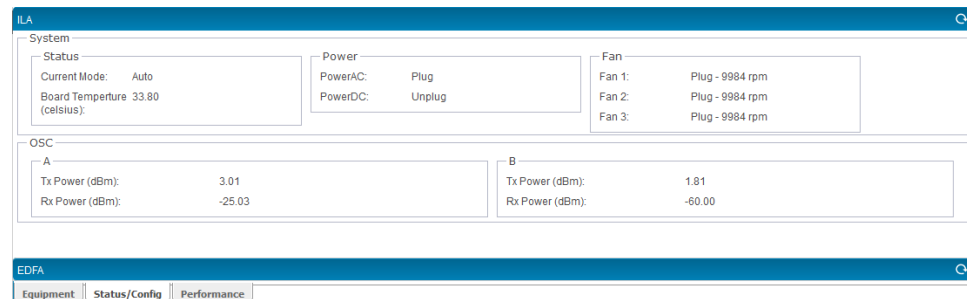
The ILA Optics dialog box is displayed at the lower part of the page. At the bottom of the dialog box, the Equipment, Status/Config, and Performance tabs are displayed.

6. Click the **Status/Config** tab at the bottom of the dialog box.

The configuration settings that pertain to the optical ILA are displayed in the ILA and EDFA panes. The ILA pane is expanded and displayed by default.

7. View the following details under different sections of the ILA pane. The ILA pane is shown in [Figure 107 on page 1584](#).

Figure 107: Status/Config Tab of an Optical ILA



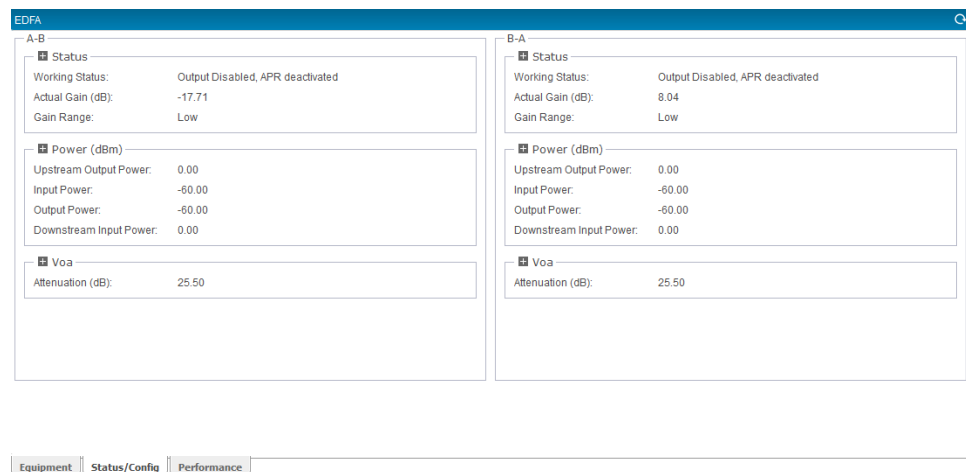
- In the System section, the following parameters are displayed:
 - Status—Operation status of the optical ILA in conjunction with the optical IPLC installed in the FPC or PIC slot
 - Current Mode—Mode of operation of the optical ILA, such as auto
 - Board Temperature (Celsius)—Temperature of the device in Celsius
 - Power—The power supplies need to be both AC or both DC. Only one power supply is required to power on the device; the second power supply provides redundancy. When the optical ILA has both power supplies installed and connected to the power supply, the device has full power redundancy. If a power supply fails or is removed, another power supply balances the electrical load without interruption. Each power supply provides 12-voltage direct current (VDC) output with a standby voltage of 12 VDC. The power supplies can be hot-swapped—you do not need to power off the router or disrupt the routing function to replace a power supply.
 - PowerAC—Indicates whether the AC power supply is connected or removed
 The AC power supplies in the optical ILA are hot-removable, and hot-insertable field-replaceable units (FRUs) that you can install without powering off the device or disrupting the routing function. The optical ILA has two power supplies. All of the power supplies are initially installed at the factory. Each of the 150-W power supplies has a single AC input. An optical ILA has twice the number of power supplies needed to power all the components in the device, which is known as 1+1 *n* redundancy.
 - PowerDC—Indicates whether the DC power supply is connected or removed
 The DC power supplies in the optical ILA are hot-removable and hot-insertable field-replaceable units (FRUs) that you can install without powering off the device or disrupting the routing function. The optical ILA has two power supplies. Both of the power supplies are initially installed at the factory. Each of the two 150-W power supplies has a single DC input. An optical ILA has twice the number of power supplies needed to power all the components in the device, which is known as 1+1 *n* redundancy.
 - Fan—The cooling system in an optical ILA consists of three 80-W fan modules. Each fan module has dual-counter rotating fans. These fan modules can be

hot-swapped—you do not need to power off the router or disrupt routing function to replace a fan module.

- Fan 1—Speed of fan 1 in revolutions per minute (rpm). Fan speed status is based on different chassis cooling requirements, such as spinning at high speed, intermediate speed, normal speed, or low speed.
- Fan 2—Speed of fan 2 in rpm
- Fan 3—Speed of fan 3 in rpm
- OSC—Displays the details of the two optical supervisory channel (OSCs) that are part of the optical ILA
 - A—Displays the transmitted and received optical power, in milliwatts (mW) and decibels referred to 1.0 mW (dBm), for the OSC A.
 - Tx Power (dBm)—Transmit laser output power (dBm) of OSC A
 - Rx Power (dBm)—Received laser input power (dBm) of OSC A
 - B—Displays the transmitted and received optical power, in milliwatts (mW) and decibels referred to 1.0 mW (dBm), for the OSC B.
 - Tx Power (dBm)—Transmit laser output power (dBm) of OSC B
 - Rx Power (dBm)—Received laser input power (dBm) of OSC B

8. Click the **EDFA** header at the bottom of the dialog box.

The EDFA pane is expanded and displayed, which shows the erbium-doped fiber amplifier (EDFA) properties for the ILA with the integrated photonic line card (IPLC) module installed in the FPC or PIC slot.



9. View the following details under different sections of the EDFA pane.

- A-B—Configuration and status settings of the EDFA in the direction from OSC A to OSC B
 - Status—Operational status of the EDFA in the direction from OSC A to OSC B

- Working Status—Working condition of the EDFA, such as output disabled or automatic power reduction (APR) deactivated
- Actual Gain (dB)—Gain or signal strength increase in decibels (dB) in the direction from OSC A to OSC B. The actual gain depends on the impedance of the attached device. An input power higher than -5 dBm can result in an alarm that can be cleared by correctly setting the gain value.
- Gain Range—Range of gain, such as high or low, in the direction from OSC A to OSC B
- Power (dBm)—Power specifications for the EDFA of the optical ILA in the direction from OSC A to OSC B
 - Upstream Output Power—Output power to the upstream network elements in the direction from OSC A to OSC B
 - Input Power—Current input power in the direction from OSC A to OSC B
 - Output Power—Current output power in the direction from OSC A to OSC B
 - Downstream Input Power—Input power to the downstream network elements in the direction from OSC A to OSC B
- Voa—Attenuation specifications of the optical ILA in the direction from OSC A to OSC B
 - Attenuation (dB)—Amount of reduction in transmitted power of the light signal in dB of the variable optical attenuator (VOA) present in the optical ILA in the direction from OSC A to OSC B
- B-A—Configuration and status settings of the EDFA in the reverse direction from OSC B to OSC A
 - Status—Operational status of the EDFA in the reverse direction from OSC B to OSC A
 - Working Status—Working condition of the EDFA, such as output disabled or ARP deactivated
 - Actual Gain (dB)—Gain or signal strength increase in decibels (dB) in the reverse direction from OSC B to OSC A. The actual gain depends on the impedance of the attached device. An input power higher than -5 dBm can result in an alarm that can be cleared by correctly setting the gain value.
 - Gain Range—Range of gain, such as high or low, in the reverse direction from OSC B to OSC A
 - Power (dBm)—Power specifications for the EDFA of the optical ILA in the reverse direction from OSC B to OSC A
 - Upstream Output Power—Output power to the upstream network elements in the reverse direction from OSC B to OSC A
 - Input Power—Current input power in the reverse direction from OSC B to OSC A

- Output Power—Current output power in the reverse direction from OSC B to OSC A
- Downstream Input Power—Input power to the downstream network elements in the reverse direction from OSC B to OSC A
- Voa—Attenuation specifications of the optical ILA in the direction from OSC B to OSC A
- Attenuation (dB)—Amount of reduction in transmitted power of the light signal in dB of the variable optical attenuator (VOA) present in the optical ILA in the direction from OSC B to OSC A

10. Click **Update** at the top of the dialog box to save the modified ILA settings. Alternatively, click **Cancel** to discard the changes.

You can click the **Refresh** (rotating arrow icon) button at the top of the dialog box to enable the latest settings be retrieved from the device and displayed.

**Related
Documentation**

- [Viewing a Graphical Image of Optical Inline Amplifier on page 1579](#)
- [Viewing Performance Monitoring Details of Optical ILAs for Detecting and Diagnosing Faults on page 1588](#)
- [Configuring Threshold-Crossing Alarms for Optical ILAs for Monitoring Link Performance on page 1597](#)
- [Changing Alarm Settings for the Optical ILAs on page 1599](#)

Viewing Performance Monitoring Details of Optical ILAs for Detecting and Diagnosing Faults

To analyze and resolve any faults associated with optical inline amplifiers (ILAs), it is essential to view the diagnostic data, warnings, and alarms for transport performance monitoring. The different types of parameters related to performance monitoring that are retrieved from the optical ILAs enable you to ensure service availability and verify or monitor individual services and the service network performance.

The performance monitoring capability in Connectivity Services Director displays information about the health of your network and changing conditions of your optical ILAs. Use this diagnosis and detection mechanism to identify problems with the equipment, pinpoint security attacks, or to analyze trends and categories of errors. This feature includes fault-monitoring details in the dashboard, in monitoring pages, and on a dedicated page that displays alarms, events, and system log messages that are generated. Performance monitoring parameters can be viewed in both chart and statistical formats. These charts and statistical details provide essential and cohesive information about system conditions, any discrepancies and malfunctioning, and protocols or components that need to be examined and debugged for better efficiency and working capacity. You can assess the performance of your network, not only at a point in time, but also over a period of time. This feature enables you to determine trending and network-health parameters; for example, whether service-level agreements (SLAs) have been violated.

To view the performance monitoring details of optical ILAs:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the device for which you want to define the optical ILA settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. Select an optical ILA in the image of the device.

The ILA Optics dialog box is displayed at the lower part of the page, which contains the Equipment, Status/Config, and Performance tabs.

6. Click the **Performance** tab at the bottom of the pane.

This pane contains the Perf Mon and TCA Config tabs. The Perf Mon tab of the ILA Optics PMs dialog box is displayed as shown in [Figure 108 on page 1589](#).

Figure 108: ILA Optics PMs Dialog Box

ILA Optics PMs (last updated: 11:58:36 AM, March 14, 2016)

Perf Mon	TCA Config				
PM Type/Group	15 Mins	TCA	24 Hrs	TCA	
Optical EDFA AB Input Power	[Chart]		[Chart]		
EDFA AB Input Power	-6000.00	--		--	
EDFA AB Input Power-Min	9900.00	<input checked="" type="checkbox"/>	9900.00	<input checked="" type="checkbox"/>	
EDFA AB Input Power-Max	-9900.00	<input checked="" type="checkbox"/>	-9900.00	<input checked="" type="checkbox"/>	
EDFA AB Input Power-Avg	-6000.00	--	-6000.00	--	
Optical EDFA AB Output Power	[Chart]		[Chart]		
EDFA AB Output Power	-6000.00	--		--	
EDFA AB Output Power-Min	9900.00	<input checked="" type="checkbox"/>	9900.00	<input checked="" type="checkbox"/>	
EDFA AB Output Power-Max	-9900.00	<input checked="" type="checkbox"/>	-9900.00	<input checked="" type="checkbox"/>	
EDFA AB Output Power-Avg	-6000.00	--	-6000.00	--	
Optical EDFA AB Pump1 Current	[Chart]		[Chart]		
EDFA AB Pump1 Current	8.00	--		--	
EDFA AB Pump1 Current-Min	5.00	<input checked="" type="checkbox"/>	4.00	<input checked="" type="checkbox"/>	
EDFA AB Pump1 Current-Max	27.00	<input checked="" type="checkbox"/>	29.00	<input checked="" type="checkbox"/>	
EDFA AB Pump1 Current-Avg	9.00	--	9.00	--	
Optical EDFA AB Pump1 Temperature	[Chart]		[Chart]		
EDFA AB Pump1 Temperature	2530.00	--		--	
EDFA AB Pump1 Temperature-Min	2530.00	<input checked="" type="checkbox"/>	2530.00	<input checked="" type="checkbox"/>	
EDFA AB Pump1 Temperature-Max	2540.00	<input checked="" type="checkbox"/>	2540.00	<input checked="" type="checkbox"/>	
EDFA AB Pump1 Temperature-Avg	2530.00	--	2530.00	--	
Optical EDFA AB Pump2 Current	[Chart]		[Chart]		
EDFA AB Pump2 Current	16.00	--		--	

Equipment | Status/Config | Performance

The following fields are displayed in the Perf Mon tab of the ILA Optics PMs dialog box. The date and time at which the dialog box was last refreshed is shown.



NOTE: Pump Turn-Down During a Loss of Signal— If LOS (Loss of Signal) is detected based on lack of receipt of the OSC signal at the input port of an amplifier, then the amplifier must turn down its pumps (to achieve no more than 0dBm total output power), until it detects receipt of a valid OSC signal at its input port. Likewise, if an upstream amplifier receives an OSC message from the downstream node that the OSC signal was not received downstream (LOS was declared downstream), it must also turn down its own pumps (to achieve no more than 0dBm total output power) until it receives an OSC message that the fault has cleared. Therefore, in addition to the automatic power reduction (APR) algorithm, the ILA software must keep the amplifier pumps disabled until a fiber connection is confirmed between the ILA output port and the input to the downstream optical node. This fiber connection is confirmed using the “handshaking” messages exchanged over Optical Supervisor Chanel (OSC). This behavior occurs during amplifier turn-up and during ongoing operation.

Local LOS—The software reads the LOS status for incoming signal from SFP. This LOS status can be used to shut off the amplifier pump. When local LOS is cleared, pumps need to be turned on again.

Remote LOS—Incoming LOS status is conveyed to OSC_FPGA. OSC_FPGA in turn sends this status to nextnode through some overhead bits. The next node OSC_FPGA would read the overhead bits and puts it in its “Remote LOS” register. OSC_FPGA also forwards the remote LOS status further down the chain through overhead bits in the same way. The software can read the “Remote LOS” value and take appropriate action of turning the amplifier pump on or off.

- Optical EDFA AB Input Power—Received input power of the optical erbium-doped fiber amplifier (EDFA) in the direction from optical supervisory channel (OSC) A to OSC B

EDFA AB Input Power—Received laser optical input power

EDFA AB Input Power-Min—Minimum received input power

EDFA AB Input Power-Avg—Average received laser power

EDFA AB Input Power-Max—Maximum received input power

- Optical EDFA AB Output Power—Transmitted output power of the optical EDFA in the direction from OSC A to OSC B

EDFA AB Output Power—Transmitted laser optical output power

EDFA AB Output Power-Min—Minimum transmitted laser output power

EDFA AB Output Power-Avg—Average transmitted laser output power

EDFA AB Output Power-Max—Maximum transmitted laser output power

- Optical EDFA AB Signal Output Power—Signal output power of the optical EDFA in the direction from OSC A to OSC B

EDFA AB Signal Output Power—Signal laser optical output power

EDFA AB Signal Output Power-Min—Minimum signal laser output power

EDFA AB Signal Output Power-Avg—Average signal laser output power

EDFA AB Signal Output Power-Max—Maximum signal laser output power

- Optical EDFA AB Pump1 Current—Pump1 current of the EDFA in the direction from OSC A to OSC B

EDFA AB Pump1 Current—Pump1 current of the EDFA from OSC A to OSC B

EDFA AB Pump1 Current-Min—Minimum pump1 current of the EDFA

EDFA AB Pump1 Current-Avg—Average pump1 current of the EDFA

EDFA AB Pump1 Current-Max—Maximum pump1 current of the EDFA

- Optical EDFA AB Pump1 Temperature—Pump1 temperature of the EDFA in the direction from OSC A to OSC B

EDFA AB Pump1 Temperature—Pump1 temperature of the EDFA from OSC A to OSC B

EDFA AB Pump1 Temperature-Min—Minimum pump1 temperature of the EDFA

EDFA AB Pump1 Temperature-Avg—Average pump1 temperature of the EDFA

EDFA AB Pump1 Temperature-Max—Maximum pump1 temperature of the EDFA

- Optical EDFA AB Pump2 Current—Pump2 current of the EDFA in the direction from OSC A to OSC B

EDFA AB Pump2 Current—Pump2 current of the EDFA from OSC A to OSC B

EDFA AB Pump2 Current-Min—Minimum pump2 current of the EDFA

EDFA AB Pump2 Current-Avg—Average pump2 current of the EDFA

EDFA AB Pump2 Current-Max—Maximum pump2 current of the EDFA

- Optical EDFA AB Pump2 Temperature—Pump2 temperature of the EDFA in the direction from OSC A to OSC B

EDFA AB Pump2 Temperature—Pump2 temperature of the EDFA from OSC A to OSC B

EDFA AB Pump2 Temperature-Min—Minimum pump2 temperature of the EDFA

EDFA AB Pump2 Temperature-Avg—Average pump2 temperature of the EDFA

EDFA AB Pump2 Temperature-Max—Maximum pump2 temperature of the EDFA

- Optical EDFA BA Input Power—Received input power of the optical erbium-doped fiber amplifier (EDFA) in the direction from optical supervisory channel (OSC) B to OSC A

EDFA BA Input Power—Received laser optical input power

EDFA BA Input Power-Min—Minimum received input power

EDFA BA Input Power-Avg—Average received laser power

EDFA BA Input Power-Max—Maximum received input power

- Optical EDFA BA Output Power—Transmitted output power of the optical EDFA in the direction from OSC B to OSC A

EDFA BA Output Power—Transmitted laser optical output power

EDFA BA Output Power-Min—Minimum transmitted laser output power

EDFA BA Output Power-Avg—Average transmitted laser output power

EDFA BA Output Power-Max—Maximum transmitted laser output power

- Optical EDFA BA Signal Output Power—Signal output power of the optical EDFA in the direction from OSC B to OSC A

EDFA BA Signal Output Power—Signal laser optical output power

EDFA BA Signal Output Power-Min—Minimum signal laser output power

EDFA BA Signal Output Power-Avg—Average signal laser output power

EDFA BA Signal Output Power-Max—Maximum signal laser output power

- Optical EDFA BA Pump1 Current—Pump1 current of the EDFA in the direction from OSC B to OSC A

EDFA BA Pump1 Current—Pump1 current of the EDFA from OSC B to OSC A

EDFA BA Pump1 Current-Min—Minimum pump1 current of the EDFA

EDFA BA Pump1 Current-Avg—Average pump1 current of the EDFA

EDFA BA Pump1 Current-Max—Maximum pump1 current of the EDFA

- Optical EDFA BA Pump1 Temperature—Pump1 temperature of the EDFA in the direction from OSC B to OSC A

EDFA BA Pump1 Temperature—Pump1 temperature of the EDFA from OSC B to OSC A

EDFA BA Pump1 Temperature-Min—Minimum pump1 temperature of the EDFA

EDFA BA Pump1 Temperature-Avg—Average pump1 temperature of the EDFA

EDFA BA Pump1 Temperature-Max—Maximum pump1 temperature of the EDFA

- Optical EDFA BA Pump2 Current—Pump2 current of the EDFA in the direction from OSC B to OSC A

EDFA BA Pump2 Current—Pump2 current of the EDFA from OSC B to OSC A

EDFA BA Pump2 Current-Min—Minimum pump2 current of the EDFA

EDFA BA Pump2 Current-Avg—Average pump2 current of the EDFA

EDFA BA Pump2 Current-Max—Maximum pump2 current of the EDFA

- Optical EDFA BA Pump2 Temperature—Pump2 temperature of the EDFA in the direction from OSC B to OSC A

EDFA BA Pump2 Temperature—Pump2 temperature of the EDFA from OSC B to OSC A

EDFA BA Pump2 Temperature-Min—Minimum pump2 temperature of the EDFA
 EDFA BA Pump2 Temperature-Avg—Average pump2 temperature of the EDFA
 EDFA BA Pump2 Temperature-Max—Maximum pump2 temperature of the EDFA

- Optical OSC A Fiber Loss—Fiber loss of OSC A
 Optical OSC A Fiber Loss—Fiber loss of OSC A
 Optical OSC A Fiber Loss-Min—Minimum fiber loss of OSC A
 Optical OSC A Fiber Loss-Avg—Average fiber loss of OSC A
 Optical OSC A Fiber Loss-Max—Maximum fiber loss of OSC A
- Optical OSC A Tx Power—Transmitted power of OSC A
 Optical OSC A Tx Power—Transmitted power of OSC A
 Optical OSC A Tx Power-Min—Minimum transmitted power of OSC A
 Optical OSC A Tx Power-Avg—Average transmitted power of OSC A
 Optical OSC A Tx Power-Max—Maximum transmitted power of OSC A
- Optical OSC A Rx Power—Received power of OSC A
 Optical OSC A Rx Power—Received power of OSC A
 Optical OSC A Rx Power-Min—Minimum received power of OSC A
 Optical OSC A Rx Power-Avg—Average received power of OSC A
 Optical OSC A Rx Power-Max—Maximum received power of OSC A
- Optical OSC B Fiber Loss—Fiber loss of OSC B
 Optical OSC B Fiber Loss—Fiber loss of OSC B
 Optical OSC B Fiber Loss-Min—Minimum fiber loss of OSC B
 Optical OSC B Fiber Loss-Avg—Average fiber loss of OSC B
 Optical OSC B Fiber Loss-Max—Maximum fiber loss of OSC B
- Optical OSC B Tx Power—Transmitted power of OSC B
 Optical OSC B Tx Power—Transmitted power of OSC B
 Optical OSC B Tx Power-Min—Minimum transmitted power of OSC B
 Optical OSC B Tx Power-Avg—Average transmitted power of OSC B
 Optical OSC B Tx Power-Max—Maximum transmitted power of OSC B
- Optical OSC B Rx Power—Received power of OSC B
 Optical OSC B Rx Power—Received power of OSC B
 Optical OSC B Rx Power-Min—Minimum received power of OSC B
 Optical OSC B Rx Power-Avg—Average received power of OSC B
 Optical OSC B Rx Power-Max—Maximum received power of OSC B

On the Perf Mon tab, for the TCA column, either a minus sign (–) is displayed that denotes that an alarm for threshold-exceed is not configured or a check mark is displayed and grayed out that indicates that the TCA for the particular attribute is configured.

7. In the 15 Mins column, click the **Chart** button for the performance monitoring parameter set for which you want to view the statistics for the last 15 minutes. This option enables you to view the statistics in a chart form. Performance monitoring information for the different parameters are displayed for the current 15-minute interval. By default, 96 records of 15-minute intervals are displayed.

A 15-Min *parameter-name* tab is displayed beside the TCA Config tab at the top-left corner of the Optics PMs dialog box. A graphical format of the statistics for the specified parameter is displayed on this tab.

8. Click the **15 Mins *parameter name*** tab.

- a. Select one of the following options from the drop-down menu:

- Select **View Chart** or the graphical icon (elliptical curve symbol) to display the chart of performance monitoring statistical metrics. A line graph is displayed with date and time along the horizontal axis and the parameter along the vertical axis. A color-coding format is used to display the different lines, and legends reference the parameter names corresponding to the lines displayed. Mouse over the points in the line graph to expand and show the value of the performance monitoring counters at a particular time.
- Select **View Grid** to switch over to the tabular format of display of performance monitoring statistics.

The records are displayed in tabular format. A serial number of the count of entries, the day, month, and year at which the entry was collected, and the time at which the entry was collected are displayed. The timestamp is the UTC time in the database that is mapped to the local time zone of the client computer.

- Select **Save Chart**, when you view the performance monitoring statistics in graphical format, to save the graph to a Microsoft Excel file, as a .png image. Click the pin icon on the upper-left corner to revert the tab to the original container panel.
- Select **Popout Tab** or the light blue triangle icon to view the dialog box as a separate window.

In the pop-up dialog box, you can do one of the following:

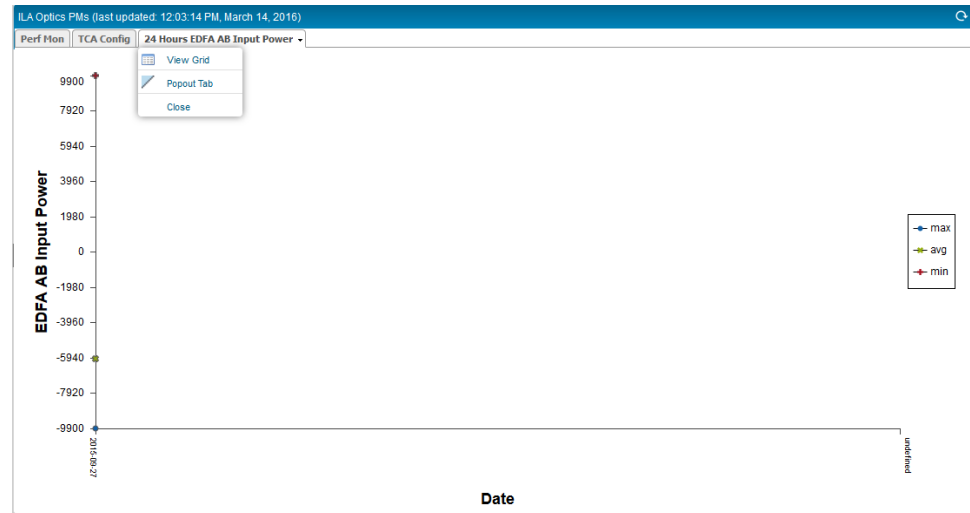
- In the From Date field, pull down the calendar and select the start date of the search. In the To Date field, pull down the calendar and select the end date of the search.
- Click **Reload** to refresh the contents and display the updated information for the specified time period.
- Click **Export Data** to transfer the data in graphical or statistical format to a spreadsheet or other business applications for future reference and archival.

The comma-separated value (CSV) format takes the raw data from the report and delineates the fields with commas so that the data is imported into popular spreadsheet programs.

- Click the **View Chart** button at the top-left corner of the dialog box to view the statistics in graphical format. Alternatively, click the **View Grid** button at the top-left corner of the dialog box to view the statistics in tabular format. The View Chart/Grid button is a toggle button.
 - Click **OK** to close the pop-up dialog box. Alternatively, press Esc to close the dialog box after you complete viewing the statistical details.
 - Click **Close** to close the 15-Min *parameter-name* tab.
9. In the 24-Hrs column, click the **Chart** button for the performance monitoring parameter set for which you want to view the statistics for the previous day. This option enables you to view the statistics in a chart form. Performance monitoring information for the different parameters are displayed for the current 24-hour interval. By default, records pertaining to the last 30 days are displayed when you view the performance monitoring counters for the 24-hour duration.

A 24 Hours *parameter-name* tab is displayed beside the TCA Config tab at the top-left corner of the Optics PMs dialog box as shown in [Figure 109 on page 1595](#). A graphical format of the statistics for the specified parameter is displayed on this tab.

Figure 109: 24 Hours Parameter-Name Tab of the ILA Optics PMs Dialog Box



10. Click the **24 Hours *parameter name*** tab.
- a. Select one of the following options from the drop-down menu:

- Select **View Chart** or the graphical icon (elliptical curve symbol) to display the chart of performance monitoring statistical metrics. A line graph is displayed with date along the horizontal axis and the parameter along the vertical axis. A color-coding format is used to display the different lines, and legends reference the parameter names corresponding to the lines displayed. Mouse over the points in the line graph to expand and show the value of the performance monitoring counters at a particular time.
- Select **View Grid** to switch over to the tabular format of display of performance monitoring statistics.
- Select **Save Chart**, when you view the performance monitoring statistics in graphical format, to save the graph to a Microsoft Excel file, as a .png image. Click the pin icon on the upper-left corner to revert the tab to the original container panel.
- Select **Popout Tab** or the light blue triangle icon to view the dialog box as a separate window.

In the pop-up dialog box, you can do one of the following:

- In the From Date field, pull down the calendar and select the start date of the search. In the To Date field, pull down the calendar and select the end date of the search. Click **Reload** to refresh the contents and display the updated information for the specified time period.
- Click **Export Data** to transfer the data in graphical or statistical format to a spreadsheet or other business applications for future reference and archival. The comma-separated value (CSV) format takes the raw data from the report and delineates the fields with commas so that the data is imported into popular spreadsheet programs.
- Click the **View Chart** button at the top-left corner of the dialog box to view the statistics in graphical format. Alternatively, click the **View Grid** button at the top-left corner of the dialog box to view the statistics in tabular format. The View Chart/Grid button is a toggle button.
- Click **OK** to close the pop-up dialog box. Alternatively, press Esc to close the dialog box after you complete viewing the statistical details.
- Click **Close** to close the 24 Hours *parameter-name* tab.

You can click the **Refresh** (rotating arrow icon) button at the top of the dialog box to enable the latest performance monitoring statistics to be polled and displayed.

Related Documentation

- [Viewing a Graphical Image of Optical Inline Amplifier on page 1579](#)
- [Viewing Optical ILA Configuration and Status Details for Simplified Administration on page 1583](#)
- [Configuring Threshold-Crossing Alarms for Optical ILAs for Monitoring Link Performance on page 1597](#)
- [Changing Alarm Settings for the Optical ILAs on page 1599](#)

Configuring Threshold-Crossing Alarms for Optical ILAs for Monitoring Link Performance

By monitoring the performance of links, you ensure that an end-to-end Ethernet service is always available over any path for a single link or multiple links spanning networks composed of multiple LANs. Link performance metrics enable operators to offer binding service-level agreements (SLAs) and generate new revenues from rate- and performance-guaranteed service packages that are customized to meet specific needs of their customers. To monitor link performance, you need to configure threshold-crossing alarms (TCAs) for optical inline amplifiers (ILAs)

TCAs are alarms that are activated when a certain configurable threshold—near-end measurement threshold or far-end measurement threshold—is crossed and remains so until the end of the 15-minute interval and the 24-hour interval for parameters such as the optical OLA. A near-end measurement is associated with ingress data frames and a far-end measurement is associated with egress data frames.

You can configure TCAs for both the minimum and maximum values for gauges and the maximum values for counters. A gauge represents a non-negative integer, which may increase or decrease, but never exceeds a maximum value. A gauge has its maximum value whenever the information being modeled is greater than or equal to the maximum value. If the TCA parameter subsequently goes below the maximum value, the gauge also decreases. A counter represents a non-negative integer that monotonically increases until it reaches a maximum value of $2^{32}-1$.

The timely detection of TCAs is essential to proactively manage an interface. TCAs are not an indication of a fault, but rather an indication that the entity may be close to a fault. You can enable the TCA that you want monitor. You can keep the default threshold settings or change the settings.

To configure the TCAs for optical ILA parameters:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner. The workspaces that are applicable to Build mode are displayed on the Tasks pane.

4. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the device for which you want to define the optical port settings.

The network tree is expanded and the selected device is highlighted.

- From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

- Select an optical ILA in the image of the device.

The ILA Optics dialog box is displayed, which contains the Equipment, Status/Config, and Performance tabs. For example, if you select an optical inline optical amplifier (ILA), which is used in conjunction with the integrated photonic line card (IPLC) that is installed in the PTX3000 routers, the optical ILA Optics dialog box is displayed beneath the graphical view of the chassis. The Equipment, Status/Config, and Performance tabs are displayed at the bottom of the page.

- Click the **Performance** tab at the bottom of the pane. The Optics PMs dialog box is displayed with the performance monitoring counters and metrics that pertain to the optical ports. This dialog box contains the Perf Mon and TCA Config tabs.

- Click the TCA Config tab to configure the TCAs for the different optical ILA attributes. The dialog box is refreshed to display the different performance monitoring parameters shown in [Figure 110 on page 1598](#). These parameters can be edited inline.

Inline editing enables you to modify previously defined settings easily and quickly. Embedded editing is enabled, which causes the grids showing the devices and interfaces to become modifiable directly; you do not need to highlight, edit, and save the changes every time.

A gray triangle in the upper-right corner of a field denotes that the value of that field or attribute has been modified.

Figure 110: TCA Config Tab of the ILA Optics PMs Dialog Box

PM Type/Group	Threshold-15Min	Threshold-24Hr	Enable
Optical EDFA AB Input Power			
EDFA AB Input Power	--	--	--
EDFA AB Input Power-Min	-2000	-2000	<input checked="" type="checkbox"/>
EDFA AB Input Power-Max	2000	2000	<input checked="" type="checkbox"/>
EDFA AB Input Power-Avg	--	--	--
Optical EDFA AB Output Power			
EDFA AB Output Power	--	--	--
EDFA AB Output Power-Min	-2000	-2000	<input checked="" type="checkbox"/>
EDFA AB Output Power-Max	2000	2000	<input checked="" type="checkbox"/>
EDFA AB Output Power-Avg	--	--	--
Optical EDFA AB Pump1 Current			
EDFA AB Pump1 Current	--	--	--
EDFA AB Pump1 Current-Min	20	20	<input checked="" type="checkbox"/>
EDFA AB Pump1 Current-Max	200	200	<input checked="" type="checkbox"/>
EDFA AB Pump1 Current-Avg	--	--	--
Optical EDFA AB Pump1 Temperature			
EDFA AB Pump1 Temperature	--	--	--
EDFA AB Pump1 Temperature-Min	2000	2000	<input checked="" type="checkbox"/>
EDFA AB Pump1 Temperature-Max	3000	3000	<input checked="" type="checkbox"/>
EDFA AB Pump1 Temperature-Avg	--	--	--

- For the parameters under each performance monitoring category for which you want to modify the TCA value, click the value in the Threshold-15Min or Threshold-24Hr

columns to set the TCA value for the 15-minute interval or 24-hour interval. You can also select Yes or No in the Enable column to enable or disable the TCA value for the specified parameter.

10. Click **Update** to save the configured threshold settings. Alternatively, click **Cancel** to discard the configuration.

**Related
Documentation**

- [Viewing a Graphical Image of Optical Inline Amplifier on page 1579](#)
- [Viewing Optical ILA Configuration and Status Details for Simplified Administration on page 1583](#)
- [Viewing Performance Monitoring Details of Optical ILAs for Detecting and Diagnosing Faults on page 1588](#)
- [Changing Alarm Settings for the Optical ILAs on page 1599](#)

Changing Alarm Settings for the Optical ILAs

You can modify the configuration settings for alarm settings of optical inline amplifiers (ILAs) using the Preferences page of the Connectivity Services Director application. To open the Preferences page, click the down arrow next to the System button in the Connectivity Services Director banner and select Preferences. The Preferences page opens with User Preferences as the default tab. Click the Fault tab of the Preferences page of the Connectivity Services Director GUI to enable individual alarms, set the retention period for alarms, configure alarm notifications, configure threshold alarms, and to specify the number of events to keep for each alarm. The Fault tab has multiple sections, which you can expand and collapse by clicking the arrow next to the section title:

- Global Settings, for configuring Faults settings such as global alarm notifications and alarm data retention.
- Individual Alarms and Threshold Settings, for configuring settings for individual alarms and threshold alarms.
- [Alarms for Optical ILAs on page 1600](#)
- [Configuring Global Alarm Notifications on page 1602](#)
- [Retaining Alarm History on page 1602](#)
- [Specifying Event History on page 1602](#)
- [Enabling Alarms on page 1602](#)
- [Changing the Severity of Individual Alarms on page 1603](#)
- [Configuring Threshold Alarms on page 1603](#)
- [Configuring Individual Alarm Notifications on page 1603](#)

Alarms for Optical ILAs

The following alarms are applicable for management of the optical ILA:

Alarm Name	Description
ILA::edfaEabCaliTableErr	Generated when the EDFA in the direction from optical supervisory channel (OSC) A to OSC B (Eab) has a calibration table error.
ILA::edfaEabCaseTemperature	Generated when the EDFA case temperature exceeds the configured threshold in the direction from OSC A to OSC B.
ILA::edfaEabInputLOS	Generated when the input loss of signal (LOS) is detected in the direction from OSC A to OSC B.
ILA::edfaEabOOG	Generated when the out-of-service out-of-gain (OOS OOG) condition occurs in the direction from OSC A to OSC B.
ILA::edfaEabOOP	Generated when the out-of-power (OOP) condition occurs in the direction from OSC A to OSC B.
ILA::edfaEabOutputLOS	Generated when an output LOS condition occurs in the direction from OSC A to OSC B.
ILA::edfaEabPump1EOL	Generated when the end-of-life (EoL) state for pump 1 of the EDFA occurs in the direction from OSC A to OSC B.
ILA::edfaEabPump2EOL	Generated when the end-of-life (EoL) state for pump 2 of the EDFA occurs in the direction from OSC A to OSC B.
ILA::edfaEabPump1Temperature	Generated when the temperature exceeds the threshold for pump 1 of the EDFA occurs in the direction from OSC A to OSC B.
ILA::edfaEabPump2Temperature	Generated when the temperature exceeds the threshold for pump 1 of the EDFA occurs in the direction from OSC A to OSC B.
ILA::edfaEabRFL	Generated when the radio frequency loss (RFL) occurs for the EDFA occurs in the direction from OSC A to OSC B.
ILA::edfaEbaCaliTableErr	Generated when the EDFA in the direction from optical supervisory channel (OSC) B to OSC A (Eba) has a calibration table error.
ILA::edfaEbaCaseTemperature	Generated when the EDFA case temperature exceeds the configured threshold in the direction from OSC B to OSC A.
ILA::edfaEbaInputLOS	Generated when the input loss of signal (LOS) is detected in the direction from OSC B to OSC A.
ILA::edfaEbaOOG	Generated when the out-of-gain (OOG) condition occurs in the direction from OSC B to OSC A.
ILA::edfaEbaOOP	Generated when the out-of-power (OOP) condition occurs in the direction from OSC B to OSC A.

Alarm Name	Description
ILA::edfaEbaOutputLOS	Generated when an output LOS condition occurs in the direction from OSC B to OSC A.
ILA::edfaEbaPump1EOL	Generated when the end-of-life (EoL) state for pump 1 of the EDFA occurs in the direction from OSC B to OSC A.
ILA::edfaEbaPump2EOL	Generated when the end-of-life (EoL) state for pump 2 of the EDFA occurs in the direction from OSC B to OSC A.
ILA::edfaEbaPump1Temperature	Generated when the temperature exceeds the threshold for pump 1 of the EDFA occurs in the direction from OSC B to OSC A.
ILA::edfaEbaPump2Temperature	Generated when the temperature exceeds the threshold for pump 1 of the EDFA occurs in the direction from OSC B to OSC A.
ILA::edfaEbaRFL	Generated when the radio frequency loss (RFL) occurs for the EDFA occurs in the direction from OSC B to OSC A.
ILA::ilaBoardTemperatureAbnormal	Generated when the ILA board temperature reaches an abnormal level.
ILA::ilaCommunicationAbnormal	Generated when the communication channel between the NMS system and the ILA reaches an abnormal level.
ILA::ilaACPowerAbnormal	Generated when the ILA AC power reaches an abnormal level.
ILA::ilaDCPowerAbnormal	Generated when the ILA DC power reaches an abnormal level.
ILA::ilaFan1OnlineAbnormal	Generated when the ILA fan tray controller 1 that is online reaches an abnormal level.
ILA::ilaFan1SpeedAbnormal	Generated when the speed of the optical ILA fan tray controller 1 reaches an abnormal level.
ILA::ilaFan2OnlineAbnormal	Generated when the ILA fan tray controller 1 that is online reaches an abnormal level.
ILA::ilaFan2SpeedAbnormal	Generated when the speed of the optical ILA fan tray controller 1 reaches an abnormal level.
ILA::ilaFan3OnlineAbnormal	Generated when the ILA fan tray controller 1 that is online reaches an abnormal level.
ILA::ilaFan3SpeedAbnormal	Generated when the speed of the optical ILA fan tray controller 1 reaches an abnormal level.
ILA::ilaSoftwareVersionAbnormal	Generated when the ILA software version reaches an abnormal level.
ILA::ilaTableErr	Generated when the ILA table error occurs.
ILA::oscaAddPowerLOS	Generated when the addition of power LOS condition occurs for the OSC A.

Alarm Name	Description
ILA::oscaDropPowerLOS	Generated when the dropping of power LOS condition occurs for the OSC A.
ILA::oscbAddPowerLOS	Generated when the addition of power LOS condition occurs for the OSC B.
ILA::oscbDropPowerLOS	Generated when the dropping of power LOS condition occurs for the OSC B.

Configuring Global Alarm Notifications

You can configure global e-mail notifications to be sent when any alarm with notifications enabled is generated. To configure global e-mail notifications, enter the e-mail addresses to receive global alarm notifications in the Alarm Notifications Destinations field in the Global Settings section. Separate addresses with a comma (,). For information about enabling notification for an alarm, see [“Configuring Individual Alarm Notifications” on page 152](#).

Retaining Alarm History

Use the **No. of days to keep Alarm** field in the Global Settings section to specify the number of days to keep alarm history. The default retention time is 120 days; but you can specify a period of 7 through 1000 days. Specifying a longer retention time consumes more database resources. To change the alarm retention duration, type a new value and click **OK** and **Yes** to confirm the change.

Specifying Event History

Use the **Events/Alarm** field in the Global Settings section to specify the number of event entries that are kept in the alarm history. The default setting for events is 20. To change the setting, type a new value and click **OK** and **Yes** to confirm the change.

Enabling Alarms

Ensure all devices are configured to send traps to Connectivity Services Director. This task is performed for the devices in Deploy mode through Set SNMP Trap Configuration.

Use the Individual Alarms and Threshold Settings section to disable and re-enable individual alarms or all alarms. Alarms appear on both tabs in the section: Alarm Settings and Threshold Settings. Fault alarms are preconfigured and initially enabled. To enable or disable alarms:

1. (Optional) Sort the alarms. By default, the list of alarms is sorted alphabetically within each category. You can also sort by description or alarm severity within a category by clicking a column heading.
2. Review the alarms and either select the check box in the heading to select all of the alarms or select the check box for the individual alarms you want to enable.
3. Click **OK** and **Yes** to confirm the alarm change.

Changing the Severity of Individual Alarms

You can change the severity of the alarms to match your corporate procedures and guidelines. For example, at your company a DoS attack might be considered a critical alarm, while Connectivity Services Director has a default severity for DoS attacks as a major alarm. Alarms appear on both tabs in the Individual Alarms and Threshold Settings section: Alarm Settings and Threshold Settings.

To change the severity of an alarm:

1. Select the current severity in the **Severity** column. A list of the severity levels appear.
2. Select the new severity level for the alarm.
3. Click **OK** and **Yes** to confirm the change to the severity setting.

To configure alarm notifications, see [“Configuring Individual Alarm Notifications” on page 152](#).

Configuring Threshold Alarms

Threshold alarms are alarms that are generated when a monitored value crosses the configured threshold. They provide enhanced visibility into potential issues on the network. You configure and manage threshold alarms the same way as other alarms. You also have the option of setting the threshold level of individual threshold alarms.

To set threshold alarm thresholds:

1. Select the **Threshold Settings** tab in the Individual Alarms and Threshold settings section of the Fault tab.
2. Click **Edit Settings** in the Threshold Settings column of the alarm threshold you want to edit.
3. Set the threshold in the window that opens.
4. Click **Save** to save the new threshold.

To configure alarm notifications, see [“Configuring Individual Alarm Notifications” on page 152](#).

Configuring Individual Alarm Notifications

You can configure e-mail notifications to be sent when an individual alarm is generated. When you enable notification for an alarm, the notifications are sent to the e-mail addresses configured for the alarm and the addresses configured for global alarm notifications. Alarms appear on both tabs in the Individual Alarms and Threshold Settings section: Alarm Settings and Threshold Settings.

To configure e-mail notification for an alarm name:

1. Select the check box in the alarm's Notification column.
If you later want to disable notification for the alarm, clear the check box.
2. Click **Edit Notification** in the Notification column. The Alarm Notification Details window opens.
3. Enter one or more e-mail addresses in the Notification Email Addresses field. Separate addresses with a comma (.).
You can later edit the addresses to send notifications to different addresses.
4. (Optional) Enter a comment in the Comments field. This comment is included in the e-mail notification message.
5. Click **Save**.

**Related
Documentation**

- [Viewing a Graphical Image of Optical Inline Amplifier on page 1579](#)
- [Viewing Optical ILA Configuration and Status Details for Simplified Administration on page 1583](#)
- [Viewing Performance Monitoring Details of Optical ILAs for Detecting and Diagnosing Faults on page 1588](#)
- [Configuring Threshold-Crossing Alarms for Optical ILAs for Monitoring Link Performance on page 1597](#)

Configuring and Monitoring Optical Integrated Photonic Line Cards

- Viewing a Graphical Image of the Optical Integrated Photonic Line Card on page 1605
- Configuring Optical IPLC for Easy and Optimal Deployment on page 1609
- Viewing Performance Monitoring Details of Optical IPLCs for Detecting and Diagnosing Faults on page 1617
- Configuring Threshold-Crossing Alarms for Optical IPLCs for Monitoring Link Performance on page 1629
- Increasing the Add and Drop Port Capacity of the IPLC Node to 64 Channels on page 1634
- Configuring a Two-Degree IPLC Node for Express Traffic by Increasing the Line Capacity on page 1636
- Configuring Optical IPLC Line Connectivity for Interoperation with Optical ILAs on page 1638
- Configuring the Wavelengths That Are Added and Dropped by the IPLC on page 1645
- Configuring the IPLC to Add or Drop Wavelengths to an Optical Interface on a Remote Chassis on page 1649
- Configuring the IPLC to Add or Drop Wavelengths to an Optical Interface on the Same Chassis on page 1651
- Bypassing a Wavelength on the IPLC on page 1652
- Changing Alarm Settings for the Optical IPLCs on page 1654
- Viewing Routing Engine Switchover Indicators in the Chassis Image on page 1661
- Viewing Alarm Indicators in the Chassis Image on page 1663
- Viewing Port Statistics for OTN PICs on page 1664
- Example: Configuring Two Fiber Line Terminations Using IPLCs for Optical Amplification in a Metro Linear Packet Optical Network on page 1668

Viewing a Graphical Image of the Optical Integrated Photonic Line Card

The Chassis View provides a pictorial representation of the optical integrated photonic line card (IPLC) of a PTX Series router. The optical ILA is used in conjunction with the IPLC that is installed in the PTX3000 Packet Transport Routers. The optical ILA operates with redundant hot-swappable pluggable power supplies which are either AC or DC.

The purpose of this view is to try and provide a comprehensive monitoring view of the health and status of deployed devices across the network. In this view all the managed devices are shown with their appropriate status and health based on the services and device settings applied. This view helps the operator to know the health and status across the network, it provides with the operator to quickly see the macro level information, which allows the operator to further analyze the information provided and quickly navigate to individual devices and take any further corrective measure required. It provides a cohesive tool for the operator to quickly see the micro-level information and take any further remediation action required.

To view a graphical image of the optical IPLC of PTX300 routers:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the PTX3000 router for which you want to view and configure the IPLC settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. From the graphical image of the PTX3000 router, click a particular IPLC module to display the associated details in the lower portion of the page. The Rotate and Perspective buttons enable you to view the images in required orientation.

6. Click the View Back (arrows in a square symbol) icon to cause the device image to rotate along the x-axis and display the rear view of the device. Alternatively, click the View Front icon to view the front plane of the device. The View Back and View Front icons are toggle options.

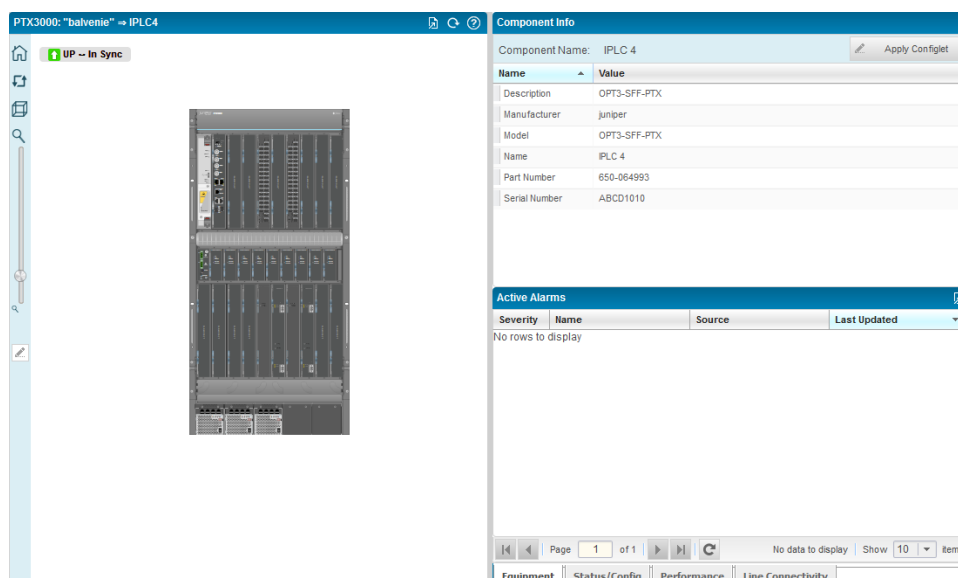
7. Click the Perspective (cube symbol) icon to display the device image in three-dimensional format. It is a toggle button, which causes the device image to be shown in either three-dimensional or one-dimensional format.

8. Select the level of magnification of the image by clicking the Zoom (magnifying glass) icon. The image is expanded and displayed.

Alternatively, use the slider control beneath the Zoom icon to change the level of magnification.

- Click the home icon to return to the front view of the chassis. The selected interface is surrounded with a colored outline based on the operational status. An interface that is operationally up is denoted in green and an interface that is operationally down is represented in red. The components are depicted as small colored icons in the front view of the equipment image as shown in [Figure 111 on page 1607](#).

Figure 111: Chassis View of a PTX Series Router with an Optical IPLC



In the graphical image of the device displayed, you can mouse over the different parts of the device, such as the interfaces, line cards, and slots. When you mouse over the different modules, their corresponding details are displayed as tooltips. On clicking the device components, the corresponding description for the selected component is displayed by default in the Component Info pane and the Equipment tab with the following values.

- Description—Configured textual description of the component.
- Manufacturer—Name of the company that built and shipped the device.
- Model—Model of the FRU component.
- Name—Name of the chassis component.
- Part number—Part number of the chassis component.
- Serial number—Serial number of the chassis component. The serial number of the backplane is also the serial number of the router or switch chassis. Use this serial number when you need to contact Juniper Networks Customer Support about the router or switch chassis.

The Component Info pane and the Active Alarms monitor are displayed in the lower portion of the page.

The Active Alarms monitor shows any active alarm that has not yet been cleared. You can view the alarm name, the unique identifier assigned to the alarm, the person to which the alarm is assigned for corrective action, and the severity of the alarm. Click the **Launch Alarm Mgmt** icon (right upward-slanting arrow enclosed in a square) to navigate to the Fault mode and view the four standard alarm monitors available in Fault mode.

Active Alarms for the respective components are displayed when the component is clicked in the image of the chassis displayed. The components for which the alarms are displayed are Flexible Port Concentrator (FPC), Dense Port Concentrator (DPC), Physical Interface Card (PIC), Modular Interface Card (MIC), Routing Engine, Control Boards, fan trays, Switch Interface Board (SIB), and power supply module (PSM).

The following fields are displayed in the Active Alarms pane:

Table 243: Active Alarms Monitor

Table Column	Description
Severity	The severity of the alarm. Severity levels are: <ul style="list-style-type: none"> • Critical—A critical condition exists; immediate action is necessary. • Major—A major error has occurred; escalate or notify as necessary. • Minor—A minor error has occurred; notify or monitor the condition. • Info—An informational message; no action is necessary.
Name	The alarm name.
Source	The IP address of the device or network element that generated the alarm. The SNMP agent is located at the source IP. In most cases, the source IP is the IP address of the switch or controller.
Last Updated	The date and time that the information for the alarm was last modified.

From the Chassis View window, click the **Details** icon (arrow enclosed in a square) at the top-right corner of the window to open the Chassis View Details page that lists the configured devices and their parameters in the form of a table.

Click the **Apply Configlet** button (pencil icon displayed beside the button) and use the links shown on the components in Chassis View to select the context and apply configlets.

Related Documentation

- [Deleting Devices from Chassis View on page 1345](#)
- [Rebooting Devices After Examining the Status in Chassis View on page 1346](#)
- [About Chassis View on page 1335](#)

Configuring Optical IPLC for Easy and Optimal Deployment

Instead of using Junos OS CLI statements and operational commands to configure optical integrated photonic line card (IPLC) settings and view the configured parameters, you can view an image of the optical IPLC using Connectivity Services Director to obtain an intuitive and high-level understanding of the settings and alarms. This view enables you to modify the optical IPLC settings to suit your network deployment needs in a simplified and optimal manner. Because the important optical IPLC settings can be configured alongside the visual representation of the entire chassis that is displayed, this method of managing the optical IPLC settings provides a consolidated and cohesive interface for easy deployment of settings on the optical IPLC.

To configure an optical IPLC:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the PTX3000 router for which you want to define the optical port settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. In the image of the device, select an optical IPLC—for example, an optical IPLC installed in a PTX3000 router.

The Component Info dialog box is displayed. At the lower part of the dialog box, the Equipment, Status/Config, Performance, and Line Connectivity tabs are displayed.

6. Click the **Status/Config** tab at the bottom of the dialog box.

The IPLC Line dialog box is displayed on the right pane with the configuration settings that pertain to the IPLC as shown in [Figure 112 on page 1610](#).

Figure 112: Status/Config Tab of the IPLC Line Dialog Box

IPLC Line

Update Cancel

Settings/Status

Expansion IPLC: NONE

Express IPLC: NONE

Main: Firmware Consistent alarm

EDFA 1: No Alarm

EDFA 2: No Alarm

WSS: No Alarm

Wavelength Configuration

Update Cancel Show All Wavelengths

Wavelength	configuration	end-point
1561.01	express-in	NA
1559.39	switch	et-10/0/0

Equipment Status/Config Performance Line Connectivity

7. In the Settings/Status section, do the following:

- a. From the Expansion IPLC list, select the FPC or PIC slot in which the expansion module of the IPLC is installed. Alternatively, select **NONE** if you do not want to specify an expansion module for the IPLC.

This setting creates an association between the specified IPLC base module and IPLC expansion module. The IPLC expansion module is an optical multiplexing and demultiplexing card that, when associated with an IPLC base module by using this statement, increases the ADD or DROP capacity of the system to 64 channels.



NOTE: When you increase the capacity to 64 channels, the IPLC base module handles the *odd* channels and the IPLC expansion module handles the *even* channels.

- b. From the Express IPLC list, select the FPC or PIC slot in which the IPLC that you want to configure as the express-in mode is configured. Alternatively, select **NONE** if you do not want to specify an express-in mode for the IPLC. You can switch the IPLC's wavelength to another IPLC residing on the same chassis by using the express-in mode. There can be only one association between two IPLC cards in express-in mode. For example, the IPLC in slot 0 can be configured to be bypassed and switched to the IPLC in slot 2. If you change the association, then the latest association is considered.

This setting enables you to form a logical connection between two IPLC base modules to form a single two-line node that can communicate either east-west or north-south. This configuration is used in IPLC ring scenarios and other network scenarios that require the IPLC to support two-line terminations.



NOTE: Before setting this option, you must connect the two IPLC base modules together through the PT IN and PT OUT ports on the front panel; otherwise a proper association between the two modules is not formed.



NOTE: You can configure only one logical association between two IPLC base modules in express-in mode.

- c. In the Main field, view the alarm, if any, that has been generated for the main board of the IPLC. A gray circle denotes no alarm, whereas a red circle denotes that an active alarm is present. Firmware Consistency Alarm, Internal Diagnostic Alarm, or Power Rail Alarm are possible values that can be displayed.
- d. In the EDFA1 field, view the alarm, if any, that has been generated for the ingress erbium-doped fiber amplifier (EDFA) of the IPLC. A gray circle denotes no alarm, whereas a red circle denotes that an active alarm is present. Input Power alarm, Out of Gain alarm, or Pump EOL alarm are possible values that can be displayed for EDFA1.

- e. In the EDFA2 field, view the alarm, if any, that has been generated for the egress EDFA of the IPLC. A gray circle denotes no alarm, whereas a red circle denotes that an active alarm is present. Output Power alarm, Out of Gain alarm, or Pump EOL alarm are possible values that can be displayed for EDFA2.
 - f. In the WSS field, view the alarm, if any, that has been generated for the wavelength selective switching (WSS) module of the optical IPLC. A gray circle denotes no alarm, whereas a red circle denotes that an active alarm is present. WSS Module FAIL, WSS Firmware Image Corrupted, WSS Firmware Version out-of-date, WSS Voltage Alarm - High, WSS Voltage Alarm - Low, WSS Temperature - High, or WSS temperature - Low are possible values that can be displayed.
 - g. Click **Update** above the Settings/Status section to save the specified configuration settings. Alternatively, click **Cancel** to discard the configuration settings.
8. In the Wavelength Configuration section, do the following:

All port wavelength frequencies are controlled by the WSS of the optical IPLC and configured on a wavelength-by-wavelength basis. The mapping for the wavelengths, frequencies, and ports is fixed. Each port is assigned a specific frequency and wavelength depending on whether the port is on the IPLC base module or expansion module.

- a. Select the **Show All Wavelengths** check box to display all available wavelengths supported by the PTX3000 router. The wavelength values can be any of the following:
 - **1528.38**—1528.38 nanometers (nm), corresponds to a 50-GHz grid
 - **1528.77**—1528.77 nm, corresponds to 50-GHz and 100-GHz grids
 - **1529.16**—1529.16 nm, corresponds to a 50-GHz grid
 - **1529.55**—1529.55 nm, corresponds to 50-GHz and 100-GHz grids
 - **1529.94**—1529.94 nm, corresponds to a 50-GHz grid
 - **1530.33**—1530.33 nm, corresponds to 50-GHz and 100-GHz grids
 - **1530.72**—1530.72 nm, corresponds to a 50-GHz grid
 - **1531.12**—1531.12 nm, corresponds to 50-GHz and 100-GHz grids
 - **1531.51**—1531.51 nm, corresponds to a 50-GHz grid
 - **1531.90**—1531.90 nm, corresponds to 50-GHz and 100-GHz grids
 - **1532.29**—1532.29 nm, corresponds to a 50-GHz grid
 - **1532.68**—1532.68 nm, corresponds to 50-GHz and 100-GHz grids
 - **1533.07**—1533.07 nm, corresponds to a 50-GHz grid
 - **1533.47**—1533.47 nm, corresponds to 50-GHz and 100-GHz grids
 - **1533.86**—1533.86 nm, corresponds to a 50-GHz grid
 - **1534.25**—1534.25 nm, corresponds to 50-GHz and 100-GHz grids
 - **1534.64**—1534.64 nm, corresponds to a 50-GHz grid

- **1535.04**—1535.04 nm, corresponds to 50-GHz and 100-GHz grids
- **1535.43**—1535.43 nm, corresponds to a 50-GHz grid
- **1535.82**—1535.82 nm, corresponds to 50-GHz and 100-GHz grids
- **1536.22**—1536.22 nm, corresponds to a 50-GHz grid
- **1536.61**—1536.61 nm, corresponds to 50-GHz and 100-GHz grids
- **1537.00**—1537.00 nm, corresponds to a 50-GHz grid
- **1537.40**—1537.40 nm, corresponds to 50-GHz and 100-GHz grids
- **1537.79**—1537.79 nm, corresponds to a 50-GHz grid
- **1538.19**—1538.19 nm, corresponds to 50-GHz and 100-GHz grids
- **1538.58**—1538.58 nm, corresponds to a 50-GHz grid
- **1538.98**—1538.98 nm, corresponds to 50-GHz and 100-GHz grids
- **1539.37**—1539.37 nm, corresponds to a 50-GHz grid
- **1539.77**—1539.77 nm, corresponds to 50-GHz and 100-GHz grids
- **1540.16**—1540.16 nm, corresponds to a 50-GHz grid
- **1540.56**—1540.56 nm, corresponds to 50-GHz and 100-GHz grids
- **1540.95**—1540.95 nm, corresponds to a 50-GHz grid
- **1541.35**—1541.35 nm, corresponds to 50-GHz and 100-GHz grids
- **1541.75**—1541.75 nm, corresponds to a 50-GHz grid
- **1542.14**—1542.14 nm, corresponds to 50-GHz and 100-GHz grids
- **1542.54**—1542.54 nm, corresponds to a 50-GHz grid
- **1542.94**—1542.94 nm, corresponds to 50-GHz and 100-GHz grids
- **1543.33**—1543.33 nm, corresponds to a 50-GHz grid
- **1543.73**—1543.73 nm, corresponds to 50-GHz and 100-GHz grids
- **1544.13**—1544.13 nm, corresponds to a 50-GHz grid
- **1544.53**—1544.53 nm, corresponds to 50-GHz and 100-GHz grids
- **1544.92**—1544.92 nm, corresponds to a 50-GHz grid
- **1545.32**—1545.32 nm, corresponds to 50-GHz and 100-GHz grids
- **1545.72**—1545.72 nm, corresponds to a 50-GHz grid
- **1546.12**—1546.12 nm, corresponds to 50-GHz and 100-GHz grids
- **1546.52**—1546.52 nm, corresponds to a 50-GHz grid
- **1546.92**—1546.92 nm, corresponds to 50-GHz and 100-GHz grids
- **1547.32**—1547.32 nm, corresponds to a 50-GHz grid
- **1547.72**—1547.72 nm, corresponds to 50-GHz and 100-GHz grids

- **1548.11**—1548.11 nm, corresponds to a 50-GHz grid
- **1548.51**—1548.51 nm, corresponds to 50-GHz and 100-GHz grids
- **1548.91**—1548.91 nm, corresponds to a 50-GHz grid
- **1549.32**—1549.32 nm, corresponds to 50-GHz and 100-GHz grids
- **1549.72**—1549.72 nm, corresponds to a 50-GHz grid
- **1550.12**—1550.12 nm, corresponds to 50-GHz and 100-GHz grids
- **1550.52**—1550.52 nm, corresponds to a 50-GHz grid
- **1550.92**—1550.92 nm, corresponds to 50-GHz and 100-GHz grids
- **1551.32**—1551.32 nm, corresponds to a 50-GHz grid
- **1551.72**—1551.72 nm, corresponds to 50-GHz and 100-GHz grids
- **1552.12**—1552.12 nm, corresponds to a 50-GHz grid
- **1552.52**—1552.52 nm, corresponds to 50-GHz and 100-GHz grids
- **1552.93**—1552.93 nm, corresponds to a 50-GHz grid
- **1553.33**—1554.33 nm, corresponds to 50-GHz and 100-GHz grids
- **1553.73**—1554.73 nm, corresponds to a 50-GHz grid
- **1554.13**—1554.13 nm, corresponds to 50-GHz and 100-GHz grids
- **1554.54**—1554.54 nm, corresponds to a 50-GHz grid
- **1554.94**—1554.94 nm, corresponds to 50-GHz and 100-GHz grids
- **1555.34**—1555.34 nm, corresponds to a 50-GHz grid
- **1555.75**—1555.75 nm, corresponds to 50-GHz and 100-GHz grids
- **1556.15**—1556.15 nm, corresponds to a 50-GHz grid
- **1556.55**—1556.55 nm, corresponds to 50-GHz and 100-GHz grids
- **1556.96**—1556.96 nm, corresponds to a 50-GHz grid
- **1557.36**—1557.36 nm, corresponds to 50-GHz and 100-GHz grids
- **1557.77**—1557.77 nm, corresponds to a 50-GHz grid
- **1558.17**—1558.17 nm, corresponds to 50-GHz and 100-GHz grids
- **1558.58**—1558.58 nm, corresponds to a 50-GHz grid
- **1558.98**—1558.98 nm, corresponds to 50-GHz and 100-GHz grids
- **1559.39**—1559.39 nm, corresponds to a 50-GHz grid
- **1559.79**—1559.79 nm, corresponds to 50-GHz and 100-GHz grids
- **1560.20**—1560.20 nm, corresponds to a 50-GHz grid
- **1560.61**—1560.61 nm, corresponds to 50-GHz and 100-GHz grids
- **1561.01**—1561.01 nm, corresponds to a 50-GHz grid

- **1561.42**—1561.42 nm, corresponds to 50-GHz and 100-GHz grids
- **1561.83**—1561.83 nm, corresponds to a 50-GHz grid
- **1562.23**—1562.23 nm, corresponds to 50-GHz and 100-GHz grids
- **1562.64**—1562.64 nm, corresponds to a 50-GHz grid
- **1563.05**—1563.05 nm, corresponds to 50-GHz and 100-GHz grids
- **1563.45**—1563.45 nm, corresponds to a 50-GHz grid
- **1563.86**—1563.86 nm, corresponds to 50-GHz and 100-GHz grids
- **1564.27**—1564.27 nm, corresponds to a 50-GHz grid
- **1564.68**—1564.68 nm, corresponds to 50-GHz and 100-GHz grids
- **1565.09**—1565.09 nm, corresponds to a 50-GHz grid
- **1565.50**—1565.50 nm, corresponds to 50-GHz and 100-GHz grids
- **1565.90**—1565.90 nm, corresponds to a 50-GHz grid
- **1566.31**—1566.31 nm, corresponds to 50-GHz and 100-GHz grids
- **1566.72**—1566.72 nm, corresponds to a 50-GHz grid
- **1567.13**—1567.13 nm, corresponds to 50-GHz and 100-GHz grids
- **1567.54**—1567.54 nm, corresponds to a 50-GHz grid
- **1567.95**—1567.95 nm, corresponds to 50-GHz and 100-GHz grids
- **1568.36**—1568.36 nm, corresponds to a 50-GHz grid
- **1568.77**—1568.77 nm, corresponds to 50-GHz and 100-GHz grids

The default is 1550.12—1550.12 nm, corresponds to 50-GHz and 100-GHz grids

b. For a particular wavelength displayed in the table, click in the cell in the **configuration** column, and then click the drop-down arrow. The following values are displayed on the drop-down menu:

- **blocked**—By default, if there is no explicit configuration for the IPLC wavelength, then that wavelength is in blocked mode.
- **switch**—Enables you to switch a wavelength present on an IPLC module to an optical interface on the same or different chassis. You can specify the dense wavelength-division multiplexing (DWDM) interface on the local chassis to which you want to switch the specified wavelength. Otherwise, you can switch the specified wavelength on the local chassis to the remote chassis.
- **express-in**—Enables you to form a logical connection between two IPLC base modules to form a single two-line node that can communicate either east-west or north-south. This configuration is used in IPLC ring scenarios and other network scenarios that require the IPLC to support two-line terminations.

c. For a particular wavelength setting that you specified in the **configuration** column for the IPLC, click in the cell in the **end-point** column, and then click the drop-down arrow.

A list of interface names that are present on the same chassis as the IPLC are displayed on the drop-down menu. You can select the optical interface on the same chassis to which the IPLC base module must switch the wavelength. Before you configure this setting, be sure to configure the wavelength on the local optical interface so that the wavelength is compatible with the wavelength you are switching on the IPLC. Alternatively, select **remote** to configure the IPLC to switch a particular wavelength to an optical interface on a remote chassis. Before you configure this setting, be sure to configure the wavelength on the remote optical interface so that the wavelength is compatible with the wavelength you are switching on the IPLC.



NOTE: The end-point field displays NA if you select the value in the configuration column for a specific wavelength as **blocked** or **express-in**. The end-point field is configurable only for switch wavelength mode.

- d. Click **Update** in the Wavelength Configuration section to save the specified configuration settings. Alternatively, click **Cancel** to discard the configuration settings.

You can click the **Refresh** (rotating arrow icon) button at the top of the dialog box to enable the latest settings be retrieved from the device and displayed.

**Related
Documentation**

- [Viewing Performance Monitoring Details of Optical IPLCs for Detecting and Diagnosing Faults on page 1617](#)
- [Configuring Threshold-Crossing Alarms for Optical IPLCs for Monitoring Link Performance on page 1629](#)

Viewing Performance Monitoring Details of Optical IPLCs for Detecting and Diagnosing Faults

To analyze and resolve any faults associated with optical integrated photonic line cards (IPLCs), it is essential to view the diagnostic data, warnings, and alarms for transport performance monitoring. The different types of parameters related to performance monitoring that are retrieved from the optical IPLCs enable you to ensure service availability and verify or monitor individual services and the service network performance.

The performance monitoring capability in Connectivity Services Director displays information about the health of your network and changing conditions of your optical IPLCs. Use this diagnosis and detection mechanism to identify problems with the equipment, pinpoint security attacks, or to analyze trends and categories of errors. This feature includes fault-monitoring details in the dashboard, in monitoring pages, and on a dedicated page that displays alarms, events, and system log messages that are generated. Performance monitoring parameters can be viewed in both chart and statistical formats. These charts and statistical details provide essential and cohesive information about system conditions, any discrepancies and malfunctioning, and protocols or components that need to be examined and debugged for better efficiency and working capacity. You can assess the performance of your network, not only at a point in time, but also over a period of time. This feature enables you to determine trending and network-health parameters; for example, whether service-level agreements (SLAs) have been violated.

To view the performance monitoring details of IPLC optics:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the PTX300 router for which you want to define the optical IPLC settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. In the image of the device, select an optical IPLC in the image of the device—for example, an optical integrated photonic line card (IPLC) installed in a PTX3000 router.

The Component Info dialog box is displayed. At the lower part of the dialog box, the Equipment, Status/Config, Performance, and Line Connectivity tabs are displayed.

- Click the **Performance** tab at the bottom of the pane.

The performance monitoring counters and metrics that pertain to the IPLC are displayed. The IPLC Optics PMs dialog box is displayed. This dialog box contains the Perf Mon and TCA Config tabs as shown in [Figure 113 on page 1618](#).

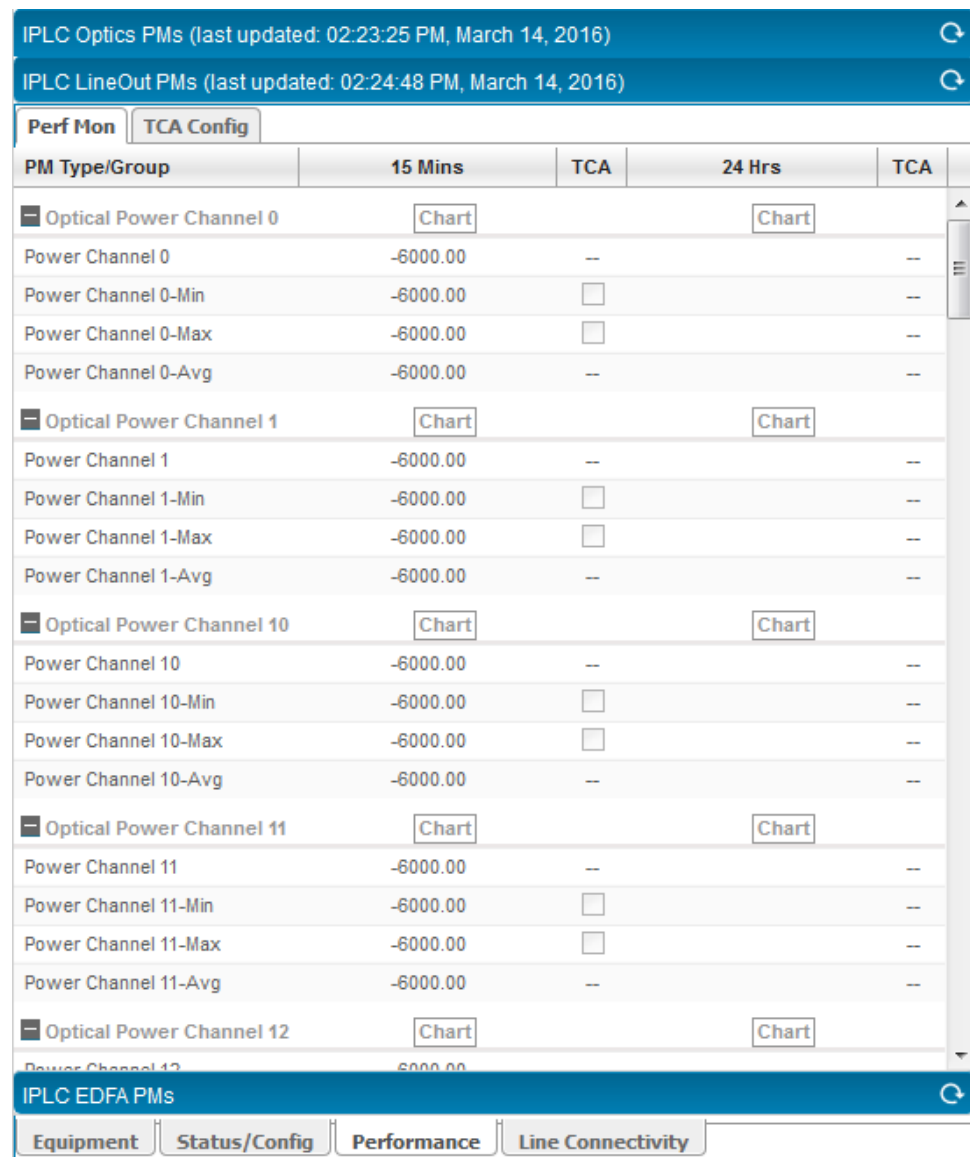
The following fields are displayed in the Perf Mon tab of the IPLC Optics PMs dialog box. The date and time at which the dialog box was last refreshed is shown.

Figure 113: Perf Mon Tab of the IPLC Optics PMs Dialog Box

IPLC Optics PMs (last updated: 02:19:43 PM, March 14, 2016)				
<div> <div>Perf Mon</div> <div>TCA Config</div> </div>				
PM Type/Group	15 Mins	TCA	24 Hrs	TCA
<div>Optical Line OUT VOA</div> <div>Chart</div>			<div>Chart</div>	
Line OUT VOA	260.00	--		--
Line OUT VOA-Min	170.00	<input type="checkbox"/>	450.00	<input type="checkbox"/>
Line OUT VOA-Max	360.00	<input type="checkbox"/>	1130.00	<input type="checkbox"/>
Line OUT VOA-Avg	265.00	--	840.00	--
<div>Optical OSC Fiber Loss</div> <div>Chart</div>			<div>Chart</div>	
OSC Fiber Loss	0.00	--		--
OSC Fiber Loss-Min	0.00	<input type="checkbox"/>	0.00	<input type="checkbox"/>
OSC Fiber Loss-Max	0.00	<input type="checkbox"/>	0.00	<input type="checkbox"/>
OSC Fiber Loss-Avg	0.00	--	0.00	--
<div>Optical OSC Rx Power</div> <div>Chart</div>			<div>Chart</div>	
OSC Rx Power	171.00	--		--
OSC Rx Power-Min	171.00	<input type="checkbox"/>	0.00	<input type="checkbox"/>
OSC Rx Power-Max	172.00	<input type="checkbox"/>	0.00	<input type="checkbox"/>
OSC Rx Power-Avg	171.00	--	0.00	--
<div>Optical OSC Tx Power</div> <div>Chart</div>			<div>Chart</div>	
OSC Tx Power	8650752.00	--		--
OSC Tx Power-Min	8650752.00	<input type="checkbox"/>	0.00	<input type="checkbox"/>
OSC Tx Power-Max	8650752.00	<input type="checkbox"/>	0.00	<input type="checkbox"/>
OSC Tx Power-Avg	8650752.00	--	0.00	--
<div>Optical Power AWG Add</div> <div>Chart</div>			<div>Chart</div>	
Power AWG Add	0.00	--		--
IPLC LineOut PMs				
IPLC EDFA PMs				
<div> <div>Equipment</div> <div>Status/Config</div> <div>Performance</div> <div>Line Connectivity</div> </div>				

- Line OUT VOA—Line-out Variable Optical Attenuator (VOA).
 - Line OUT VOA-Min—Minimum line-out VOA
 - Line OUT VOA-Max—Maximum line-out VOA
 - Line OUT VOA-Avg—Average line-out VOA
 - OSC Fiber Loss—Fiber loss of the Optical Service Channel (OSC)
 - OSC Fiber Loss-Min—Minimum fiber loss of the OSC
 - OSC Fiber Loss-Avg—Average fiber loss of the OSC
 - OSC Fiber Loss-Max—Maximum fiber loss of the OSC
 - OSC Tx Power—Transmitted power of the OSC
 - OSC Tx Power-Min—Minimum transmitted power of the OSC
 - OSC Tx Power-Avg—Average transmitted power of the OSC
 - OSC Tx Power-Max—Maximum transmitted power of the OSC
 - OSC Rx Power—Received power of the OSC
 - OSC Rx Power-Min—Minimum received power of the OSC
 - OSC Rx Power-Avg—Average received power of the OSC
 - OSC Rx Power-Max—Maximum received power of the OSC
 - Power AWG Add—Arrayed Waveguide Grating (AWG) added power
 - Power AWG Add-Min—Minimum AWG added power
 - Power AWG Add-Avg—Average AWG added power
 - Power AWG Add-Max—Maximum AWG added power
 - Power Express In—Power of the express-in mode of the IPLC
 - Power Express In-Min—Minimum power of the express-in mode of the IPLC
 - Power Express In-Avg—Average power of the express-in mode of the IPLC
 - Power Express In-Max—Maximum power of the express-in mode of the IPLC
7. Click the **IPLC LineOut PMs** header at the bottom of the dialog box. The IPLC LineOut PMs pane is expanded and displayed as shown in [Figure 114 on page 1620](#). This pane contains the PerfMon and TCA Config tabs.

Figure 114: IPLC LineOut PMs Dialog Box



The following fields are displayed in the Perf Mon tab of the IPLC LineOut PMs dialog box. The date and time at which the dialog box was last refreshed is shown.

- OCM Power Channel—Power line-out reading of the Optical Channel Monitor (OCM)
- OCM Power Channel-Min—Minimum power line-out of the OCM
- OCM Power Channel-Avg—Average power line-out of the OCM
- OCM Power Channel-Max—Maximum power line-out of the OCM

The power line-out values for 31 power channels that are present in the IPLC are listed in the IPLC LineOut PMs dialog box.

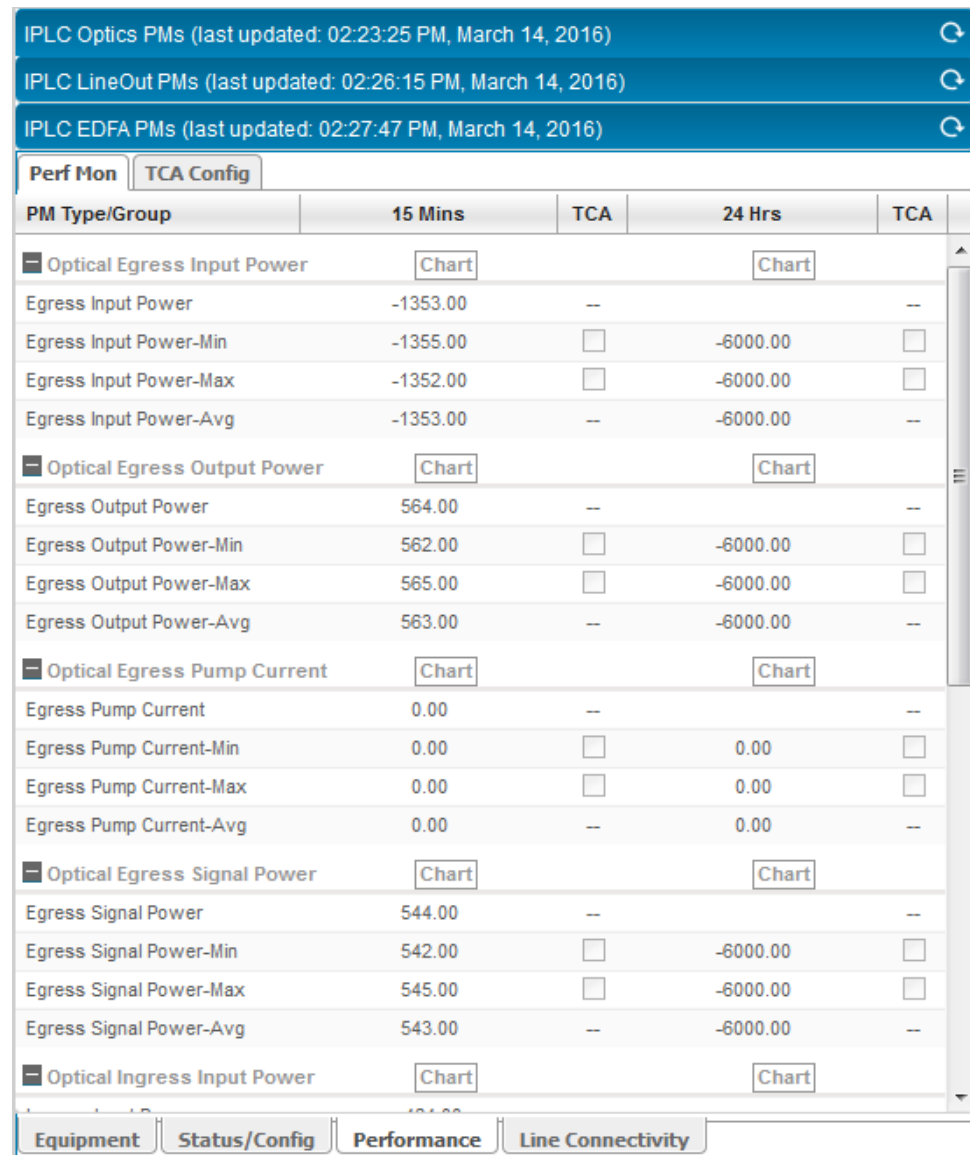


NOTE: An optical channel monitor (OCM) with three points of observation including:

- The booster EDFA (E1) output
- The pre-amplifier EDFA (E2) output.
- The combined channels of the local add function at the input of the WSS, which indicates which channels (both odd and even channels) are being added locally.
- An optical supervisory channel (OSC), which communicates in-band with the far end IPLC modules and is used for the analysis of the fiber span characteristics, performance monitoring, and IPLC fault handling. Simple topology discovery logic communicates with the ILAs and PTX3000 nodes.
- An optical splitter is used to broadcast the received signal from the output of the pre-amplifier (E2) towards both DROP and PT IN and PT OUT ports.
- The following are the four power monitors:
 - **AWG Add**—Monitors the input of the wavelength selective switch (WSS) measuring the total input power of the combined channels of the local add function (both odd and even channels).
 - **Express In**—Monitors the input of the WSS measuring the total input power at the input to the WSS coming from the PT IN and PT OUT express ports.
 - **Line In**—Monitors the input at the LINE IN port, for detection of the incoming line signal optical power. The remaining PDs
 - **Line Out**—Monitors the output at the LINE OUT port, for detection of the outgoing line signal optical power.

8. Click the **IPLC EDFA PMs** header at the bottom of the dialog box. The IPLC EDFA PMs pane is expanded and displayed as shown in [Figure 115 on page 1622](#). This pane contains the PerfMon and TCA Config tabs.

Figure 115: IPLC EDFA PMs Dialog Box



The following fields are displayed in the Perf Mon tab of the IPLC EDFA PMs dialog box. The date and time at which the dialog box was last refreshed is shown.

- Ingress Input Power—Ingress EDFA input power
 - Ingress Input Power-Min—Minimum ingress EDFA input power
 - Ingress Input Power-Avg—Average ingress EDFA input power
 - Ingress Input Power-Max—Maximum ingress EDFA input power
- Ingress Output Power—Ingress EDFA output power
 - Ingress Output Power-Min—Minimum ingress EDFA output power
 - Ingress Output Power-Avg—Average ingress EDFA output power

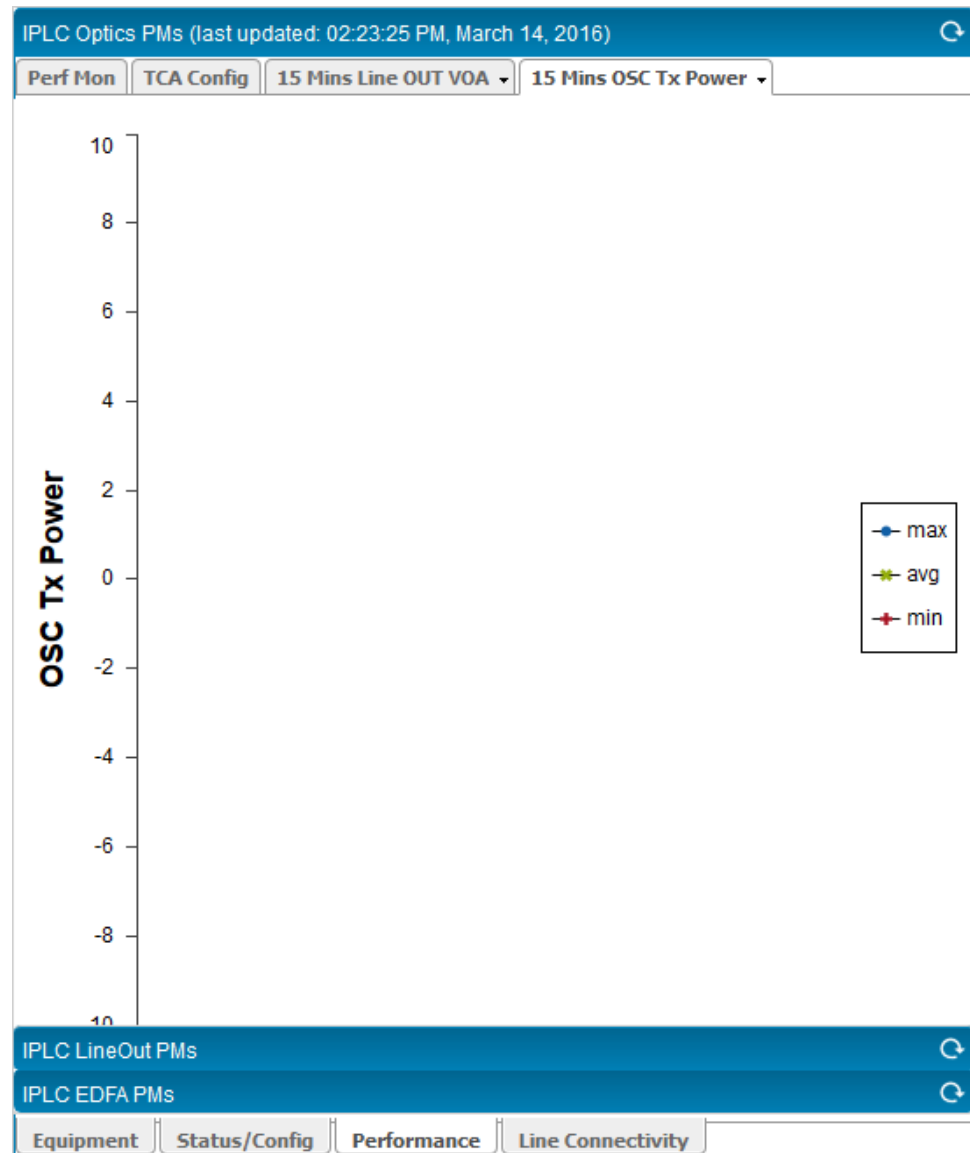
- Ingress Output Power-Max—Maximum ingress EDFA output power
- Ingress Signal Power—Ingress EDFA signal power
 - Ingress Signal Power-Min—Minimum ingress EDFA signal power
 - Ingress Signal Power-Avg—Average ingress EDFA signal power
 - Ingress Signal Power-Max—Maximum ingress EDFA signal power
- Ingress Pump Current—Ingress EDFA pump current
 - Ingress Pump Current-Min—Minimum ingress EDFA pump current
 - Ingress Pump Current-Avg—Average ingress EDFA pump current
 - Ingress Pump Current-Max—Maximum ingress EDFA pump current
- Egress Input Power—Egress EDFA input power
 - Egress Input Power-Min—Minimum egress EDFA input power
 - Egress Input Power-Avg—Average egress EDFA input power
 - Egress Input Power-Max—Maximum egress EDFA input power
- Egress Output Power—Egress EDFA output power
 - Egress Output Power-Min—Minimum egress EDFA output power
 - Egress Output Power-Avg—Average egress EDFA output power
 - Egress Output Power-Max—Maximum egress EDFA output power
- Egress Signal Power—Egress EDFA signal power
 - Egress Signal Power-Min—Minimum egress EDFA signal power
 - Egress Signal Power-Avg—Average egress EDFA signal power
 - Egress Signal Power-Max—Maximum egress EDFA signal power
- Egress Pump Current—Egress EDFA pump current
 - Egress Pump Current-Min—Minimum egress EDFA pump current
 - Egress Pump Current-Avg—Average egress EDFA pump current
 - Egress Pump Current-Max—Maximum egress EDFA pump current

On the Perf Mon tab, for the TCA column, either a minus sign (–) is displayed that denotes that an alarm for threshold-exceed is not configured or a check mark is displayed and grayed out that indicates that the TCA for the particular attribute is configured.

9. From the IPLC Optics PMs, IPLC LineOut PMs, or IPLC EDFA PMs dialog boxes, in the 15 Mins column, click the **Chart** button for the performance monitoring parameter set for which you want to view the statistics for the last 15 minutes. This option enables you to view the statistics in a chart form. Performance monitoring information for the different parameters are displayed for the current 15-minute interval. By default, 96 records of 15-minute intervals are displayed.

A 15-Min *parameter-name* tab is displayed beside the TCA Config tab at the top-left corner of the Optics PMs dialog box as shown in [Figure 116 on page 1624](#). A graphical format of the statistics for the specified parameter is displayed on this tab.

Figure 116: 15 Mins Parameter-Name Tab of the IPLC Optics PMs Dialog Box



10. Click the **15 Mins *parameter name*** tab.
 - a. Select one of the following options from the drop-down menu:

- Select **View Chart** or the graphical icon (elliptical curve symbol) to display the chart of performance monitoring statistical metrics. A line graph is displayed with date and time along the horizontal axis and the parameter along the vertical axis. A color-coding format is used to display the different lines, and legends reference the parameter names corresponding to the lines displayed. Mouse over the points in the line graph to expand and show the value of the performance monitoring counters at a particular time.
- Select **View Grid** to switch over to the tabular format of display of performance monitoring statistics.

The records are displayed in tabular format. A serial number of the count of entries, the day, month, and year at which the entry was collected, and the time at which the entry was collected are displayed. The timestamp is the UTC time in the database that is mapped to the local time zone of the client computer.

- Select **Save Chart**, when you view the performance monitoring statistics in graphical format, to save the graph to a Microsoft Excel file, as a .png image. Click the pin icon on the upper-left corner to revert the tab to the original container panel.
- Select **Popout Tab** or the light blue triangle icon to view the dialog box as a separate window.

In the pop-up dialog box, you can do one of the following:

- In the From Date field, pull down the calendar and select the start date of the search. In the To Date field, pull down the calendar and select the end date of the search.
 - Click **Reload** to refresh the contents and display the updated information for the specified time period.
 - Click **Export Data** to transfer the data in graphical or statistical format to a spreadsheet or other business applications for future reference and archival. The comma-separated value (CSV) format takes the raw data from the report and delineates the fields with commas so that the data is imported into popular spreadsheet programs.
 - Click the **View Chart** button at the top-left corner of the dialog box to view the statistics in graphical format. Alternatively, click the **View Grid** button at the top-left corner of the dialog box to view the statistics in tabular format. The View Chart/Grid button is a toggle button.
 - Click **OK** to close the pop-up dialog box. Alternatively, press Esc to close the dialog box after you complete viewing the statistical details.
 - Click **Close** to close the 15-Min *parameter-name* tab.
11. From the IPLC Optics PMs, IPLC LineOut PMs, or IPLC EDFA PMs dialog boxes, in the 24-Hrs column, click the **Chart** button for the performance monitoring parameter set for which you want to view the statistics for the previous day. This option enables you to view the statistics in a chart form. Performance monitoring information for the different parameters are displayed for the current 24-hour interval. By default, records

pertaining to the last 30 days are displayed when you view the performance monitoring counters for the 24-hour duration.

A 24 Hours *parameter-name* tab is displayed beside the TCA Config tab at the top-left corner of the Optics PMs dialog box as shown in [Figure 117 on page 1626](#) and [Figure 118 on page 1627](#). A graphical format of the statistics for the specified parameter is displayed on this tab.

Figure 117: 24 Hours Parameter-Name Tab of the IPLC LineOut Optics PMs Dialog Box

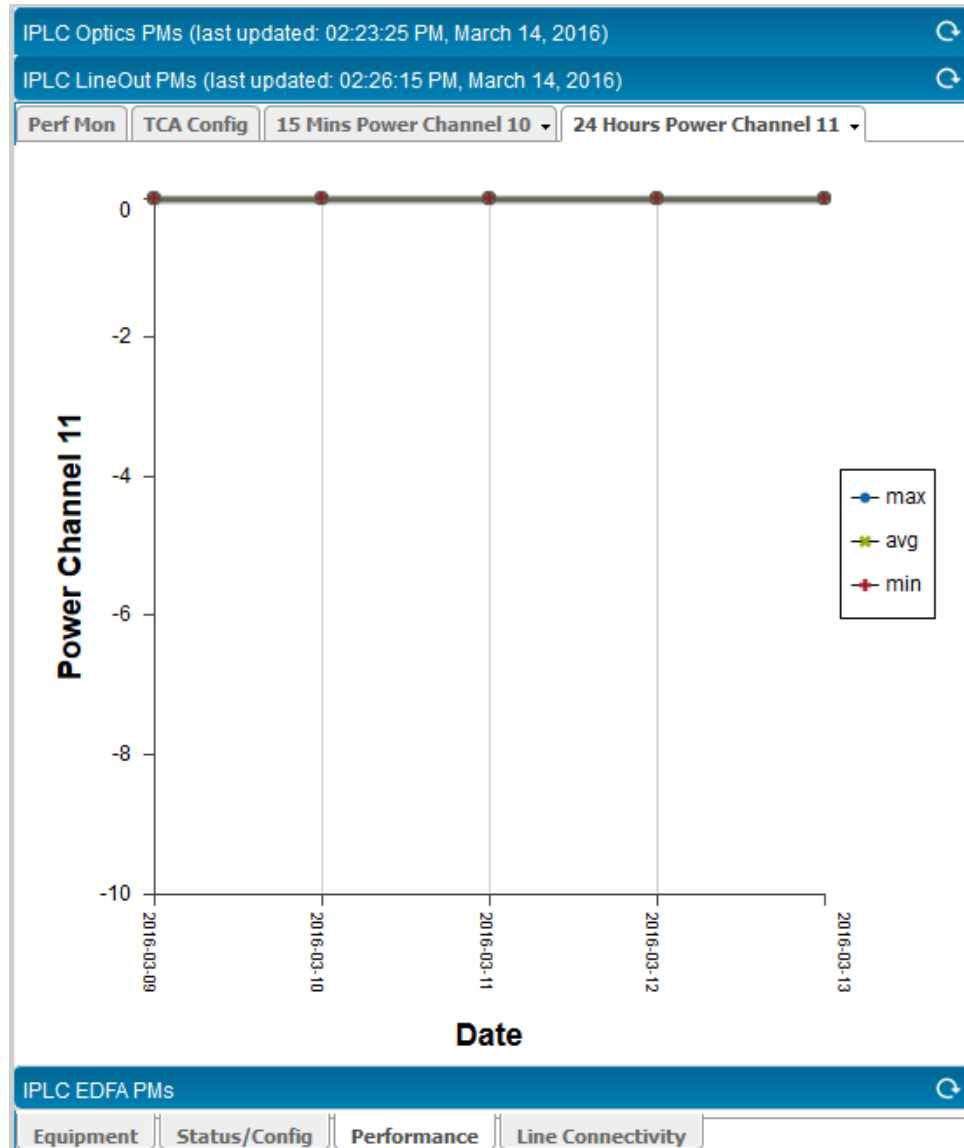
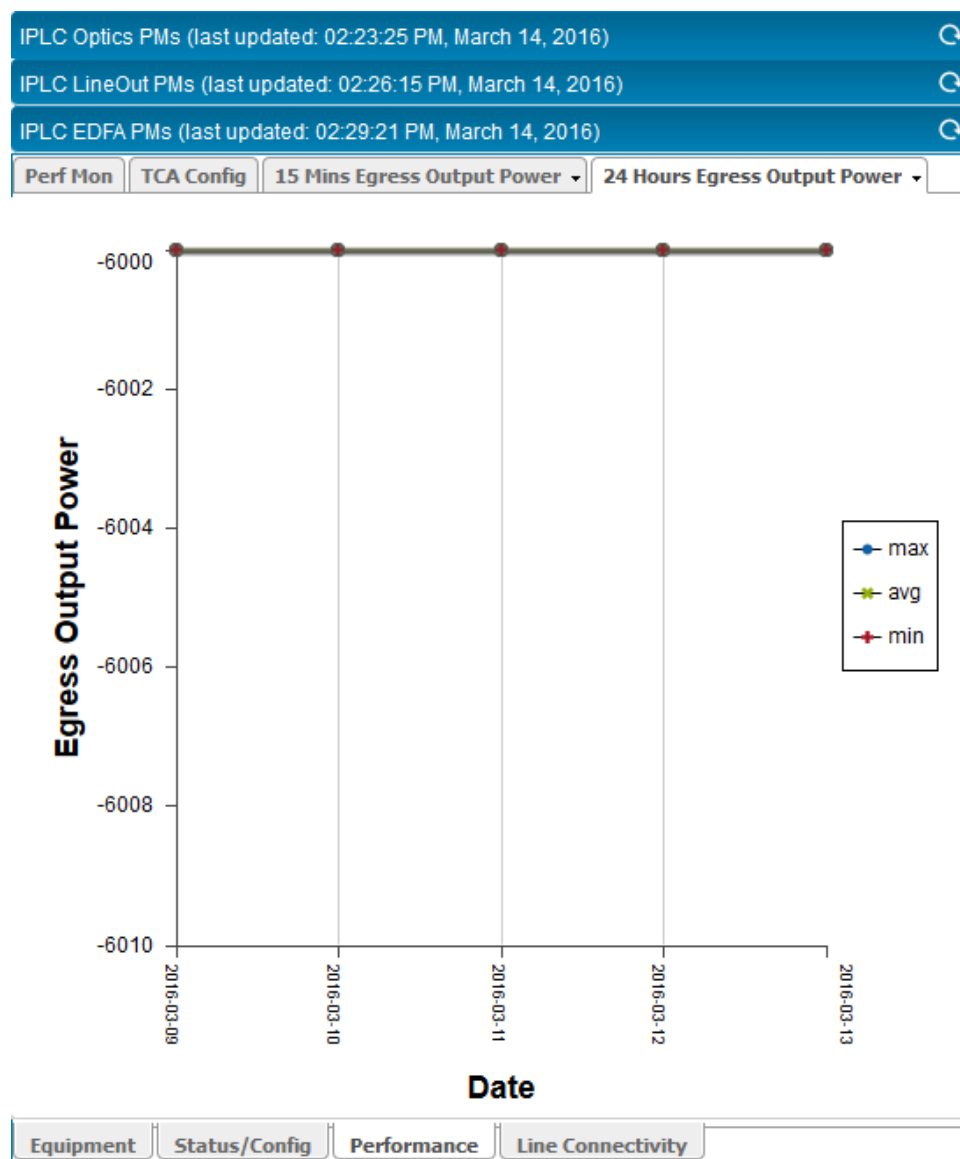


Figure 118: 24 Hours Parameter-Name Tab of the IPLC EDFA Optics PMs Dialog Box



12. Click the **24 Hours parameter name** tab.

- a. Select one of the following options from the drop-down menu:

- Select **View Chart** or the graphical icon (elliptical curve symbol) to display the chart of performance monitoring statistical metrics. A line graph is displayed with date along the horizontal axis and the parameter along the vertical axis. A color-coding format is used to display the different lines, and legends reference the parameter names corresponding to the lines displayed. Mouse over the points in the line graph to expand and show the value of the performance monitoring counters at a particular time.
- Select **View Grid** to switch over to the tabular format of display of performance monitoring statistics.
- Select **Save Chart**, when you view the performance monitoring statistics in graphical format, to save the graph to a Microsoft Excel file, as a .png image. Click the pin icon on the upper-left corner to revert the tab to the original container panel.
- Select **Popout Tab** or the light blue triangle icon to view the dialog box as a separate window.

In the pop-up dialog box, you can do one of the following:

- In the From Date field, pull down the calendar and select the start date of the search. In the To Date field, pull down the calendar and select the end date of the search. Click **Reload** to refresh the contents and display the updated information for the specified time period.
- Click **Export Data** to transfer the data in graphical or statistical format to a spreadsheet or other business applications for future reference and archival. The comma-separated value (CSV) format takes the raw data from the report and delineates the fields with commas so that the data is imported into popular spreadsheet programs.
- Click the **View Chart** button at the top-left corner of the dialog box to view the statistics in graphical format. Alternatively, click the **View Grid** button at the top-left corner of the dialog box to view the statistics in tabular format. The View Chart/Grid button is a toggle button.
- Click **OK** to close the pop-up dialog box. Alternatively, press Esc to close the dialog box after you complete viewing the statistical details.
- Click **Close** to close the 24 Hours *parameter-name* tab.

You can click the **Refresh** (rotating arrow icon) button at the top of the dialog box to enable the latest performance monitoring statistics to be polled and displayed.

**Related
Documentation**

- [Configuring Optical IPLC for Easy and Optimal Deployment on page 1609](#)
- [Configuring Threshold-Crossing Alarms for Optical IPLCs for Monitoring Link Performance on page 1629](#)

Configuring Threshold-Crossing Alarms for Optical IPLCs for Monitoring Link Performance

Threshold crossing alarms (TCAs) can give the management system an early indication as to the state of the associated entity when it crosses a certain threshold. TCAs can be set for both minimum and maximum values for gauges and maximum values for counters. Gauges and counters are the types of metrics for which TCAs are configured. A gauge represents a non-negative integer, which may increase or decrease, but never exceeds a maximum value. A gauge value has its maximum value whenever the information being modeled is greater than or equal to that maximum value. If the TCA parameter subsequently decreases below the maximum value, the gauge value also decreases. A counter represents a non-negative integer that monotonically increases until it reaches a maximum value of 2^{32} (2 raised to the power of 32)-1.

The timely detection of TCAs is essential to proactively manage an interface. TCAs are not an indication of a fault, but rather an indication that the entity maybe close to a fault. You can enable the TCA that you want monitor. You can either keep the default threshold settings or change the settings.

You can enable threshold-crossing alarms (TCAs) on the IPLC for the following:

- Erbium-doped fiber amplifier (EDFA)
- Optical Channel Monitor (OCM)
- Optical Service Channel (OSC)
- Variable Optical Attenuator (VOA)

To configure the TCAs for optical IPLCs:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the PTX300 router for which you want to define the optical IPLC settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. In the image of the device, select an optical IPLC—for example, an optical IPLC installed in a PTX3000 router.


The Component Info dialog box is displayed. The Equipment, Status/Config, Performance, and Line Connectivity tabs are displayed at the bottom of the dialog box.

6. Click the **Performance** tab at the bottom of the pane.



The IPLC Optics PMs dialog box is displayed with the performance monitoring counters and metrics that pertain to the IPLC. This dialog box contains the Perf Mon and TCA Config tabs. Apart from the IPLC Optics PMs pane, which is expanded and displayed, the IPLC LineOut PMs and IPLC EDPA PMs panes are displayed in a collapsed form.





7. Click the **TCA Config** tab to configure the TCAs for the different optical IPLC attributes. The dialog box is refreshed to display the different performance monitoring parameters shown in [Figure 119 on page 1631](#), [Figure 120 on page 1632](#), and [Figure 121 on page 1633](#). These parameters can be edited in an inline form.


Figure 119: TCA Config Tab of the IPLC Optics PMs Dialog Box


IPLC Optics PMs (last updated: 02:34:56 PM, March 14, 2016) 

Perf Mon **TCA Config** 15 Mins Line OUT VOA ▾ 15 Mins OSC Tx Power ▾

 Update  Cancel


PM Type/Group	Threshold-15Min	Threshold-24Hr	Enable
 Optical Line OUT VOA			
Line OUT VOA	--	--	--
Line OUT VOA-Min	0	0	<input type="checkbox"/>
Line OUT VOA-Max	0	0	<input type="checkbox"/>
Line OUT VOA-Avg	--	--	--
 Optical OSC Fiber Loss			
OSC Fiber Loss	--	--	--
OSC Fiber Loss-Min	0	0	<input type="checkbox"/>
OSC Fiber Loss-Max	0	0	<input type="checkbox"/>
OSC Fiber Loss-Avg	--	--	--
 Optical OSC Rx Power			
OSC Rx Power	--	--	--
OSC Rx Power-Min	0	0	<input type="checkbox"/>
OSC Rx Power-Max	0	0	<input type="checkbox"/>
OSC Rx Power-Avg	--	--	--
 Optical OSC Tx Power			
OSC Tx Power	--	--	--
OSC Tx Power-Min	0	0	<input type="checkbox"/>
OSC Tx Power-Max	0	0	<input type="checkbox"/>
OSC Tx Power-Avg	--	--	--


IPLC LineOut PMs (last updated: 02:26:15 PM, March 14, 2016) 

IPLC EDFA PMs (last updated: 02:29:21 PM, March 14, 2016) 



Equipment **Status/Config** **Performance** **Line Connectivity**





Figure 120: TCA Config Tab of the IPLC LineOut PMs Dialog Box


IPLC Optics PMs (last updated: 02:34:56 PM, March 14, 2016) 

IPLC LineOut PMs (last updated: 02:26:15 PM, March 14, 2016) 

Perf Mon | **TCA Config** | 15 Mins Power Channel 10 ▾ | 24 Hours Power Channel 11 ▾


 Update  Cancel


PM Type/Group	Threshold-15Min	Threshold-24Hr	Enable
 Optical Power Channel 0			
Power Channel 0	--	--	--
Power Channel 0-Min	0	0	<input type="checkbox"/>
Power Channel 0-Max	0	0	<input type="checkbox"/>
Power Channel 0-Avg	--	--	--
 Optical Power Channel 1			
Power Channel 1	--	--	--
Power Channel 1-Min	0	0	<input type="checkbox"/>
Power Channel 1-Max	0	0	<input type="checkbox"/>
Power Channel 1-Avg	--	--	--
 Optical Power Channel 10			
Power Channel 10	--	--	--
Power Channel 10-Min	0	0	<input type="checkbox"/>
Power Channel 10-Max	0	0	<input type="checkbox"/>
Power Channel 10-Avg	--	--	--
 Optical Power Channel 11			
Power Channel 11	--	--	--
Power Channel 11-Min	0	0	<input type="checkbox"/>
Power Channel 11-Max	0	0	<input type="checkbox"/>
Power Channel 11-Avg	--	--	--


IPLC EDFA PMs (last updated: 02:29:21 PM, March 14, 2016) 

Equipment | **Status/Config** | **Performance** | **Line Connectivity**



Figure 121: TCA Config Tab of the IPLC EDFA PMs Dialog Box





IPLC Optics PMs (last updated: 02:23:25 PM, March 14, 2016) 

IPLC LineOut PMs (last updated: 02:26:15 PM, March 14, 2016) 

IPLC EDFA PMs (last updated: 02:29:21 PM, March 14, 2016) 

Perf Mon **TCA Config** 15 Mins Egress Output Power ▾ 24 Hours Egress Output Power ▾

 Update  Cancel

PM Type/Group	Threshold-15Min	Threshold-24Hr	Enable
 Optical Egress Input Power			
Egress Input Power	--	--	--
Egress Input Power-Min	0	0	<input type="checkbox"/>
Egress Input Power-Max	0	0	<input type="checkbox"/>
Egress Input Power-Avg	--	--	--
 Optical Egress Output Power			
Egress Output Power	--	--	--
Egress Output Power-Min	0	0	<input type="checkbox"/>
Egress Output Power-Max	0	0	<input type="checkbox"/>
Egress Output Power-Avg	--	--	--
 Optical Egress Pump Current			
Egress Pump Current	--	--	--
Egress Pump Current-Min	0	0	<input type="checkbox"/>
Egress Pump Current-Max	0	0	<input type="checkbox"/>
Egress Pump Current-Avg	--	--	--
 Optical Egress Signal Power			
Egress Signal Power	--	--	--
Egress Signal Power-Min	0	0	<input type="checkbox"/>
Egress Signal Power-Max	0	0	<input type="checkbox"/>
Egress Signal Power-Avg	--	--	--

Equipment **Status/Config** **Performance** **Line Connectivity**

Inline editing enables you to modify previously defined settings easily and quickly. Embedded editing is enabled, which causes the grids showing the devices and interfaces to become modifiable directly; you do not need to highlight, edit, and save the changes every time.

A gray triangle in the upper-right corner of a field denotes that the value of that field or attribute has been modified.

- For the parameters under each performance monitoring category for which you want to modify the TCA value, click the value in the Threshold-15Min or Threshold-24Hr columns to set the TCA value for the 15-minute interval or 24-hour interval. You can

also select or clear the check box in the Enable column to enable or disable the TCA value for the specified parameter, respectively.

9. Click **Update** to save the configured threshold settings. Alternatively, click **Cancel** to discard the configuration.
10. Similarly, you can configure the TCA values for the IPLC line-out and EDFA modules. To configure the TCA settings for the IPLC line-out and EDFA modules, click the **IPLC LineOut PMs** and **IPLC EDFA PMs** headers at the bottom of the IPLC Optics PMs dialog box. The IPLC LineOut PMs and IPLC EDFA PMs panes are expanded and displayed. These panes contain the Performance tab selected.
11. From the IPLC LineOut PMs and IPLC EDFA PMs panes, Click the **TCA Config** tab to configure the TCAs for the different optical IPLC attributes. The dialog box is refreshed to display the different performance monitoring parameters in editable form.
12. Edit the TCA values as necessary for the IPLC line-out and EDFA modules.

**Related
Documentation**

- [Configuring Optical IPLC for Easy and Optimal Deployment on page 1609](#)
- [Viewing Performance Monitoring Details of Optical IPLCs for Detecting and Diagnosing Faults on page 1617](#)

Increasing the Add and Drop Port Capacity of the IPLC Node to 64 Channels

The IPLC base module can accept and multiplex (add) and demultiplex (drop) up to 32 individual wavelengths into a single fiber pair. If you require more than 32 channels, you can increase the IPLC node capacity to 64 channels by connecting the IPLC expansion module to the IPLC base module. This procedure describes how to connect these two modules and configure the IPLC node to support 64 channels.

Before you begin, you must physically connect the IPLC base module and expansion module together as follows:

- Install the IPLC base module and the IPLC expansion module into the PTX3000 chassis.



BEST PRACTICE: We recommend that you place the IPLC modules into the same FPC or PIC slot pair in the PTX3000 chassis.

- Connect the two IPLC modules together as follows:
 - Connect the **XPN IN** port of the IPLC base module to the **XPN OUT** of the IPLC expansion module.
 - Connect the **XPN OUT** port of the IPLC base module to the **XPN IN** of the IPLC expansion module.

This procedure describes how to upgrade an IPLC configuration to 64 channels.

To upgrade an IPLC configuration to 64 channels you must create an association between the between the IPLC base module and the IPLC expansion module:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the PTX300 router for which you want to define the optical IPLC settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. In the image of the device, select an optical IPLC—for example, an optical IPLC installed in a PTX3000 router.

The Component Info dialog box is displayed. At the lower part of the dialog box, the Equipment, Status/Config, Performance, and Line Connectivity tabs are displayed.

6. Click the **Status/Config** tab at the bottom of the dialog box.

The IPLC Line dialog box is displayed on the right pane with the configuration settings that pertain to the IPLC.

7. Specify the FPC or PIC slot in which the IPLC base module resides by selecting the slot in the Chassis View.

For example, if the IPLC base module resides in slot 1, select the **IPLC 1** component in the image of the chassis.

8. Specify the FPC or PIC slot in which the IPLC expansion module resides.

For example, if the IPLC expansion module resides in slot 2, select **FPC 2** from the Expansion IPLC list in the Settings/Status section.

9. Configure the wavelength supported by the OTN transponder and make sure it is supported by the IPLC base module.

For example, to configure the wavelength as 1532.29, select the **Show All Wavelengths** check box, and select **blocked** from the drop-down menu in the **configuration** column of the table for the corresponding wavelength.

10. Click **Update** to save the specified configuration settings.

**Related
Documentation**

- [Configuring a Two-Degree IPLC Node for Express Traffic by Increasing the Line Capacity on page 1636](#)
- [Configuring Optical IPLC Line Connectivity for Interoperation with Optical ILAs on page 1638](#)
- [Configuring the Wavelengths That Are Added and Dropped by the IPLC on page 1645](#)

Configuring a Two-Degree IPLC Node for Express Traffic by Increasing the Line Capacity

For metro linear and metro ring topologies that require either north-south or east-west communications, you can connect two IPLC base modules together to form a two-degree IPLC node. This enables you to run express traffic in two directions. This topic describes how to setup and configure an IPLC two-degree node.

Using the express-in software capability of the IPLC, you can configure the IPLC to accept a wavelength from another IPLC residing in the same chassis. For example, when you have configured an IPLC node using two IPLC base modules. This topic describes how to express-in a wavelength from one IPLC to another IPLC within the same chassis.

Before you begin, complete the following tasks:

- Install and connect the two IPLC base modules through the **PT IN** and **PT OUT** ports. These two IPLC modules form the two-line IPLC node.



BEST PRACTICE: We recommend that you place the IPLC modules into the same FPC or PIC slot pair on the PTX3000 chassis.

To configure the IPLC for two-line terminations to express-in a wavelength from another IPLC:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the PTX300 router for which you want to define the optical IPLC settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. In the image of the device, select an optical IPLC—for example, an optical IPLC installed in a PTX3000 router.

The Component Info dialog box is displayed. At the lower part of the dialog box, the Equipment, Status/Config, Performance, and Line Connectivity tabs are displayed.

6. Click the **Status/Config** tab at the bottom of the dialog box.

The IPLC Line dialog box is displayed on the right pane with the configuration settings that pertain to the IPLC.

7. Specify the FPC or PIC slot in which the IPLC base module resides by selecting the slot in the Chassis View.

For example, if the IPLC base module resides in slot 1, select the **IPLC 1** component in the image of the chassis.

8. Create a logical association between the two IPLC modules and specify that you want the IPLC to express-in a wavelength.

For example, if the other IPLC resides in slot 2, select **IPLC 2** from the Express IPLC list in the Settings/Status section.

9. Configure the wavelength supported by the OTN transponder and make sure it is supported by the IPLC base module.

For example, to configure the wavelength as 1532.29, select the **Show All Wavelengths** check box, and select **express** from the drop-down menu in the **configuration** column of the table for the corresponding wavelength.

10. Click **Update** to save the specified configuration settings.

Related Documentation

- [Increasing the Add and Drop Port Capacity of the IPLC Node to 64 Channels on page 1634](#)
- [Configuring Optical IPLC Line Connectivity for Interoperation with Optical ILAs on page 1638](#)
- [Configuring the Wavelengths That Are Added and Dropped by the IPLC on page 1645](#)

Configuring Optical IPLC Line Connectivity for Interoperation with Optical ILAs

Each optical inline amplifier (ILA) is connected to other optical ILAs or optical integrated photonic line cards (IPLCs) using optical ports or optical supervisory channels (OSCs). There are two optical ports for each optical ILA, designated as OSC A and OSC B. For IP connectivity over OSC, the optical IPLC is used as a gateway. There is no direct IP connectivity between the optical ILA and external servers.

An optical IPLC is a standalone appliance in PTX3000 routers, running Linux. It has host path connectivity to the PTX3000 Routing Engine and other FPCs in the chassis (over internal routing instance). It does not have any router interfaces or switch fabric connectivity; therefore, there is no data path connectivity to other FPC interfaces. The optical IPLC software responds to SNMP commands from the network management server (NMS). SNMP commands are received by the transport daemon (transportd) running on the Routing Engine and are relayed to the optical IPLC CPU running the transport process. For providing IP connectivity, all optical IPLC and optical ILA in the chain are considered to be over a LAN.

Because all communication to an optical ILA is through an optical IPLC, one of the optical IPLCs in the chain is designated as the *anchor IPLC*. All optical ILA commands are directed to the anchor IPLC (which denotes the FPC slot number of the optical IPLC on a specific router) with a parameter indicating the optical ILA identity (OSC management IP address or the serial number). The anchor IPLC maintains a table of IP addresses for all optical ILA OSC-management ports (along with the optical ILA identifier) in the chain. This table is created through the optical IPLC CLI. The IPLC software forwards the commands to the required optical ILA. Each optical ILA in the chain also contains the anchor optical IPLC configuration. This optical ILA is used to send periodic updates and traps.

To configure connectivity between an optical IPLC and an optical ILA on a PTX3000 router:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the PTX300 router for which you want to define the optical IPLC settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. In the image of the device, select an optical IPLC—for example, an optical IPLC installed in a PTX3000 router.

The Component Info dialog box is displayed. The Equipment, Status/Config, Performance, and Line Connectivity tabs are displayed at the bottom of the dialog box.

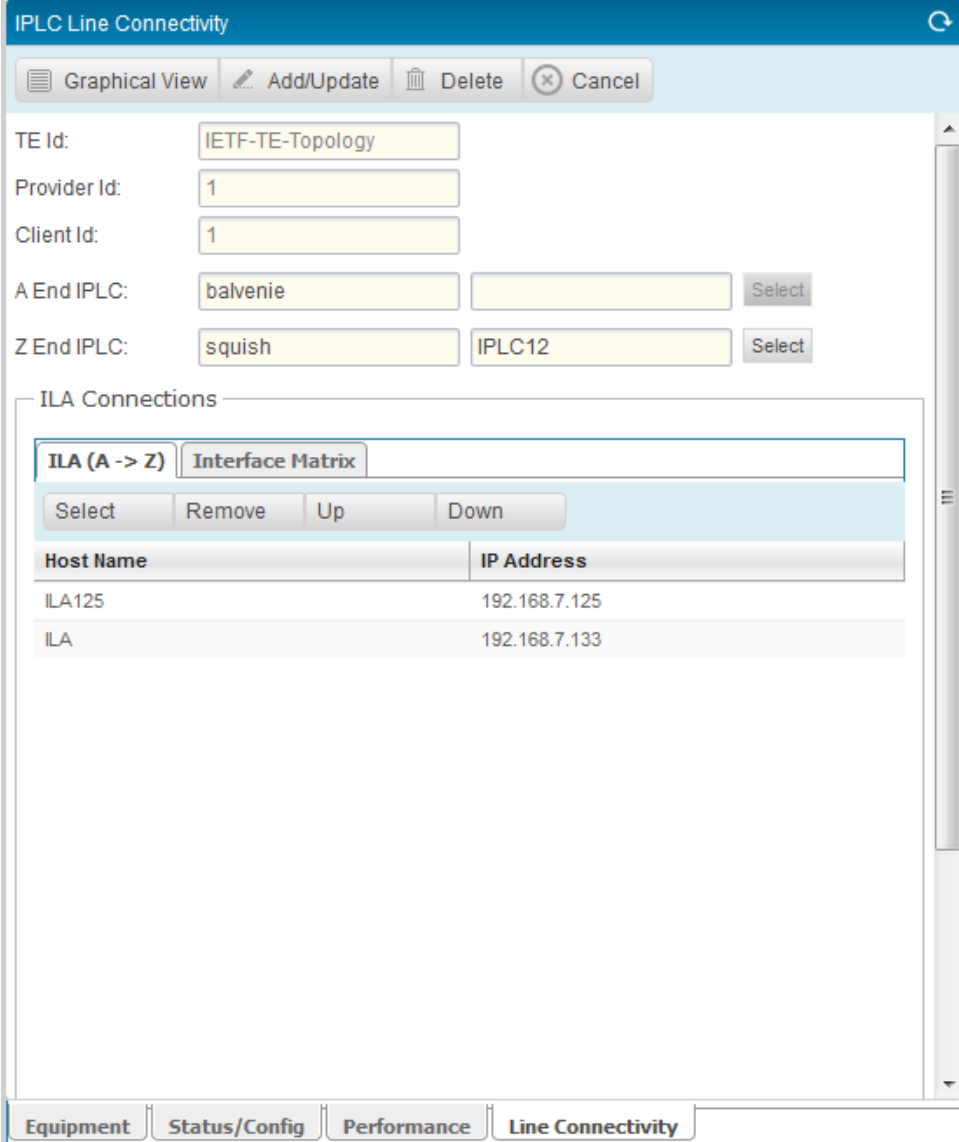
6. Click the **Status/Config** tab at the bottom of the dialog box.

The IPLC Line dialog box is displayed on the right pane with the configuration settings that pertain to the IPLC.

7. Click the **Line Connectivity** tab at the bottom of the dialog box.

The IPLC Line Connectivity dialog box is displayed on the right pane with the configuration settings that can be used to establish a link between the optical IPLC and an optical ILA as shown in [Figure 122 on page 1640](#). You can establish the connectivity between a particular IPLC and optical ILAs that exist on the same PTX3000 router chassis using the fields in this dialog box.

Figure 122: IPLC Line Connectivity Dialog Box



The dialog box is titled "IPLC Line Connectivity" and features a toolbar with "Graphical View", "Add/Update", "Delete", and "Cancel" buttons. Below the toolbar, there are input fields for "TE Id" (pre-filled with "IETF-TE-Topology"), "Provider Id" (pre-filled with "1"), and "Client Id" (pre-filled with "1"). There are also fields for "A End IPLC" (pre-filled with "balvenie") and "Z End IPLC" (pre-filled with "squish"), each followed by a "Select" button. A section titled "ILA Connections" contains two tabs: "ILA (A -> Z)" and "Interface Matrix". Below these tabs are "Select", "Remove", "Up", and "Down" buttons. A table with two columns, "Host Name" and "IP Address", lists two entries: "ILA125" with IP "192.168.7.125" and "ILA" with IP "192.168.7.133". At the bottom, there is a tabbed interface with "Equipment", "Status/Config", "Performance", and "Line Connectivity" tabs, with "Line Connectivity" currently selected.

8. In the TE Id field, enter the traffic engineering (TE) unique identifier that you want to use for the connectivity between the optical IPLC and optical ILA.

By default, this field is prepopulated with the *IETF-TE-Topology* value as the identifier for the topology Information about the IPLC module installed in the FPC or PIC slot. You can modify this value as needed.

9. In the Provider Id field, specify the unique identifier of the provider or the originating module, which is the IPLC in this case.

By default, this field is prepopulated with 1. You can modify this value as needed.

10. In the Client Id field, specify the unique identifier of the client or the receiving module, which is the optical ILA in this case.

By default, this field is prepopulated with 1. You can modify this value as needed.

11. In the A End IPLC field, click **Select** beside the field to select the endpoint or destination IPLC with which the connection must be established.

The Choose IPLC dialog box is displayed. The dialog box contains two panes. The top pane lists all the routers that are present in the network, and the bottom pane lists all the optical IPLCs that reside on the router chassis that you select in the top pane. You can sort and filter the displayed routers by entering a match criterion, such as the router name, in the search field, and click the **Search** icon in both the top and bottom panes. [Table 244 on page 1641](#) describes the fields displayed in the top pane of the Choose IPLC dialog box. [Table 245 on page 1642](#) describes the fields displayed in the bottom pane of the Choose IPLC dialog box.

Table 244: Choose IPLC Dialog Box—Top Pane

Field	Description
Name	Configured name of the device or IP address if no hostname is configured
IP Address	IP Address of the device
State	<p>Connection status of the device in Connectivity Services Director:</p> <ul style="list-style-type: none"> • UP—The device is connected to Connectivity Services Director. • DOWN—The device is not connected to Connectivity Services Director. • N/A—The device state is unavailable to Connectivity Services Director.
Managed State	<p>Configuration status of the device:</p> <ul style="list-style-type: none"> • In Sync—The configuration on the device is in sync with the Connectivity Services Director configuration for the device. • Out Of Sync—The configuration on the device does not match the Connectivity Services Director configuration for the device. This state is usually the result of the device configuration being altered outside of Connectivity Services Director. You cannot deploy the configuration on a device from Connectivity Services Director when the device is out-ofsync. To resolve this state, use the Resynchronize Device Configuration task in Deploy mode. • Sync failed—An attempt to resynchronize an out-of-sync device failed. • Synchronizing—The device configuration is in the process of being resynchronized. • N/A—The device is down.
Platform	Model number of the device, which is PTX3000 in this case
OS Version	Operating system version running on the device

Table 245: Choose IPLC Dialog Box—Bottom Pane

Field	Description
Name	Name of the IPLC with the slot number in which the module resides
Description	Brief description of the hardware item
Serial Number	Serial number of IPLC
Available	Displays whether the device is active or not: <ul style="list-style-type: none"> • true—IPLC is enabled and available • false—IPLC is disabled and unavailable

To select the router and the associated IPLC from the Choose IPLCs dialog box:

- a. Select the check box beside a router in the top pane.

The dialog box refreshes and displays all the corresponding IPLCs for the selected router in the bottom pane.

- b. Select the check box beside an IPLC in the bottom pane, and click **OK**.

You are returned to the IPLC Line Connectivity dialog box. The router name and the IPLC name are displayed in the two text fields, respectively, beside the Z End IPLC field.

In the Z End IPLC field, the PTX3000 router name on which the IPLC for which you are configuring line connectivity resides is displayed in the first field. The IPLC name, which is the same as the one for which you are configuring settings, is displayed in the second field. The **Select** button is displayed beside these text fields.

12. In the ILA Connections section, do the following:

- a. Click the **ILA (A -> Z)** tab.

The table that contains fields to specify the optical ILAs in the connection between the source and destination IPLCs is displayed. The Host Name and IP Address fields are displayed in the ILA (A-> Z) tab, which lists the name of the IPLC and the IP address of the optical supervisory channel (OSC) of the IPLC.

- b. Click **Select** above the table to specify the optical ILAs that must be configured in an ordered fashion as a chain between the source IPLC and the destination IPLC.

The Choose ILA dialog box is displayed, with the list of all the optical ILAs available on the chassis.

- c. Select the check boxes beside the optical ILAs that must be included in the connectivity chain with the IPLC, and click **OK**.

The Choose ILA dialog box closes, and the optical ILAs that you selected are listed in the ILA (A -> Z) tab in the order in which you selected them.

- d. Click a row in the table to select an optical ILA, and then click **Up** or **Down** to move the optical ILAs up or down in the table.

- e. Select an optical ILA from the table, and click **Remove** to delete any ILA that you do not want to participate in the IPLC connectivity chain.

You are not prompted to confirm the deletion. You can readd the optical ILAs as necessary to the connectivity chain.

- f. Click the **Interface Matrix** tab.

The wavelengths configured for the A and Z end interfaces are displayed. The following fields are displayed in a table:

- **Wavelength**—All the available wavelengths supported by the PTX3000 router
- **A End Interfaces**—Optical interface name with the FPC, PIC, and port number of the A end or source interface
- **Z End Interfaces**—Optical interface name with the FPC, PIC, and port number of the Z end or the destination end of the connection. The Z end interface is an optical interface to which the IPLC is connected (for switch mode) or the IPLC expansion module to which the IPLC base module is connected (for express-in mode).

All port wavelength frequencies are controlled by the wavelength selective switch (WSS of the IPLC) and configured on a wavelength-by-wavelength basis. The mapping for the wavelengths, frequencies, and ports is fixed. Each port is assigned a specific frequency and wavelength depending on whether the port is on the IPLC base module or expansion module.

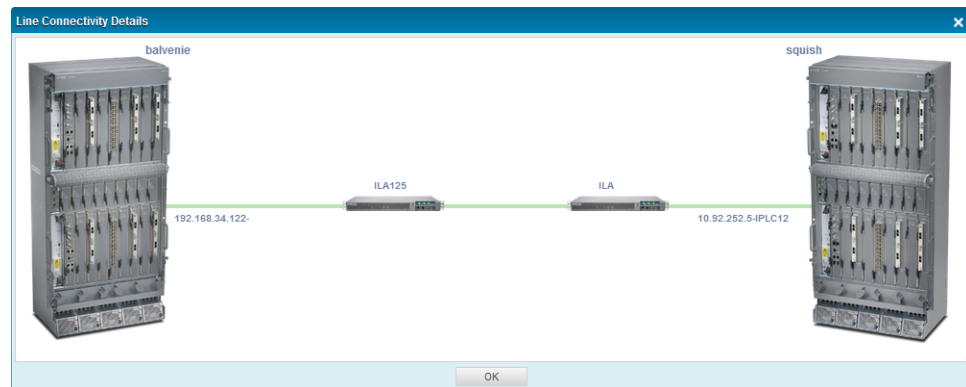
13. Click **Add/Update** at the top of the IPLC Line Connectivity dialog box to save the connection settings between the optical IPLC and optical ILAs that you specified.

A job is created and run to create IPLC line connectivity. The Create IPLC Line Connectivity dialog box is displayed after the job is completed, with the job name, start and end times of the job, job status, and summary. Click **Close** to close the job dialog box.

You can click **Refresh** to update the contents of the dialog box.

14. Click **Graphical View** at the top of the IPLC Line Connectivity dialog box to view the connection between the source IPLC and the destination IPLC through the specified optical ILAs in the chain in a pictorial form as shown in [Figure 123 on page 1644](#).

Figure 123: Line Connectivity Details Dialog Box



The Line Connectivity Details dialog box is displayed, with the source and destination PTX3000 router chassis displayed. Green connector lines are shown to indicate the link between the source and destination routers. IPLC and optical ILA IP addresses are displayed above the green connector lines. Click **OK** when you have completed viewing the graphical representation of the connectivity.

15. (Optional) Click **Delete** at the top of the dialog box to delete the connectivity you created for the IPLC.

A job is created and run to delete IPLC line connectivity. The Delete IPLC Line Connectivity dialog box is displayed after the job is completed, with the job name, start and end times of the job, job status, and summary. Click **Close** to close the job dialog box.

You can click **Refresh** to update the contents of the dialog box.

Alternatively, click **Cancel** if you want to discard the configured IPLC line connectivity settings. You can click the **Refresh** (rotating arrow icon) button at the top of the dialog box to enable the latest settings be retrieved from the device and displayed.

Related Documentation

- [Increasing the Add and Drop Port Capacity of the IPLC Node to 64 Channels on page 1634](#)
- [Configuring a Two-Degree IPLC Node for Express Traffic by Increasing the Line Capacity on page 1636](#)
- [Configuring the Wavelengths That Are Added and Dropped by the IPLC on page 1645](#)

Configuring the Wavelengths That Are Added and Dropped by the IPLC

By default, wavelengths on the IPLC ports are in blocked mode. You must configure the IPLC to add or drop a specific wavelength. This topic describes the default wavelength mapping for the IPLC ports and how to configure the IPLC to add or drop a specific wavelength.

All port wavelength frequencies are controlled by the IPLC's wavelength selective switch (WSS) and configured on a wavelength-by-wavelength basis.



NOTE: IPLC ports can also be switched-in to an optical interface on the same chassis or a remote chassis, or you can express-in a wavelength to a different IPLC.

Table 229 on page 1473 lists the default port, frequency, and wavelength mapping for both of the IPLC modules. The wavelength you want to support must be listed in Table 229 on page 1473.

Table 246: IPLC Port, Frequency, and Wavelength Mapping

Frequency [THz]	Central Wavelength [nm]	Present on IPLC Module	Label on IPLC Module	Present on IPLC Expansion Module	Label on IPLC Expansion Module
192.05	1561.01	Yes	0	No	No
192.1	1560.61	No	No	Yes	32
192.15	1560.2	Yes	1	No	No
192.2	1559.79	No	No	Yes	33
192.25	1559.39	Yes	2	No	No
192.3	1558.98	No	No	Yes	34
192.35	1558.58	Yes	3	No	No
192.4	1558.17	No	No	Yes	35
192.45	1557.77	Yes	4	No	No
192.5	1557.36	No	No	Yes	36
192.55	1556.96	Yes	5	No	No
192.6	1556.55	No	No	Yes	37
192.65	1556.15	Yes	6	No	No

Table 246: IPLC Port, Frequency, and Wavelength Mapping (continued)

Frequency [THz]	Central Wavelength [nm]	Present on IPLC Module	Label on IPLC Module	Present on IPLC Expansion Module	Label on IPLC Expansion Module
192.7	1555.75	No	No	Yes	38
192.75	1555.34	Yes	7	No	No
192.8	1554.94	No	No	Yes	39
192.85	1554.54	Yes	8	No	No
192.9	1554.13	No	No	Yes	40
192.95	1553.73	Yes	9	No	No
193	1553.33	No	No	Yes	41
193.05	1552.93	Yes	10	No	No
193.1	1552.52	No	No	Yes	42
193.15	1552.12	Yes	11	No	No
193.2	1551.72	No	No	Yes	43
193.25	1551.32	Yes	12	No	No
193.3	1550.92	No	No	Yes	44
193.35	1550.52	Yes	13	No	No
193.4	1550.12	No	No	Yes	45
193.45	1549.72	Yes	14	No	No
193.5	1549.32	No	No	Yes	46
193.55	1548.91	Yes	15	No	No
193.6	1548.51	No	No	Yes	47
193.65	1548.11	Yes	16	No	No
193.7	1547.72	No	No	Yes	48
193.75	1547.32	Yes	17	No	No
193.8	1546.92	No	No	Yes	49

Table 246: IPLC Port, Frequency, and Wavelength Mapping (continued)

Frequency [THz]	Central Wavelength [nm]	Present on IPLC Module	Label on IPLC Module	Present on IPLC Expansion Module	Label on IPLC Expansion Module
193.85	1546.52	Yes	18		
193.9	1546.12	No	No	Yes	50
193.95	1545.72	Yes	19	No	No
194	1545.32	No	No	Yes	51
194.05	1544.92	Yes	20	No	No
194.1	1544.53	No	No	Yes	52
194.15	1544.13	Yes	21	No	No
194.2	1543.73	No	No	Yes	53
194.25	1543.33	Yes	22	No	No
194.3	1542.94	No	No	Yes	54
194.35	1542.54	Yes	23	No	No
194.4	1542.14	No	No	Yes	55
194.45	1541.75	Yes	24	No	No
194.5	1541.35	No	No	Yes	56
194.55	1540.95	Yes	25	No	No
194.6	1540.56	No	No	Yes	57
194.65	1540.16	Yes	26	No	No
194.7	1539.77	No	No	Yes	58
194.75	1539.37	Yes	27	No	No
194.8	1538.98	No	No	Yes	59
194.85	1538.58	Yes	28	No	No
194.9	1538.19	No	No	Yes	60
194.95	1537.79	Yes	29	No	No

Table 246: IPLC Port, Frequency, and Wavelength Mapping (continued)

Frequency [THz]	Central Wavelength [nm]	Present on IPLC Module	Label on IPLC Module	Present on IPLC Expansion Module	Label on IPLC Expansion Module
195.00	1537.40	No	No	Yes	61
195.05	1537.00	Yes	30	No	No
195.10	1536.61	No	No	Yes	62
195.15	1536.22	Yes	31	No	No
195.20	1535.82	No	No	Yes	63

You can configure the IPLC to switch a particular wavelength to an optical interface on a remote chassis.

Before you start this procedure, make sure that you configure the wavelength on the remote optical interface so that the wavelength is compatible with the wavelength you are switching on the IPLC.

To configure an IPLC port to add or drop a specific wavelength:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the PTX300 router for which you want to define the optical IPLC settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. In the image of the device, select an optical IPLC—for example, an optical IPLC installed in a PTX3000 router.

The Component Info dialog box is displayed. At the lower part of the dialog box, the Equipment, Status/Config, Performance, and Line Connectivity tabs are displayed.

6. Click the **Status/Config** tab at the bottom of the dialog box.

The IPLC Line dialog box is displayed on the right pane with the configuration settings that pertain to the IPLC.

7. Specify the FPC or PIC slot in which the IPLC base module resides by selecting the slot in the Chassis View.

For example, if the IPLC base module resides in slot 1, select the **IPLC 1** component in the image of the chassis.

8. Specify the wavelength number for the IPLC. For example, for wavelength 1550.12, select the **Show All Wavelengths** check box, beside the **1550.12** row in the **wavelength** column, modify the values in the **configuration** and **end-point** columns as necessary for this wavelength.

9. Click **Update** to save the specified configuration settings.

Related Documentation

- [Increasing the Add and Drop Port Capacity of the IPLC Node to 64 Channels on page 1634](#)
- [Configuring a Two-Degree IPLC Node for Express Traffic by Increasing the Line Capacity on page 1636](#)
- [Configuring Optical IPLC Line Connectivity for Interoperation with Optical ILAs on page 1638](#)

Configuring the IPLC to Add or Drop Wavelengths to an Optical Interface on a Remote Chassis

The IPLC is designed to connect the **ADD** and **DROP** ports on the front panel to compatible optical PICs or MICs on the local or remote chassis. Wavelengths configured on the local IPLC **ADD** ports are multiplexed and sent over the **Line OUT** port of the IPLC base module. The remote IPLC base module receives the signal on the **Line IN** port and demultiplexes the wavelengths to the **DROP** ports on the front panel of the IPLC according to the configuration of the remote IPLC. After you have made the physical connections between the IPLC ports and the local and remote optical interfaces, you need to configure the IPLC to switch the wavelengths to the optical interfaces. This topic describes how to configure the IPLC to switch the wavelengths on the **ADD** and **DROP** ports to compatible optical interfaces on the local chassis or a remote chassis.

You can configure the IPLC to switch a particular wavelength to an optical interface on a remote chassis.

Before you begin, complete the following tasks:

- Install the optical interfaces and configure the wavelength on the local optical interface so that it is compatible with the wavelength on the IPLC. See, [Configuring the 10-Gigabit or 100-Gigabit Ethernet DWDM Interface Wavelength](#)
- Install the IPLC module at the remote location and connect the **ADD** and **DROP** ports to the respective local optical interfaces.

To configure the IPLC base module to switch a wavelength to an optical interface on a remote chassis:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the PTX300 router for which you want to define the optical IPLC settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. In the image of the device, select an optical IPLC—for example, an optical IPLC installed in a PTX3000 router.

The Component Info dialog box is displayed. At the lower part of the dialog box, the Equipment, Status/Config, Performance, and Line Connectivity tabs are displayed.

6. Click the **Status/Config** tab at the bottom of the dialog box.

The IPLC Line dialog box is displayed on the right pane with the configuration settings that pertain to the IPLC.

7. Specify the FPC or PIC slot in which the IPLC base module resides by selecting the slot in the Chassis View.

For example, if the IPLC base module resides in slot 1, select the **IPLC 1** component in the image of the chassis.

8. Specify the wavelength number and that you want to switch it to the remote chassis. For example, if you want to switch wavelength 1550.12 on the IPLC in slot 1 to the remote chassis, in the Wavelength Configuration section, select the **Show All Wavelengths** check box, and beside the 1550.12 row in the **wavelength** column, select **switch** from the drop-down menu in the **configuration** column of the table for the corresponding wavelength.

9. From the **end-point** column, click in the cell corresponding to the wavelength of 1550.12, and then click the drop-down arrow.

From the drop-down menu, select **remote** to specify the remote chassis to which you want the wavelength of the IPLC base module to be switched.

10. Click **Update** to save the specified configuration settings.

**Related
Documentation**

- [Configuring the IPLC to Add or Drop Wavelengths to an Optical Interface on the Same Chassis on page 1651](#)
- [Bypassing a Wavelength on the IPLC on page 1652](#)

Configuring the IPLC to Add or Drop Wavelengths to an Optical Interface on the Same Chassis

This topic provides a procedure for switching a wavelength present on the local IPLC modules to an optical interface on the same chassis.

Before you begin, complete the following tasks:

- Install the optical interfaces and configure the wavelength on the local optical interface so that it is compatible with the wavelength on the IPLC. See, [Configuring the 10-Gigabit or 100-Gigabit Ethernet DWDM Interface Wavelength](#)
- Install the IPLC module and connect the **ADD** and **DROP** ports to the respective local optical interfaces.

To configure the IPLC base module to switch a wavelength to an optical interface on the same chassis:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the PTX300 router for which you want to define the optical IPLC settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. In the image of the device, select an optical IPLC—for example, an optical IPLC installed in a PTX3000 router.

The Component Info dialog box is displayed. At the lower part of the dialog box, the Equipment, Status/Config, Performance, and Line Connectivity tabs are displayed.

6. Click the **Status/Config** tab at the bottom of the dialog box.

The IPLC Line dialog box is displayed on the right pane with the configuration settings that pertain to the IPLC.

7. Specify the FPC or PIC slot in which the IPLC base module resides by selecting the slot in the Chassis View.

For example, if the IPLC base module resides in slot 1, select the **IPLC 1** component in the image of the chassis.

8. Specify the wavelength you want to switch and the name of the physical optical interface to which you want to switch it. For example, if you want to switch wavelength 1550.12 on the IPLC in slot 1 to the optical interface on FPC slot 3, PIC 0, port 0, in the Wavelength Configuration section, select the **Show All Wavelengths** check box, and beside the 1550.12 row in the **wavelength** column, select **switch** from the drop-down menu in the **configuration** column of the table for the corresponding wavelength.

9. From the **end-point** column, click in the cell corresponding to the wavelength of 1550.12, and then click the drop-down arrow.

From the drop-down menu, select **et-3/0/0** to which you want the wavelength of the IPLC base module to be switched.

10. Click **Update** to save the specified configuration settings.

Related Documentation

- [Configuring the IPLC to Add or Drop Wavelengths to an Optical Interface on a Remote Chassis on page 1649](#)
- [Bypassing a Wavelength on the IPLC on page 1652](#)

Bypassing a Wavelength on the IPLC

The IPLC enables you to optically bypass a wavelength by entering a few simple configuration statements. Bypassing a wavelength does not terminate the wavelength at the local IPLC but instead passes the wavelength on to the next downstream IPLC node. This topic describes how to bypass a wavelength on the IPLC.

Optical bypasses are software configurable and controlled through the IPLC's wavelength selective switch (WSS) so there is no need to manual intervention. The IPLCs software optical bypass enables wavelengths that do not terminate on the given node to be passed-through to the remote node without optical-electrical-optical (OEO) conversion.

Before you begin, configure the IPLC two-degree intermediate node for express traffic.

To configure the IPLC to bypass a wavelength:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the PTX300 router for which you want to define the optical IPLC settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. In the image of the device, select an optical IPLC—for example, an optical IPLC installed in a PTX3000 router.

The Component Info dialog box is displayed. At the lower part of the dialog box, the Equipment, Status/Config, Performance, and Line Connectivity tabs are displayed.

6. Click the **Status/Config** tab at the bottom of the dialog box.

The IPLC Line dialog box is displayed on the right pane with the configuration settings that pertain to the IPLC.

7. Specify the FPC or PIC slot in which the IPLC base module resides by selecting the slot in the Chassis View.

For example, if the IPLC base module resides in slot 1, select the **IPLC 1** component in the image of the chassis.

8. Configure the wavelength that you want to bypass from the IPLC base module to another IPLC module

For example, to bypass the wavelength of 1532.29, select the **Show All Wavelengths** check box, and select **express** from the drop-down menu in the **configuration** column of the table for the corresponding wavelength.

9. Create a logical association between the two IPLC modules and specify that you want the IPLC to express-in a wavelength.

For example, if the other IPLC resides in slot 2, select **IPLC 2** from the Express IPLC list in the Settings/Status section.

10. Click **Update** to save the specified configuration settings.

**Related
Documentation**

- [Configuring the IPLC to Add or Drop Wavelengths to an Optical Interface on a Remote Chassis on page 1649](#)
- [Configuring the IPLC to Add or Drop Wavelengths to an Optical Interface on the Same Chassis on page 1651](#)

Changing Alarm Settings for the Optical IPLCs

You can modify the configuration settings for alarm settings of optical integrated photonic line cards (IPLCs), which are used in conjunction with optical inline amplifiers (ILAs) on PTX3000 Packet Transport Routers, using the Preferences page of the Connectivity Services Director application. To open the Preferences page, click the down arrow next to the System button in the Connectivity Services Director banner and select Preferences. The Preferences page opens with User Preferences as the default tab. Click the Fault tab of the Preferences page of the Connectivity Services Director GUI to enable individual alarms, set the retention period for alarms, configure alarm notifications, configure threshold alarms, and to specify the number of events to keep for each alarm. The Fault tab has multiple sections, which you can expand and collapse by clicking the arrow next to the section title:

- Global Settings, for configuring Faults settings such as global alarm notifications and alarm data retention.
- Individual Alarms and Threshold Settings, for configuring settings for individual alarms and threshold alarms.
- [Alarms for Optical IPLCs on page 1655](#)
- [Configuring Global Alarm Notifications on page 1659](#)
- [Retaining Alarm History on page 1659](#)
- [Specifying Event History on page 1659](#)
- [Enabling Alarms on page 1659](#)
- [Changing the Severity of Individual Alarms on page 1659](#)
- [Configuring Threshold Alarms on page 1660](#)
- [Configuring Individual Alarm Notifications on page 1660](#)

Alarms for Optical IPLCs

The following alarms are applicable for management of the optical IPLC:

Alarm Name	Description
jnxlplcFpcAwgAddLosAlarm	Generated as the FPC arrayed waveguide gratings (AWG) add LOS alarm for the IPLC
jnxlplcFpcExpInLosAlarm	Generated as the FPC input LOS alarm for the express-in mode of the IPLC.
jnxlplcFpcOscAddLosAlarm	Generated as the FPC add LOS alarm for the optical service channel (OSC) of the IPLC. The OSC is an in-band channel used to communicate with ILAs and other optical nodes in the line system that are not directly accessible over the DCN. OSC framing logic is implemented in the FPGA.
jnxlplcFpcOscDrpLosAlarm	Generated as the FPC drop LOS alarm for the OSC of the IPLC.
jnxlplcFpcLineInLosAlarm	Generated as the FPC input line-in LOS alarm for the IPLC.
jnxlplcFpcEdfa1RefPwAlarm	Generated as the FPC erbium doped fiber amplifier (EDFA) 1 reflect power alarm for the IPLC. EDFA1 is considered as ingress EDFA and EDFA2 is considered as egress EDFA
jnxlplcFpcEdfa1OutPwAlarm	Generated as the FPC EDFA1 output power alarm for the IPLC.
jnxlplcFpcEdfa1OutGain	Generated as the FPC EDFA1 output gain alarm for the IPLC
jnxlplcFpcEdfa1PumpEolAlarm	Generated as the FPC EDFA1 pump end-of-life (EoL) alarm for the IPLC.
jnxlplcFpcEdfa1TempAlarm	Generated as the FPC EDFA1 temperature alarm for the IPLC.
jnxlplcFpcEdfa1OutLosAlarm	Generated as the FPC EDFA1 output LOS alarm for the IPLC.
jnxlplcFpcEdfa1InLosAlarm	Generated as the FPC EDFA1 input LOS alarm for the IPLC.
jnxlplcFpcEdfa2RefPwAlarm	Generated as the FPC erbium doped fiber amplifier (EDFA) 2 reflect power alarm for the IPLC. EDFA1 is considered as ingress EDFA and EDFA2 is considered as egress EDFA
jnxlplcFpcEdfa2OutPwAlarm	Generated as the FPC EDFA2 output power alarm for the IPLC.
jnxlplcFpcEdfa2OutGainAlarm	Generated as the FPC EDFA2 output gain alarm for the IPLC
jnxlplcFpcEdfa2PumpEolAlarm	Generated as the FPC EDFA2 pump end-of-life (EoL) alarm for the IPLC.
jnxlplcFpcEdfa2TempAlarm	Generated as the FPC EDFA2 temperature alarm for the IPLC.
jnxlplcFpcEdfa2OutLosAlarm	Generated as the FPC EDFA2 output LOS alarm for the IPLC.
jnxlplcFpcEdfa2InLosAlarm	Generated as the FPC EDFA2 input LOS alarm for the IPLC.

Alarm Name	Description
jnxlplcFpcWssTempAlarm	Generated as the FPC wavelength selective switching (WSS) temperature alarm for the IPLC.
jnxlplcFpcWssVoltAlarm	Generated as the FPC WSS voltage alarm for the IPLC.
jnxlplcFpcInterDiagAlarm	Generated as the FPC internal diagnostic alarm for the IPLC.
jnxlplcFpcFwCnsistAlarm	Generated as the FPC firmware consistency alarm for the IPLC.
jnxlplcFpcHwFailAlarm	Generated as the FPC hardware failure alarm for the IPLC.
jnxlplcFpcFwFailAlarm	Generated as the FPC firmware failure alarm for the IPLC.
jnxlplcFpcOcmFailAlarm	Generated as the FPC optical channel monitor (OCM) failure alarm for the IPLC.
jnxlplcFpcWssFailAlarm	Generated as the FPC WSS failure alarm for the IPLC.
jnxlplcFpcEdfa2FailAlarm	Generated as the FPC EDFA2 failure alarm for the IPLC.
jnxlplcFpcEdfa1FailAlarm	Generated as the FPC EDFA1 alarm for the IPLC.
jnxlplcFpcPwrFailAlarm	Generated as the FPC power rail failure alarm for the IPLC.
jnxlplcOscTxPowerHigh15minAlert	Generated as an alarm when the OSC transmitted high power exceeds the threshold within the 15-minute interval for the IPLC.
jnxlplcOscTxPowerLow15minAlert	Generated as an alarm when the OSC transmitted low power exceeds the threshold within the 15-minute interval for the IPLC.
jnxlplcOscRxPowerHigh15minAlert	Generated as an alarm when the OSC received high power exceeds the threshold within the 15-minute interval for the IPLC.
jnxlplcOscRxPowerLow15minAlert	Generated as an alarm when the OSC received low power exceeds the threshold within the 15-minute interval for the IPLC.
jnxlplcOscFiberLosHigh15minAlert	Generated as an alarm when the OSC fiber high LOS exceeds the threshold within the 15-minute interval for the IPLC.
jnxlplcOscFiberLosLow15minAlert	Generated as an alarm when the OSC fiber low LOS exceeds the threshold within the 15-minute interval for the IPLC.
jnxlplcLineOutVoaHigh15minAlert	Generated as the line-out Variable Optical Attenuator (VOA) high threshold setting trigger within the 15-minute period for the IPLC.
jnxlplcLineOutVoaLow15minAlert	Generated as the line-out Variable Optical Attenuator (VOA) low threshold setting trigger within the 15-minute period for the IPLC.
jnxlplcIngressEdfaInputPwHigh15minAlert	Generated as the ingress EDFA input power high threshold setting trigger within the 15-minute period for the IPLC.

Alarm Name	Description
jnxlplcIngressEdfaInputPwLow15minAlert	Generated as the ingress EDFA input power low threshold setting trigger within the 15-minute period for the IPLC.
jnxlplcOcmPwHigh15minAlert	Generated as the OCM module power high threshold setting trigger within the 15-minute period for the IPLC.
jnxlplcOcmPwLow15minAlert	Generated as the OCM module power low threshold setting trigger within the 15-minute period for the IPLC.
jnxlplcOscTxPowerHigh24hourAlert	Generated as the OSC transmitted high power threshold setting trigger within the 15-minute period for the IPLC.
jnxlplcOscTxPowerLow24hourAlert	Generated as the OSC transmitted high power threshold setting trigger within the 15-minute period for the IPLC.
jnxlplcOscRxPowerHigh24hourAlert	Generated as an alarm when the OSC received high power exceeds the threshold within the 24-hour interval for the IPLC.
jnxlplcOscRxPowerLow24hourAlert	Generated as an alarm when the OSC received low power exceeds the threshold within the 24-hour interval for the IPLC.
jnxlplcOscFiberLosHigh24hourAlert	Generated as an alarm when the OSC fiber high LOS exceeds the threshold within the 24-hour interval for the IPLC.
jnxlplcOscFiberLosLow24hourAlert	Generated as an alarm when the OSC fiber low LOS exceeds the threshold within the 24-hour interval for the IPLC.
jnxlplcLineOutVoaHigh24hourAlert	Generated as the line-out Variable Optical Attenuator (VOA) high threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcLineOutVoaLow24hourAlert	Generated as the line-out Variable Optical Attenuator (VOA) low threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcIngressEdfaInputPwHigh24hourAlert	Generated as the ingress EDFA input high power threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcIngressEdfaInputPwLow24hourAlert	Generated as the ingress EDFA input low power threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcIngressEdfaOutputPwHigh24hourAlert	Generated as the ingress EDFA output high power threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcIngressEdfaOutputPwLow24hourAlert	Generated as the ingress EDFA output low power threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcIngressEdfaSignalPwHigh24hourAlert	Generated as the ingress EDFA signal high power threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcIngressEdfaSignalPwLow24hourAlert	Generated as the ingress EDFA signal low power threshold setting trigger within the 24-hour period for the IPLC.

Alarm Name	Description
jnxlplcIngressEdfaPumpCurrentHigh24hourAlert	Generated as the ingress EDFA pump current high temperature threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcIngressEdfaPumpCurrentLow24hourAlert	Generated as the ingress EDFA pump current low temperature threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcEgressEdfaInputPwHigh24hourAlert	Generated as the egress EDFA input high power threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcEgressEdfaInputPwLow24hourAlert	Generated as the egress EDFA input low power threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcEgressEdfaOutputPwHigh24hourAlert	Generated as the egress EDFA output high power threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcEgressEdfaOutputPwLow24hourAlert	Generated as the egress EDFA output low power threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcEgressEdfaSignalPwHigh24hourAlert	Generated as the egress EDFA signal high power threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcEgressEdfaSignalPwLow24hourAlert	Generated as the egress EDFA signal low power threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcEgressEdfaPumpCurrentHigh24hourAlert	Generated as the egress EDFA pump current high temperature threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcEgressEdfaPumpCurrentLow24hourAlert	Generated as the egress EDFA pump current low temperature threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcPowerMonitorAwgAddHigh24hourAlert	Generated as the power monitor AWG add high threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcPowerMonitorAwgAddLow24hourAlert	Generated as the power monitor AWG add low threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcPowerMonitorExpressInHigh24hourAlert	Generated as the power monitor express-in mode high threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcPowerMonitorExpressInLow24hourAlert	Generated as the power monitor express-in mode low threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcOcmPwHigh24hourAlert	Generated as the OCM module power high threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcOcmPwLow24hourAlert	Generated as the OCM module power low threshold setting trigger within the 24-hour period for the IPLC.
jnxlplcFpcSfpLosAlarm	Generated as the FPC SFP loss of signal (LOS) alarm for the IPLC.
jnxlplcFpcSfpLofAlarm	Generated as the FPC SFP loss of frame (LOF) alarm for the IPLC.

Configuring Global Alarm Notifications

You can configure global e-mail notifications to be sent when any alarm with notifications enabled is generated. To configure global e-mail notifications, enter the e-mail addresses to receive global alarm notifications in the Alarm Notifications Destinations field in the Global Settings section. Separate addresses with a comma (,). For information about enabling notification for an alarm, see [“Configuring Individual Alarm Notifications” on page 152](#).

Retaining Alarm History

Use the **No. of days to keep Alarm** field in the Global Settings section to specify the number of days to keep alarm history. The default retention time is 120 days; but you can specify a period of 7 through 1000 days. Specifying a longer retention time consumes more database resources. To change the alarm retention duration, type a new value and click **OK** and **Yes** to confirm the change.

Specifying Event History

Use the **Events/Alarm** field in the Global Settings section to specify the number of event entries that are kept in the alarm history. The default setting for events is 20. To change the setting, type a new value and click **OK** and **Yes** to confirm the change.

Enabling Alarms

Ensure all devices are configured to send traps to Connectivity Services Director. This task is performed for the devices in Deploy mode through Set SNMP Trap Configuration.

Use the Individual Alarms and Threshold Settings section to disable and re-enable individual alarms or all alarms. Alarms appear on both tabs in the section: Alarm Settings and Threshold Settings. Fault alarms are preconfigured and initially enabled. To enable or disable alarms:

1. (Optional) Sort the alarms. By default, the list of alarms is sorted alphabetically within each category. You can also sort by description or alarm severity within a category by clicking a column heading.
2. Review the alarms and either select the check box in the heading to select all of the alarms or select the check box for the individual alarms you want to enable.
3. Click **OK** and **Yes** to confirm the alarm change.

Changing the Severity of Individual Alarms

You can change the severity of the alarms to match your corporate procedures and guidelines. For example, at your company a DoS attack might be considered a critical alarm, while Connectivity Services Director has a default severity for DoS attacks as a major alarm. Alarms appear on both tabs in the Individual Alarms and Threshold Settings section: Alarm Settings and Threshold Settings.

To change the severity of an alarm:

1. Select the current severity in the **Severity** column. A list of the severity levels appear.
2. Select the new severity level for the alarm.
3. Click **OK** and **Yes** to confirm the change to the severity setting.

To configure alarm notifications, see [“Configuring Individual Alarm Notifications” on page 152](#).

Configuring Threshold Alarms

Threshold alarms are alarms that are generated when a monitored value crosses the configured threshold. They provide enhanced visibility into potential issues on the network. You configure and manage threshold alarms the same way as other alarms. You also have the option of setting the threshold level of individual threshold alarms.

To set threshold alarm thresholds:

1. Select the **Threshold Settings** tab in the Individual Alarms and Threshold settings section of the Fault tab.
2. Click **Edit Settings** in the Threshold Settings column of the alarm threshold you want to edit.
3. Set the threshold in the window that opens.
4. Click **Save** to save the new threshold.

To configure alarm notifications, see [“Configuring Individual Alarm Notifications” on page 152](#).

Configuring Individual Alarm Notifications

You can configure e-mail notifications to be sent when an individual alarm is generated. When you enable notification for an alarm, the notifications are sent to the e-mail addresses configured for the alarm and the addresses configured for global alarm notifications. Alarms appear on both tabs in the Individual Alarms and Threshold Settings section: Alarm Settings and Threshold Settings.

To configure e-mail notification for an alarm name:

1. Select the check box in the alarm's Notification column.
If you later want to disable notification for the alarm, clear the check box.
2. Click **Edit Notification** in the Notification column. The Alarm Notification Details window opens.

3. Enter one or more e-mail addresses in the Notification Email Addresses field. Separate addresses with a comma (,).

You can later edit the addresses to send notifications to different addresses.

4. (Optional) Enter a comment in the Comments field. This comment is included in the e-mail notification message.

5. Click **Save**.

Related Documentation

- [Configuring the IPLC to Add or Drop Wavelengths to an Optical Interface on a Remote Chassis on page 1649](#)
- [Configuring the IPLC to Add or Drop Wavelengths to an Optical Interface on the Same Chassis on page 1651](#)
- [Bypassing a Wavelength on the IPLC on page 1652](#)

Viewing Routing Engine Switchover Indicators in the Chassis Image

Redundant Routing Engines are two Routing Engines that are installed in the same routing platform. One functions as the master, while the other stands by as a backup should the master Routing Engine fail. On routing platforms with dual Routing Engines, network reconvergence takes place more quickly than on routing platforms with a single Routing Engine.

The Chassis View provides a pictorial representation of the chassis or device, and the modules or components that are installed in it, such as the line cards, interfaces, and other hardware elements. To view a pictorial representation of a device chassis and the configured components, such as interfaces, line cards, and hardware elements, select a managed device listed in the My Network tree in Device View of Build mode of the Connectivity Services Director GUI, and select **Device Management > View Physical Inventory** from the tasks pane.

The active or master and the standby or backup Routing Engines indicated on the Routing Engine in the Chassis View with a descriptive text label. "ACT" denotes an active Routing Engine, whereas "SDBY" denotes a standby Routing Engine. The status is updated on the Routing Engine only after a polling request because of the implications on the Junos Space application and device performance.

Routing Engine Redundancy Overview

When a Routing Engine is configured as master, it has full functionality. It receives and transmits routing information, builds and maintains routing tables, communicates with interfaces and Packet Forwarding Engine components, and has full control over the chassis. When a Routing Engine is configured to be the backup, it does not communicate with the Packet Forwarding Engine or chassis components.



NOTE: On devices running Junos OS Release 8.4 or later, both Routing Engines cannot be configured to be master at the same time. This configuration causes the commit check to fail.

A failover from the master Routing Engine to the backup Routing Engine occurs automatically when the master Routing Engine experiences a hardware failure or when you have configured the software to support a change in mastership based on specific conditions. You can also manually switch Routing Engine mastership by issuing one of the **request chassis routing-engine** commands. In this topic, the term *failover* refers to an automatic event, whereas *switchover* refers to either an automatic or a manual event.

When a failover or a switchover occurs, the backup Routing Engine takes control of the system as the new master Routing Engine.

- If graceful Routing Engine switchover is not configured, when the backup Routing Engine becomes master, it resets the switch plane and downloads its own version of the microkernel to the Packet Forwarding Engine components. Traffic is interrupted while the Packet Forwarding Engine is reinitialized. All kernel and forwarding processes are restarted.
- If graceful Routing Engine switchover is configured, interface and kernel information is preserved. The switchover is faster because the Packet Forwarding Engines are not restarted. The new master Routing Engine restarts the routing protocol process (rpd). All hardware and interfaces are acquired by a process that is similar to a warm restart.
- If graceful Routing Engine switchover and nonstop active routing (NSR) are configured, traffic is not interrupted during the switchover. Interface, kernel, and routing protocol information is preserved.
- If graceful Routing Engine switchover and graceful restart are configured, traffic is not interrupted during the switchover. Interface and kernel information is preserved. Graceful restart protocol extensions quickly collect and restore routing information from the neighboring routers.

Conditions That Trigger a Routing Engine Failover

The following events can result in an automatic change in Routing Engine mastership, depending on your configuration:

- The routing platform experiences a hardware failure. A change in Routing Engine mastership occurs if either the Routing Engine or the associated host module or subsystem is abruptly powered off. You can also configure the backup Routing Engine to take mastership if it detects a hard disk error on the master Routing Engine.
- The routing platform experiences a software failure, such as a kernel crash or a CPU lock. You must configure the backup Routing Engine to take mastership when it detects a loss of keepalive signal.
- A specific software process fails. You can configure the backup Routing Engine to take mastership when one or more specified processes fail at least four times within 30 seconds.

If any of these conditions is met, a message is logged and the backup Routing Engine attempts to take mastership. By default, an alarm is generated when the backup Routing Engine becomes active. After the backup Routing Engine takes mastership, it continues to function as master even after the originally configured master Routing Engine has successfully resumed operation. You must manually restore it to its previous backup status. (However, if at any time one of the Routing Engines is not present, the other Routing Engine becomes master automatically, regardless of how redundancy is configured.)

Related •
Documentation

Viewing Alarm Indicators in the Chassis Image

Activity on a network device consists of a series of events. A software component on the network device, called an entity, is responsible for running the Simple Network Management Protocol (SNMP) to log and monitor these events. When certain types of events are persistent, or when the condition causing the event crosses a threshold, SNMP sends a notification, also called a trap to Connectivity Services Director. Connectivity Services Director correlates traps, describing a condition, into an alarm.

The Chassis View provides a pictorial representation of the chassis or device, and the modules or components that are installed in it, such as the line cards, interfaces, and other hardware elements. To view a pictorial representation of a device chassis and the configured components, such as interfaces, line cards, and hardware elements, select a managed device listed in the My Network tree in Device View of Build mode of the Connectivity Services Director GUI, and select **Device Management > View Physical Inventory** from the tasks pane.

The alarms are correlated for each FPC in conjunction with other modules that are installed on a specific device chassis. This alarm value is added as a property to the FPC details. Apart from the Active Alarms pane that is displayed to the right of the graphical image of the chassis (in the Component Info pane), you can also view the alarm indicator as a circle or an LED icon that is displayed at the top of each FPC. A gray circle denotes that no alarm is present for the FPC module, whereas a red circle denotes that an active alarm is present for the FPC module.

Related •
Documentation

Viewing Port Statistics for OTN PICs

The performance monitoring capability in Connectivity Services Director displays information about the health of your network and changing conditions of your optical interfaces. Use this diagnosis and detection mechanism to identify problems with the equipment, pinpoint security attacks, or to analyze trends and categories of errors. This feature includes fault-monitoring details in the dashboard, monitoring pages, and in a dedicated page that displays alarms, events, and system log messages that are generated. Performance monitoring parameters can be viewed in both chart and statistical formats. These charts and statistical details provide essential and cohesive information about system conditions, any discrepancies and malfunctioning, and protocols or components that need to be examined and debugged for better efficiency and working capacity. You can assess the performance of your network, not only at a point in time, but also over a period of time. This feature enables you to determine trending and network-health parameters; for example, whether service-level agreements (SLAs) have been violated.

The port statistics are available for viewing when the port on the FPC is selected. The Packets and Error counters for the selected port are displayed in the Optics PMs dialog box.

To view the port statistical details for OTN PICs:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the device for which you want to define the optical port settings.

The selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. Select an OTN PIC, such as a 2-port 100-Gigabit Ethernet OTN PIC, in the image of the device.

The Component Info dialog box is displayed on the right pane with the PIC specifications. For example, if you select a 100-Gigabit Ethernet PIC installed in a PTX Series router, the Component Info dialog box is displayed to the right of the graphical view of the chassis. Select the Performance tab at the bottom of the dialog box to open the Optics PMs dialog box.

6. Click the **Performance** tab at the bottom of the dialog box.

The Optics PMs dialog box is displayed with the performance monitoring attributes for the OTN PIC. The Packet Counters and Error Counters tabs are displayed in the dialog box. The date and time at which the dialog box was last refreshed is shown.

The following fields are displayed in the Packet Counters tab of the Optics PMs dialog box:

- UniCast In—Ingress unicast packets per second
- BroadCast In—Ingress broadcast In packet per second
- Multicast In—Ingress multicast In packet per second
- Unicast Out—Egress unicast packets per second
- Broadcast Out—Egress broadcast packets per second
- Multicast Out—Egress multicast packets per second

The following fields are displayed in the Error Counters tab of the Optics PMs dialog box:

- **Errors In**—Sum of the incoming frame aborts and FCS errors.
- **Drops In**—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism.
- **Framing errors In**—Number of packets received with an invalid frame checksum (FCS).
- **Runts In**—Number of frames received that are smaller than the runt threshold.
- **Policed discards In**—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle.
- **L3 incompletes In**—Number of incoming packets discarded because they failed Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with less than 20 bytes of available IP header is discarded. L3 incomplete errors can be ignored by configuring the **ignore-l3-incompletes** statement.
- **L2 channel errors In**—Number of times the software did not find a valid logical interface for an incoming frame.
- **L2 mismatch timeouts In**—Number of malformed or short packets that caused the incoming packet handler to discard the frame as unreadable.
- **FIFO errors In**—Number of FIFO errors in the receive direction that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.
- **Resource errors In**—Sum of transmit drops.
- **Oversized frames In**—Number of frames that exceed 1518 octets.
- **Jabber frames In**—Number of frames that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment

error. This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition in which any packet exceeds 20 ms. The allowed range to detect jabber is from 20 ms to 150 ms.

- **Fragment frames In**—Total number of packets that were less than 64 octets in length (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. Fragment frames normally increment because both runts (which are normal occurrences caused by collisions) and noise hits are counted.
 - **CRC errors In**—Total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
 - **Carrier transitions Out**—Number of times the interface has gone from **down** to **up**. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC or PIM is malfunctioning.
 - **Errors Out**—Sum of the outgoing frame aborts and FCS errors.
 - **Drops Out**—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism.
 - **Collisions Out**—Number of Ethernet collisions. The Gigabit Ethernet PIC supports only full-duplex operation, so for Gigabit Ethernet PICs, this number should always remain 0. If it is nonzero, there is a software bug.
 - **Aged packets Out**—Number of packets that remained in shared packet SDRAM so long that the system automatically purged them. The value in this field should never increment. If it does, it is most likely a software bug or possibly malfunctioning hardware.
 - **FIFO errors Out**—Number of FIFO errors in the send direction as reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.
 - **HS link CRC errors Out**—Number of errors on the high-speed links between the ASICs responsible for handling the router interfaces.
 - **MTU errors Out**—Number of packets whose size exceeded the MTU of the interface.
 - **Resource errors Out**—Sum of transmit drops.
7. To view a graphical representation of the port statistics, click the **Show Chart** button above the Packet Counters and Error Counters tabs. The Port Statistics pop-up dialog box is displayed.

You can view the interface statuses, such as errors and the operational conditions of the interfaces, that enables you in analyzing, troubleshooting, and rectifying problems with dropped packets or untransmitted bytes. Some of the causes for such a loss of traffic or a block in transmission of data packets include overloaded system conditions, profiles and policies that restrict the bandwidth or priority of traffic, network outages,

or disruption with physical cable faults. This operation is equivalent to the `show interface statistics` command that you can run from the Junos OS CLI interface. You can search for specific devices or interfaces by entering a search item and clicking the Search icon. A line graph is displayed with the input packets and errors, and output packets and errors shown on the vertical axis and the time shown on the horizontal axis. The following color-coded legends reference the line graphs:

- Packets In (Orange)—Number of packets received on the interface
- Packets Out (Green)—Number of packets sent from the interface
- Errors In (Blue)—Number of inbound errors received on the interface
- Errors Out (Purple)—Number of outbound errors transmitted from the interface

From the Time Interval drop-down box, select 1 Hour, 8 Hours, 1 Day, 1 Week, 1 Month, 3 Months, 6 Months, 1 Year, or Custom to specify the duration for which the data polled from devices needs to be displayed. If you select the Custom option, the Time range popup dialog box is displayed. Specify the date from the calendar, and select the Time From (Start time in the 24-hour time format of collection of data), and Time To (End time in the 24-hour time format of collection of data). Click OK to save the settings. Else, click Cancel to discard the configuration.

The Interface Details table displays all the UNI parts of the service. Also, the physical interface for the logical interface participating in the service is displayed.

- Serial Num—Serial number of the hardware component
- Port Name—Name of the interface
- Interface Type—Whether the interface is physical or logical
- Link Type—Operational status of the physical interface: Up, Down.
- MAC Address—MAC address of the physical interface.
- Input Packets—Number of packets received on the interface.
- Output Packets—Number of packets sent from the interface.
- Last Poll Time—Date and time at which the statistical detail was obtained by polling and retrieving from the device for the specified interface.

The Packet Counter tab on the right side of the page displays the following fields in a table. It is applicable for physical interfaces only. The values displayed are in rates of packets per second.

- Input Unicasts—Number of input unicast packets for the physical interface
- Output Unicasts—Number of output unicast packets for the physical interface
- Input Multicast—Number of input multicast packets for the physical interface
- Output Multicast—Number of output multicast packets for the physical interface
- Input Broadcast—Number of input broadcast packets for the physical interface
- Output Broadcast—Number of output broadcast packets for the physical interface

The Error Counter tab on the right side of the page displays the following fields in a table. It is available for physical interfaces only. The values displayed are in rates of packets per second.

- Input Errors—Number of errors packets received on the physical interface
- Output Drops—Number of outgoing packets that are dropped by the physical interface
- Input Framing Errors—Number of packets with framing errors that are received on the physical interface
- Input Drops—Number of incoming packets that are dropped by the physical interface
- Input Discards—Number of incoming packets discarded by the physical interface
- Output Errors—Number of error packets sent out from the physical interface

You can click the **Refresh** (rotating arrow icon) button at the top of the dialog box to enable the latest settings be retrieved from the device and displayed.

Related Documentation

Example: Configuring Two Fiber Line Terminations Using IPLCs for Optical Amplification in a Metro Linear Packet Optical Network

For metro linear and metro ring topologies that require either north-south or east-west communications, you can connect two integrated photonic line card (IPLC) base modules together to form a single node with two fiber line terminations. This example shows how to configure the Junos OS to support the IPLC base modules in a Metro linear packet optical configuration for adding and dropping wavelengths to a local optical interface, and for bypassing wavelengths to another IPLC. You can set up and configure an IPLC node with two line-side fiber terminations.

- [Requirements on page 1668](#)
- [Overview on page 1669](#)
- [Configuration on page 1673](#)
- [Verification on page 1681](#)

Requirements

This example uses the following hardware and software components:

- Three PTX3000 Packet Transport Routers running Junos OS Release 15.1F6
- Four IPLC base modules
- Compatible 10-Gigabit or 100-Gigabit Ethernet OTN PICs

For complete information on all PTX Series Packet Transport Routers hardware components, see [PTX Series Packet Transport Routers](#).

For complete information on all PTX Series Packet Transport Routers software features, see [Junos OS for PTX Series Packet Transport Routers, Release 15.1](#).

Before you start this procedure, complete the following tasks:

- Install the IPLCs, FPCs, and PICs in the PTX3000 chassis.



BEST PRACTICE: We recommend that you place the two IPLC modules at Node B into the same FPC/PIC slot pair on the PTX3000 chassis. In this example the IPLCs at Node B are located in FPC slots 2 and 3.

- Make all connections to and from the PICs in the PTX3000 chassis to the **Add** and **Drop** ports on front panel of each IPLC node as shown in [Figure 124 on page 1670](#).
- Connect your fiber pairs to the **Line IN** and **Line OUT** ports on the front panel of each IPLC node as shown in [Figure 124 on page 1670](#).

For simplicity, [Figure 124 on page 1670](#) does not show the optical ILAs between the three IPLC nodes.

- On Node B, connect the two IPLC modules together using the **PT IN** and **PT OUT** ports on the front panel of the IPLC as shown in [Figure 124 on page 1670](#).
- Be sure to specify wavelength values on each interface as shown in [Figure 124 on page 1670](#). If you must adjust the wavelength values, make sure that you enter a value supported on the IPLC.



BEST PRACTICE: Anytime you need to disconnect or connect the fiber span from the Line IN and Line OUT ports on the IPLC module, we recommend you disable the optical supervisory channel and the erbium-doped fiber amplifiers on the IPLC.

Always refer to the PTX3000 Packet Transport Router Hardware Guide when connecting or disconnecting cables on the IPLC modules. See [PTX3000 Packet Transport Router Hardware Guide](#).

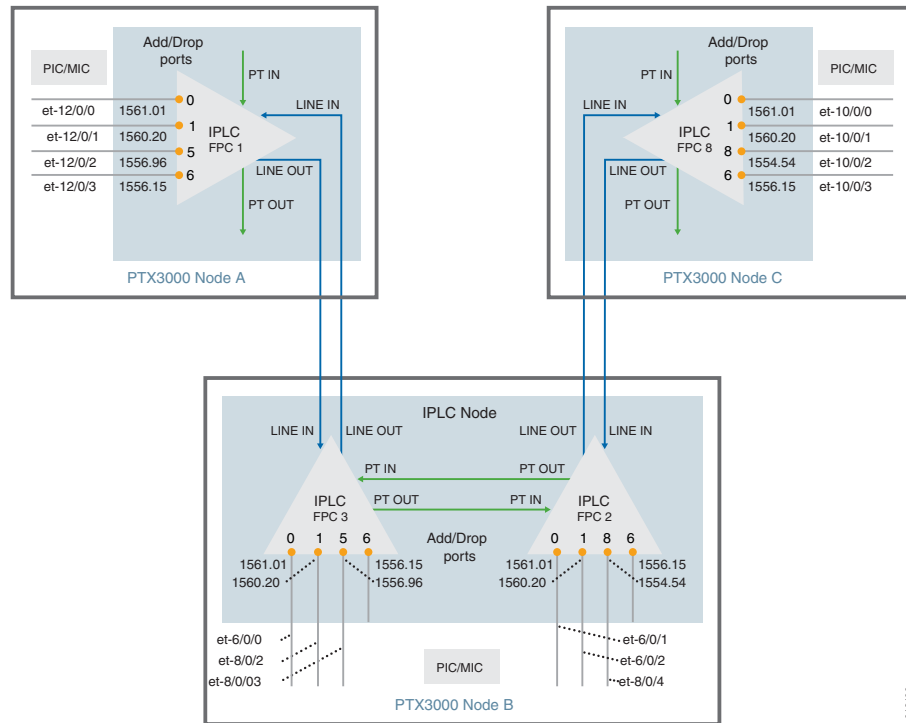
Overview

This examples describes how to configure Junos OS to support IPLC base modules in a Metro linear packet optical deployment. The Add/Drop ports of the IPLC modules are physically connected to interfaces housed in the same PTX3000 chassis.

The IPLC modules provide the combined functionality of a 32-port Reconfigurable Optical Add/Drop Multiplexer (ROADM), optical amplification, optical equalization, and optical channel monitoring on a single card.

Topology

Figure 124: IPLC in Metro Linear Packet Optical Deployment



This procedure describes how to configure Junos OS for the IPLC modules. This is not a complete configuration and does not include full instructions for configuring the router or the associated line cards. Before you start this procedure, complete the following hardware and software tasks on the PTX 3000 router:

- Install the IPLCs, associated line cards, and PICs into the PTX3000 chassis so that the hardware configuration matches what is shown in [Figure 124 on page 1670](#). If you need to make changes to the positions of the cards in the chassis, adjust the FPC numbers referenced in [Figure 124 on page 1670](#) and configure them accordingly.



BEST PRACTICE: We recommend that you place the two IPLC modules at Node B into the same FPC or PIC slot pair on the PTX3000 chassis. In this example the IPLCs at Node B are located in FPC slots 2 and 3.

- Configure the associated wavelengths on the interfaces of the PTX3000 by using the following procedure:
 - Specify the interface to configure.

```
[edit]
user@host# edit interfaces interface-name
```

For example:

```
[edit]
user@host# edit interfaces et-6/0/0]
```

- Specify the wavelength value supported on the interface.

```
[edit interfaces et-6/0/0]
user@host# set wavelength
```



NOTE: Be sure to specify wavelength values on each interface as shown in [Figure 124 on page 1670](#). If you must adjust the wavelength values, make sure that you enter a value supported on the IPLC.

- Make all connections to and from the PICs in the PTX3000 chassis to the ADD or DROP ports on front panel of each IPLC node as shown in [Figure 124 on page 1670](#).
- Connect your fiber pairs to the LINE IN and LINE OUT ports on the front panel of each IPLC node as shown in [Figure 124 on page 1670](#).

For simplicity, [Figure 124 on page 1670](#) does not show the optical inline amplifiers (optical ILAs) between the three IPLC nodes.

- On Node B, connect the two IPLC modules together using the PT IN and PT OUT ports on the front panel of the IPLC as shown in [Figure 124 on page 1670](#).

This example results in the following configuration:

Table 247: Wavelength, Port, and IPLC Nodes Mapping

Wavelength	Node A		Node B		Node C	
	Optical Interface Waveform is Switched to on PTX3000 Chassis	IPLC Slot: Port: Mode:	Optical Interface Waveform is Switched to on PTX3000 Chassis	IPLC Slot: Port: Mode:	Optical Interface Waveform is Switched to on PTX3000 Chassis	IPLC Slot: Port: Mode:
1554.54	—	—	et-8/0/4	Slot: 2 Port: 8 Mode: switch	et-10/0/2	Slot: 8 Port: 8 Mode: switch

Table 247: Wavelength, Port, and IPLC Nodes Mapping (continued)

Wavelength	Node A		Node B		Node C	
	Optical Interface Waveform is Switched to on PTX3000 Chassis	IPLC Slot: Port: Mode:	Optical Interface Waveform is Switched to on PTX3000 Chassis	IPLC Slot: Port: Mode:	Optical Interface Waveform is Switched to on PTX3000 Chassis	IPLC Slot: Port: Mode:
1556.15	et-12/0/3	Slot: 1 Port: 6 Mode: switch	—	Slot: 2 Port: 6 Mode: wss-express-in (bypass) Slot: 3 Port: 6 Mode: wss-express-in (bypass)	et-10/0/3	Slot: 8 Port: 6 Mode: switch
1556.96	et-12/0/2	Slot: 1 Port: 5 Mode: switch	et-8/0/3	Slot: 3 Port: 5 Mode: switch	—	—
1560.20	et-12/0/1	Slot: 1 Port: 1 Mode: switch	et-6/0/2	Slot: 2 Port: 1 Mode: switch Slot: 3 Port: 1 Mode: switch	et-10/0/1	Slot: 8 Port: 1 Mode: switch
1561.01	et-12/0/0	Slot: 1 Port: 0 Mode: switch	et-6/0/1 et-6/0/0	Slot: 2 Port: 0 Mode: switch Slot: 3 Port: 0 Mode: switch	et-10/0/0	Slot: 8 Port: 0 Mode: switch

- 3x100G of Ethernet between Node A and Node B through a multi-span link.
- 3x100G of Ethernet between Node B and Node C through a multi-span link.
- 1x100G of Ethernet between Node A and Node C through a multi-span link including an optical bypass at through Node B.
- In this example:
 - Wavelengths 1561.01 and 1560.20 are dropped at Node B and are also reused in both directions (Node A and Node C).
- Other wavelengths such as wavelength 1556.96 between Node A and Node B and wavelength 1554.54 between Node B and Node C are used in only a single direction.
- Wavelengths used in both directions can also be configured for optical buypass if it was necessary to reduce the packet throughput between the nodes. You can configure optical bypasses through the CLI, they do not require manual connection.
- If traffic changes, you could configure Node B with 1561.01 and 1560.20 as optical bypass and that creates an additional 2x100G between Node A and Node C, leaving only 100 Gbps of traffic to Node B (and leaving four interfaces unused).

Configuration

The following example requires you to navigate various levels in the configuration hierarchy.

For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode*.

Before you start this procedure, be sure to complete the tasks described in the “Requirements” on page 1668 section of this example.

To configure the IPLC base modules in this example, perform these tasks:

- [Configuring the IPLC Base Module at Node A on page 1674](#)
- [Configuring the Two IPLC Base Modules at Node B on page 1676](#)
- [Configuring the IPLC Base Module at Node C on page 1679](#)
- [Results on page ?](#)

CLI Quick Configuration

To quickly configure this example, copy the following commands into a text file, remove any line breaks, and then paste the commands into the CLI at the [edit] hierarchy level.

```
set chassis fpc 1 optical-options wavelength 1556.15 switch et-12/0/3
set chassis fpc 1 optical-options wavelength 1556.96 switch et-12/0/2
set chassis fpc 1 optical-options wavelength 1560.20 switch et-12/0/1
set chassis fpc 1 optical-options wavelength 1561.01 switch et-12/0/0
set chassis fpc 2 optical-options wavelength 1554.54 switch et-8/0/4
set chassis fpc 2 optical-options wavelength 1556.15 wss-express-in
set chassis fpc 2 optical-options wavelength 1560.20 switch et-6/0/2
set chassis fpc 2 optical-options wavelength 1561.01 switch et-6/0/1
set chassis fpc 2 optical-options express-in fpc 3
set chassis fpc 3 optical-options wavelength 1556.15 wss-express-in
```

```
set chassis fpc 3 optical-options wavelength 1556.96 switch et-8/0/3
set chassis fpc 3 optical-options wavelength 1560.20 switch et-8/0/2
set chassis fpc 3 optical-options wavelength 1561.01 switch et-6/0/0
set chassis fpc 3 optical-options express-in fpc 2
set chassis fpc 8 optical-options wavelength 1554.54 switch et-10/0/2
set chassis fpc 8 optical-options wavelength 1556.15 switch et-10/0/3
set chassis fpc 8 optical-options wavelength 1560.20 switch et-10/0/1
set chassis fpc 8 optical-options wavelength 1561.01 switch et-10/0/0
```

Configuring the IPLC Base Module at Node A

Step-by-Step Procedure

This procedure describes how to configure the IPLC base module in slot 1 of Node A in this example.

Before you start this procedure, be sure to complete the tasks described in the [“Requirements” on page 1668](#) section of this example.

To configure the IPLC base module in slot 1 of Node A:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.
2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.
3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the PTX300 router for which you want to define the optical IPLC settings.

The network tree is expanded and the selected device is highlighted.
4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.
5. Select an optical IPLC in the image of the device.

The Component Info dialog box is displayed.
6. Click the **Status/Config** tab at the bottom of the dialog box.

The IPLC Line dialog box is displayed on the right pane with the configuration settings that pertain to the IPLC.
7. Specify the FPC or PIC slot in which the IPLC base module resides by selecting the slot in the Chassis View.

In this case, because the IPLC base module resides in FPC slot 1, select the **IPLC 1** component in the image of the chassis.

8. Configure wavelength 1561.01 on port 0 of the IPLC base module to be switched to optical interface et-12/0/0. In the Wavelength Configuration section, select the **Show All Wavelengths** check box, and beside the **1561.01** row in the **wavelength** column, select **switch** from the drop-down menu in the **configuration** column of the table for the corresponding wavelength.
9. From the **end-point** column, click in the cell corresponding to the wavelength of 1561.01, and then click the drop-down arrow. From the drop-down menu, select **et-12/0/0** to which you want the wavelength of the IPLC base module to be switched.
10. Configure wavelength 1560.20 on port 1 of the IPLC base module to be switched to optical interface et-12/0/1. In the Wavelength Configuration section, beside the **1560.20** row in the **wavelength** column, select **switch** from the drop-down menu in the **configuration** column of the table for the corresponding wavelength.
11. From the **end-point** column, click in the cell corresponding to the wavelength of 1560.20, and then click the drop-down arrow. From the drop-down menu, select **et-12/0/1** to which you want the wavelength of the IPLC base module to be switched.
12. Configure wavelength 1556.96 on port 5 of the IPLC base module to be switched to optical interface et-12/0/2. In the Wavelength Configuration section, beside the **1556.96** row in the **wavelength** column, select **switch** from the drop-down menu in the **configuration** column of the table for the corresponding wavelength.
13. From the **end-point** column, click in the cell corresponding to the wavelength of 1556.96, and then click the drop-down arrow. From the drop-down menu, select **et-12/0/2** to which you want the wavelength of the IPLC base module to be switched.
14. Configure wavelength 1556.15 on port 6 of the IPLC base module to be switched to optical interface et-12/0/3. In the Wavelength Configuration section, beside the **1556.15** row in the **wavelength** column, select **switch** from the drop-down menu in the **configuration** column of the table for the corresponding wavelength.
15. From the **end-point** column, click in the cell corresponding to the wavelength of 1556.15, and then click the drop-down arrow. From the drop-down menu, select **et-12/0/3** to which you want the wavelength of the IPLC base module to be switched.
16. Click **Update** to save the specified configuration settings.

Configuring the Two IPLC Base Modules at Node B

Step-by-Step Procedure This procedure describes how to configure the IPLC base module in slot 2 of Node B in this example.

Before you start this procedure, be sure to complete the tasks described in the [“Requirements” on page 1668](#) section of this example.



BEST PRACTICE: We recommend that you place the two IPLC modules in the same FPC or PIC slot pair on the PTX3000 chassis.

To configure the IPLC base module in slot 2 of Node B:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.
The workspaces that are applicable to Build mode are displayed on the Tasks pane.
2. From the View selector, select **Device View**.
The functionalities that you can configure in this view are displayed.
3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the PTX300 router for which you want to define the optical IPLC settings.
The network tree is expanded and the selected device is highlighted.
4. From the Tasks pane, select **Device Management > View Physical Inventory**.
An image of the device is displayed on the right pane.
5. Select an optical IPLC in the image of the device.
The Component Info dialog box is displayed.
6. Click the **Status/Config** tab at the bottom of the dialog box.
The IPLC Line dialog box is displayed on the right pane with the configuration settings that pertain to the IPLC.
7. Specify the FPC or PIC slot in which the IPLC base module resides by selecting the slot in the Chassis View.
In this case, because the IPLC base module resides in FPC slot 2, select the **IPLC 2** component in the image of the chassis.

8. Create a logical connection between this IPLC base module and the IPLC base module in slot 3. Select **FPC 3** from the Express IPLC list in the Settings/Status section.
9. Configure wavelength 1561.01 on port 0 of the IPLC base module to be switched to optical interface et-6/0/1. In the Wavelength Configuration section, select the **Show All Wavelengths** check box, and beside the **1561.01** row in the **wavelength** column, select **switch** from the drop-down menu in the **configuration** column of the table for the corresponding wavelength.
10. From the **end-point** column, click in the cell corresponding to the wavelength of 1561.01, and then click the drop-down arrow. From the drop-down menu, select **et-6/0/1** to which you want the wavelength of the IPLC base module to be switched.
11. Configure wavelength 1560.20 on port 1 of the IPLC base module to be switched to optical interface et-6/0/2. In the Wavelength Configuration section, beside the **1560.20** row in the **wavelength** column, select **switch** from the drop-down menu in the **configuration** column of the table for the corresponding wavelength.
12. From the **end-point** column, click in the cell corresponding to the wavelength of 1560.20, and then click the drop-down arrow. From the drop-down menu, select **et-6/0/2** to which you want the wavelength of the IPLC base module to be switched.
13. Configure wavelength 1554.54 on port 5 of the IPLC base module to be switched to optical interface et-8/0/4. In the Wavelength Configuration section, beside the **1556.54** row in the **wavelength** column, select **switch** from the drop-down menu in the **configuration** column of the table for the corresponding wavelength.
14. From the **end-point** column, click in the cell corresponding to the wavelength of 1554.54, and then click the drop-down arrow. From the drop-down menu, select **et-8/0/4** to which you want the wavelength of the IPLC base module to be switched.
15. Configure wavelength 1556.15 on port 6 of the IPLC base module in slot 2 to be bypassed. In the Wavelength Configuration section, beside the **1556.15** row in the **wavelength** column, select **express** from the drop-down menu in the **configuration** column of the table for the corresponding wavelength.
16. Click **Update** to save the specified configuration settings.

**Step-by-Step
Procedure**

This procedure describes how to configure the IPLC base module in slot 3 of Node B in this example.

Before you start this procedure, be sure to complete the tasks described in the [“Requirements” on page 1668](#) section of this example.

To configure the IPLC base module in slot 3 of Node B:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.

2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.

3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the PTX300 router for which you want to define the optical IPLC settings.

The network tree is expanded and the selected device is highlighted.

4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.

5. Select an optical IPLC in the image of the device.

The Component Info dialog box is displayed.

6. Click the **Status/Config** tab at the bottom of the dialog box.

The IPLC Line dialog box is displayed on the right pane with the configuration settings that pertain to the IPLC.

7. Specify the FPC or PIC slot in which the IPLC base module resides by selecting the slot in the Chassis View.

In this case, because the IPLC base module resides in FPC slot 3, select the **IPLC 3** component in the image of the chassis.

8. Create a logical connection between this IPLC base module and the IPLC base module in slot 2. Select **FPC 2** from the Express IPLC list in the Settings/Status section.

9. Configure wavelength 1561.01 on port 0 of the IPLC base module to be switched to optical interface et-6/0/0. In the Wavelength Configuration section, select the **Show All Wavelengths** check box, and beside the **1561.01** row in the **wavelength**

column, select **switch** from the drop-down menu in the **configuration** column of the table for the corresponding wavelength.

10. From the **end-point** column, click in the cell corresponding to the wavelength of 1561.01, and then click the drop-down arrow. From the drop-down menu, select **et-6/0/0** to which you want the wavelength of the IPLC base module to be switched.
11. Configure wavelength 1560.20 on port 0 of the IPLC base module to be switched to optical interface et-8/0/2. In the Wavelength Configuration section, beside the **1560.20** row in the **wavelength** column, select **switch** from the drop-down menu in the **configuration** column of the table for the corresponding wavelength.
12. From the **end-point** column, click in the cell corresponding to the wavelength of 1561.01, and then click the drop-down arrow. From the drop-down menu, select **et-8/0/2** to which you want the wavelength of the IPLC base module to be switched.
13. Configure wavelength 1556.96 on port 5 of the IPLC base module to be switched to optical interface et-8/0/3. In the Wavelength Configuration section, beside the **1560.20** row in the **wavelength** column, select **switch** from the drop-down menu in the **configuration** column of the table for the corresponding wavelength.
14. From the **end-point** column, click in the cell corresponding to the wavelength of 1556.96, and then click the drop-down arrow. From the drop-down menu, select **et-8/0/3** to which you want the wavelength of the IPLC base module to be switched.
15. Configure wavelength 1556.15 on port 6 of the IPLC base module in slot 3 to be bypassed. In the Wavelength Configuration section, select the **Show All Wavelengths** check box, and beside the **1560.20** row in the **wavelength** column, select **express** from the drop-down menu in the **configuration** column of the table for the corresponding wavelength.
16. Click **Update** to save the configured settings.

Configuring the IPLC Base Module at Node C

Step-by-Step Procedure

This procedure describes how to configure the IPLC base module in slot 8 of Node C in this example.

Before you start this procedure, be sure to complete the tasks described in the [“Requirements” on page 1668](#) section of this example.

**Step-by-Step
Procedure**

To configure the IPLC base module in slot 8 of Node C:

1. From the Junos Space user interface, click the **Build** icon on the Connectivity Services Director banner.

The workspaces that are applicable to Build mode are displayed on the Tasks pane.
2. From the View selector, select **Device View**.

The functionalities that you can configure in this view are displayed.
3. From the Device View pane, click the plus sign (+) next to the My Network tree to expand the tree and select the PTX300 router for which you want to define the optical IPLC settings.

The network tree is expanded and the selected device is highlighted.
4. From the Tasks pane, select **Device Management > View Physical Inventory**.

An image of the device is displayed on the right pane.
5. Select an optical IPLC in the image of the device.

The Component Info dialog box is displayed.
6. Click the **Status/Config** tab at the bottom of the dialog box.

The IPLC Line dialog box is displayed on the right pane with the configuration settings that pertain to the IPLC.
7. Specify the FPC or PIC slot in which the IPLC base module resides by selecting the slot in the Chassis View.

In this case, because the IPLC base module resides in FPC slot 8, select the **IPLC 8** component in the image of the chassis.
8. Configure wavelength 1561.01 on port 0 of the IPLC base module to be switched to optical interface et-10/0/0. In the Wavelength Configuration section, select the **Show All Wavelengths** check box, and beside the **1561.01** row in the **wavelength** column, select **switch** from the drop-down menu in the **configuration** column of the table for the corresponding wavelength.

From the **end-point** column, click in the cell corresponding to the wavelength of 1561.01, and then click the drop-down arrow. From the drop-down menu, select **et-10/0/0** to which you want the wavelength of the IPLC base module to be switched.
9. Configure wavelength 1560.20 on port 1 of the IPLC base module to be switched to optical interface et-10/0/1. In the Wavelength Configuration section, beside the

1560.20 row in the **wavelength** column, select **switch** from the drop-down menu in the **configuration** column of the table for the corresponding wavelength.

From the **end-point** column, click in the cell corresponding to the wavelength of 1560.20, and then click the drop-down arrow. From the drop-down menu, select **et-10/0/1** to which you want the wavelength of the IPLC base module to be switched.

10. Configure wavelength 1554.54 on port 8 of the IPLC base module to be switched to optical interface et-10/0/2. In the Wavelength Configuration section, beside the **1554.54** row in the **wavelength** column, select **switch** from the drop-down menu in the **configuration** column of the table for the corresponding wavelength.

From the **end-point** column, click in the cell corresponding to the wavelength of 1554.54, and then click the drop-down arrow. From the drop-down menu, select **et-10/0/2** to which you want the wavelength of the IPLC base module to be switched.

11. Configure wavelength 1556.15 on port 6 of the IPLC base module to be switched to optical interface et-10/0/3. In the Wavelength Configuration section, beside the **1556.15** row in the **wavelength** column, select **switch** from the drop-down menu in the **configuration** column of the table for the corresponding wavelength.

From the **end-point** column, click in the cell corresponding to the wavelength of 1556.15, and then click the drop-down arrow. From the drop-down menu, select **et-10/0/3** to which you want the wavelength of the IPLC base module to be switched.

12. Click **Update** to save the configured settings.

Verification

Confirm that the configuration is working properly.

- [Verifying the Topology of Each IPLC Node on page 1681](#)

Verifying the Topology of Each IPLC Node

Purpose Verify the topology of each IPLC node.

- Action** Run the **show chassis fpc optical-properties topology** command with the **detail** output level at each IPLC node and verify that the following fields match the values listed in [Table 247 on page 1671](#).
- **Port/Wavelength**—Verify that this field lists the proper wavelength values and IPLC port numbers for each node in this example.
 - **State**—Verify that the values for this field match what is listed in [Table 247 on page 1671](#) for the mode value of each IPLC port for each node in this example.
 - **Connected To**—If the wavelength is being switched, verify that this field lists the correct interface the wavelength is being switched to.

Verify the topology of each IPLC node.

1. For example, at IPLC Node A, enter the following.

```
user@host>show chassis fpc optical-properties topology detail fpc-slot 1
```

IPLC Topology Information				
Wavelength(nm)	Port	Frequency(THz)	State	Connected
To				
Express-in Port			DOWN	NA
Expansion Port			DOWN	NA
1561.01	0	192.05	Switched	et-12/0/0
1560.20	1	192.15	Switched	et-12/0/1
1559.39	2	192.25	Blocked	NA
1558.58	3	192.35	Blocked	NA
1557.77	4	192.45	Blocked	NA
1556.96	5	192.55	Switched	et-12/0/2
1556.15	6	192.65	Switched	et-12/0/3
1555.34	7	192.75	Blocked	NA
1554.54	8	192.85	Blocked	NA
1553.73	9	192.95	Blocked	NA
1552.93	10	193.05	Blocked	NA
1552.12	11	193.15	Blocked	NA
1551.32	12	193.25	Blocked	NA
1550.52	13	193.35	Blocked	NA
1549.72	14	193.45	Blocked	NA
1548.91	15	193.55	Blocked	NA
1548.11	16	193.65	Blocked	NA
1547.32	17	193.75	Blocked	NA
1546.52	18	193.85	Blocked	NA
1545.72	19	193.95	Blocked	NA
1544.92	20	194.05	Blocked	NA
1544.13	21	194.15	Blocked	NA
1543.33	22	194.25	Blocked	NA
1542.54	23	194.35	Blocked	NA
1541.75	24	194.45	Blocked	NA
1540.95	25	194.55	Blocked	NA
1540.16	26	194.65	Blocked	NA
1539.37	27	194.75	Blocked	NA
1538.58	28	194.85	Blocked	NA
1537.79	29	194.95	Blocked	NA
1537.00	30	195.05	Blocked	NA
1536.22	31	195.15	Blocked	NA

2. At Node B, enter the following:

```
user@host> show chassis fpc optical-properties topology detail fpc-slot 2
user@host> show chassis fpc optical-properties topology detail fpc-slot 3
```

3. At Node C:

```
user@host> show chassis fpc optical-properties topology detail fpc-slot 8
```

Meaning For example, in Step 1 for Node A, you can see that the IPLC module in slot 1 includes the following configuration:

- Wavelength 1561.01 is switched to optical interface et-12/0/0
- Wavelength 1560.20 is switched to optical interface et-12/0/1
- Wavelength 1556.96 is switched to optical interface et-12/0/2
- Wavelength 1556.16 is switched to optical interface et-12/0/3

This matches what is listed in [Table 247 on page 1671](#) for Node A and confirms the configuration is operating correctly.

- Related Documentation**
- [Viewing a Graphical Image of the Optical Integrated Photonic Line Card on page 1605](#)
 - [Configuring Optical IPLC for Easy and Optimal Deployment on page 1609](#)
 - [Viewing Performance Monitoring Details of Optical IPLCs for Detecting and Diagnosing Faults on page 1617](#)
 - [Configuring Threshold-Crossing Alarms for Optical IPLCs for Monitoring Link Performance on page 1629](#)

PART 18

Working with User Roles

- [Managing User Roles on page 1687](#)

Managing User Roles

- [Creating a User-Defined Role on page 1687](#)
- [Managing Roles on page 1689](#)

Creating a User-Defined Role

You can create custom roles to grant users different access rights to the Connectivity Services Director modes. Connectivity Services Director modes—Report, Deploy, Monitor, Fault, and Build are available to assign to custom user roles in the list of application workspaces and associated tasks

Junos Space Network Management Platform provides read-only predefined roles—that is, Super Administrator, System Administrator, or User Administrator—that you can use to create users to perform tasks that these roles permit. You can also create read-write user-defined roles that conform to user responsibilities and access privileges required on your network. You can modify and delete only user-defined roles that you create. You cannot modify or delete predefined roles.

The following predefined roles are applicable for Connectivity Services Director to handle different operations for devices and services with varying privileges and permissions:

- The Device Manager role allows an administrator to discover devices.
- The Service Manager role allows an administrator to perform device pre-staging actions including discovering and assigning device roles.
- The Service Designer roles allows an administrator to create and publish a service definition.
- The Service Activator (less privileged) role allows an administrator to perform provisioning tasks including creating and managing customers, service orders, and services.



NOTE: For the Service Manager, Service Designer, and Service Activator user roles that are present in Services Activation Director, the roles are migrated with additional access privileges to enable access to the different lifecycle modes of Connectivity Services Director after upgrading to Connectivity Services Director, Release 1.0.

To create a user-defined role:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > Roles**.

The Roles page appears.

2. Click the **Create Role** icon on the menu bar.

The Create Role page appears, allowing you to select workspaces and associated tasks from all deployed applications.

3. In the **Title** text box, type a user-defined role name.

The role title cannot exceed 32 characters. The title can contain only letters and numbers and can include a hyphen (-), underscore (_), or period (.). Also, the title cannot start with a space.

4. In the **Description** text box, type a user-defined role description.

The role description cannot exceed 256 characters. The description can contain only letters and numbers and can include a hyphen (-), underscore (_), period (.), or comma (,).

5. Select an application workspace from the application selection ribbon.

Mouse over an application workspace icon to view the application and workspace name. You can select one or more workspaces per user-defined role. An expandable and collapsible tree of associated tasks appear below the selection ribbon for you to modify specific tasks that you want included in the Task Summary pane.

6. Select the specific tasks that you want for the user-defined role. All application workspace tasks are selected by default in the task tree.

Only the currently edited application workspace node is expanded in the Task Summary pane; previously selected workspace nodes are collapsed. You can expand other workspace nodes manually.

Selecting the top node or workspace selects or deselects the whole task tree. Selecting any task node automatically selects all tasks under the task node. Selecting any task node automatically selects its parent and grandparent.

Only the currently active task tree appears in the Task Summary pane.

In the Task Summary pane, the top-level application node in the tree is set in bold-italic; the second-level workspace tree node is set in bold.

7. Click **Create**.

The user-defined role is created, saved, and appears on the Roles inventory page.

Scroll down or search to view it.

You cannot create or save a user-defined role when the workspace tasks are not selected. Junos Space throws the following error message:

Task tree selection can not be empty.

Creation of a role generates an audit log entry.

Related Documentation

- *Predefined Roles Overview*
- [Managing Roles on page 1689](#)
- *Modifying User-Defined Roles*
- *Deleting User-Defined Roles*
- *Creating Users in Junos Space Network Management Platform*

Managing Roles

A role is a description of tasks a user can perform in Junos Space Network Management Platform to allow access to application workspaces. The **Role Based Access Control > Roles** inventory page allows Super Administrator or User Administrator to view all predefined and user-defined roles that exist for Junos Space applications. The administrator should understand all predefined roles and create any user-defined roles before creating users.

- [Viewing User Role Details on page 1689](#)
- [Performing Manage Roles Commands on page 1690](#)

Viewing User Role Details

The **Roles** inventory page displays all predefined and user-defined roles in a tabular view.

Each role is represented by a row in the table. Roles are listed in the table in ascending alphabetical order by role title, type (that is, whether the role is a predefined role or a custom role), description, and tasks assigned. You can show or hide table columns and sort records in ascending or descending order.

You can search for roles by typing the first letters of the role title in the search box. Role title starting with the first letters you type are listed.

To view a user role detail summary:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > Roles**.

The Roles page appears.

2. Double-click a role.

The Role Detail Summary page appears.

The page displays the workspace and workspace tasks.

3. Click the expander button + adjacent to the workspaces to view subtasks.
4. Click **OK** on the Role Detail Summary page to exit this page.

You are returned to the Roles page.

Performing Manage Roles Commands

You can perform a task on predefined and user-defined roles by selecting the task from the Actions menu or the shortcut menu that is displayed when you right-click a role, or by clicking the icons at the top of the Roles page. You can perform the **Modify Role** and **Delete Roles** commands only on read-writeable user-defined roles. You cannot manipulate read-only predefined roles. To perform a command, you must first select the role.

You can perform one or more of the following actions on the roles from the Roles page:

- **View Role Details**—View details about the selected role.
- **Modify Role**—Modify the selected user-defined description, application workspaces, and tasks associated with the workspaces. You cannot modify predefined roles. For more information, see *Modifying User-Defined Roles*.
- **Delete Roles**—Delete the selected user-defined role. You cannot delete predefined roles. For more information, see *Deleting User-Defined Roles*.
- **Clone Roles**—Clone the selected user-defined or predefined role. For more information, see *Cloning Predefined and User-Defined Roles*.
- **Tag It**—Tag one or more selected inventory objects, see, see *Tagging an Object*.
- **View Tags**—View a list of tags that exist on a selected inventory object. For more information, see *Viewing Tags for a Managed Object*.
- **Untag It**—Untag a tag that is applied to an inventory object. For more information, see *Untagging Objects*.
- **Delete Private Tags**—Delete tags that you created.
- **Clear All Selections**—Clear any role selections you made on the Roles inventory page.
- **Display Quick View**—Displays or hides a small window summarizing data about the selected object.

Related Documentation

- *Role-Based Access Control Overview*
- *Predefined Roles Overview*
- *Creating Users in Junos Space Network Management Platform*
- *Creating a User-Defined Role*
- *Modifying User-Defined Roles*
- *Deleting User-Defined Roles*

PART 19

Working with Tunnel Services

- [Tunnel Services Overview on page 1693](#)
- [Service Design and Provisioning: Managing and Deploying Tunnel Services on page 1719](#)
- [Monitoring and Troubleshooting Tunnel Services on page 1781](#)

Tunnel Services Overview

- [Tunnel Services Overview on page 1693](#)
- [Traffic Engineering Capabilities on page 1694](#)
- [Components of Traffic Engineering on page 1694](#)
- [Routers in an LSP on page 1697](#)
- [MPLS and RSVP Overview on page 1702](#)
- [Fast Reroute Overview on page 1704](#)
- [Point-to-Multipoint LSPs Overview on page 1706](#)
- [RSVP Operation Overview on page 1708](#)
- [Link Protection and Node Protection on page 1712](#)

Tunnel Services Overview

Transport or tunnel services allow you to design, provision, and deploy RSVP-signaled label-switched path (LSP) services that run from a specific ingress router to a specific egress router. You can configure end-to-end point-to-point and point-to-multiple-point LSPs.

A tunnel service automates and provides a user interface for LSP service deployment, including LSP-configured Juniper Networks device discovery from the Junos Space Platform database, LSP definition configuration design, and LSP service validation and deployment.

A tunnel service is integrated with and codependent upon network services, that provide Layer 2 and Layer 3 VPN service provisioning.

Provisioning an LSP service includes the following major tasks:

- Discover Juniper Networks devices that have been configured for MPLS-Signaled LSP into Junos Space using the Devices workspace. See the MPLS-Signaled LSP Configuration Guidelines in the *Junos OS MPLS Applications Configuration Guide*.
- Discover tunneling or transport devices from the Connectivity Services Director GUI in Service View of Build mode. In the **Network Services > Connectivity** task pane, select **Prestage Devices > Prestage Devices**. View the values displayed under the Roles column of the discovered devices.

Click **Manage Device Roles** and from the drop-down list, select **Discover Roles** to retrieve the roles of the devices. A dialog box is displayed with the job ID of the discovery job that is created to obtain the latest roles of the devices.

- Assign LSP roles to provide authorization for the LSP definition designer and service activator to provision LSP services. Select **Platform > Users**.
- Create an LSP definition to use to create an LSP service. Select **TA Design > Manage TA Definitions**.
- Create and validate LSP services. Select **Service Provisioning > Manage LSPs**. You can use LSP settings in the predefined LSP definition so that they are configurable in the LSP service order.

Related Documentation

Traffic Engineering Capabilities

The task of mapping traffic flows onto an existing physical topology is called *traffic engineering*. Traffic engineering provides the ability to move traffic flow away from the shortest path selected by the interior gateway protocol (IGP) and onto a potentially less congested physical path across a network.

Traffic engineering provides the capabilities to do the following:

- Route primary paths around known bottlenecks or points of congestion in the network.
- Provide precise control over how traffic is rerouted when the primary path is faced with single or multiple failures.
- Provide more efficient use of available aggregate bandwidth and long-haul fiber by ensuring that subsets of the network do not become overutilized while other subsets of the network along potential alternate paths are underutilized.
- Maximize operational efficiency.
- Enhance the traffic-oriented performance characteristics of the network by minimizing packet loss, minimizing prolonged periods of congestion, and maximizing throughput.
- Enhance statistically bound performance characteristics of the network (such as loss ratio, delay variation, and transfer delay) required to support a multiservices Internet.

Components of Traffic Engineering

In the Junos[®] operating system (OS), traffic engineering is implemented with MPLS and RSVP. Traffic engineering is composed of four functional components:

- [Packet Forwarding Component on page 1695](#)
- [Information Distribution Component on page 1696](#)
- [Path Selection Component on page 1696](#)
- [Signaling Component on page 1697](#)

Packet Forwarding Component

The packet forwarding component of the Junos traffic engineering architecture is MPLS, which is responsible for directing a flow of IP packets along a predetermined path across a network. This path is called a *label-switched path (LSP)*. LSPs are simplex; that is, the traffic flows in one direction from the head-end (ingress) router to a tail-end (egress) router. Duplex traffic requires two LSPs: one LSP to carry traffic in each direction. An LSP is created by the concatenation of one or more label-switched hops, allowing a packet to be forwarded from one router to another across the MPLS domain.

When an ingress router receives an IP packet, it adds an MPLS header to the packet and forwards it to the next router in the LSP. The labeled packet is forwarded along the LSP by each router until it reaches the tail end of the LSP, the egress router. At this point the MPLS header is removed, and the packet is forwarded based on Layer 3 information such as the IP destination address. The value of this scheme is that the physical path of the LSP is not limited to what the IGP would choose as the shortest path to reach the destination IP address.

Packet Forwarding Based on Label Swapping

The packet forwarding process at each router is based on the concept of label swapping. This concept is similar to what occurs at each Asynchronous Transfer Mode (ATM) switch in a permanent virtual circuit (PVC). Each MPLS packet carries a 4-byte encapsulation header that contains a 20-bit, fixed-length label field. When a packet containing a label arrives at a router, the router examines the label and copies it as an index to its MPLS forwarding table. Each entry in the forwarding table contains an interface-inbound label pair mapped to a set of forwarding information that is applied to all packets arriving on the specific interface with the same inbound label.

How a Packet Traverses an MPLS Backbone

This section describes how an IP packet is processed as it traverses an MPLS backbone network.

At the entry edge of the MPLS backbone, the IP header is examined by the ingress router. Based on this analysis, the packet is classified, assigned a label, encapsulated in an MPLS header, and forwarded toward the next hop in the LSP. MPLS provides a high degree of flexibility in the way that an IP packet can be assigned to an LSP. For example, in the Junos traffic engineering implementation, all packets arriving at the ingress router that are destined to exit the MPLS domain at the same egress router are forwarded along the same LSP.

Once the packet begins to traverse the LSP, each router uses the label to make the forwarding decision. The MPLS forwarding decision is made independently of the original IP header: the incoming interface and label are used as lookup keys into the MPLS forwarding table. The old label is replaced with a new label, and the packet is forwarded to the next hop along the LSP. This process is repeated at each router in the LSP until the packet reaches the egress router.

When the packet arrives at the egress router, the label is removed and the packet exits the MPLS domain. The packet is then forwarded based on the destination IP address

contained in the packet's original IP header according to the traditional shortest path calculated by the IP routing protocol.

Information Distribution Component

Traffic engineering requires detailed knowledge about the network topology as well as dynamic information about network loading. To implement the information distribution component, simple extensions to the IGPs are defined. Link attributes are included as part of each router's link-state advertisement. IS-IS extensions include the definition of new type length values (TLVs), whereas OSPF extensions are implemented with opaque link-state advertisements (LSAs). The standard flooding algorithm used by the link-state IGPs ensures that link attributes are distributed to all routers in the routing domain. Some of the traffic engineering extensions to be added to the IGP link-state advertisement include maximum link bandwidth, maximum reserved link bandwidth, current bandwidth reservation, and link coloring.

Each router maintains network link attributes and topology information in a specialized traffic engineering database. The traffic engineering database is used exclusively for calculating explicit paths for the placement of LSPs across the physical topology. A separate database is maintained so that the subsequent traffic engineering computation is independent of the IGP and the IGP's link-state database. Meanwhile, the IGP continues its operation without modification, performing the traditional shortest-path calculation based on information contained in the router's link-state database.

Path Selection Component

After network link attributes and topology information are flooded by the IGP and placed in the traffic engineering database, each ingress router uses the traffic engineering database to calculate the paths for its own set of LSPs across the routing domain. The path for each LSP can be represented by either a strict or loose explicit route. An explicit route is a preconfigured sequence of routers that should be part of the physical path of the LSP. If the ingress router specifies all the routers in the LSP, the LSP is said to be identified by a strict explicit route. If the ingress router specifies only some of the routers in the LSP, the LSP is described as a loose explicit route. Support for strict and loose explicit routes allows the path selection process to be given broad latitude whenever possible, but to be constrained when necessary.

The ingress router determines the physical path for each LSP by applying a Constrained Shortest Path First (CSPF) algorithm to the information in the traffic engineering database. CSPF is a shortest-path-first algorithm that has been modified to take into account specific restrictions when the shortest path across the network is calculated. Input into the CSPF algorithm includes:

- Topology link-state information learned from the IGP and maintained in the traffic engineering database
- Attributes associated with the state of network resources (such as total link bandwidth, reserved link bandwidth, available link bandwidth, and link color) that are carried by IGP extensions and stored in the traffic engineering database

- Administrative attributes required to support traffic traversing the proposed LSP (such as bandwidth requirements, maximum hop count, and administrative policy requirements) that are obtained from user configuration

As CSPF considers each candidate node and link for a new LSP, it either accepts or rejects a specific path component based on resource availability or whether selecting the component violates user policy constraints. The output of the CSPF calculation is an explicit route consisting of a sequence of router addresses that provides the shortest path through the network that meets the constraints. This explicit route is then passed to the signaling component, which establishes the forwarding state in the routers along the LSP.

Signaling Component

An LSP is not known to be workable until it is actually established by the signaling component. The signaling component, which is responsible for establishing LSP state and distributing labels, relies on a number of extensions to RSVP:

- The Explicit Route object allows an RSVP path message to traverse an explicit sequence of routers that is independent of conventional shortest-path IP routing. The explicit route can be either strict or loose.
- The Label Request object permits the RSVP path message to request that intermediate routers provide a label binding for the LSP that it is establishing.
- The Label object allows RSVP to support the distribution of labels without changing its existing mechanisms. Because the RSVP Resv message follows the reverse path of the RSVP path message, the Label object supports the distribution of labels from downstream nodes to upstream nodes.

Routers in an LSP

Each router in an LSP performs one of the following functions:

- Ingress router—The router at the beginning of an LSP. This router encapsulates IP packets with an MPLS Layer 2 frame and forwards it to the next router in the path. Each LSP can have only one ingress router.
- Egress router—The router at the end of an LSP. This router removes the MPLS encapsulation, thus transforming it from an MPLS packet to an IP packet, and forwards the packet to its final destination using information in the IP forwarding table. Each LSP can have only one egress router. The ingress and egress routers in an LSP cannot be the same router.
- Transit router—Any intermediate router in the LSP between the ingress and egress routers. A transit router forwards received MPLS packets to the next router in the MPLS path. An LSP can contain zero or more transit routers, up to a maximum of 253 transit routers in a single LSP.

A single router can be part of multiple LSPs. It can be the ingress or egress router for one or more LSPs, and it also can be a transit router in one or more LSPs. The functions that each router supports depend on your network design.

How a Packet Travels Along an LSP

When an IP packet enters an LSP, the ingress router examines the packet and assigns it a label based on its destination, placing the label in the packet's header. The label transforms the packet from one that is forwarded based on its IP routing information to one that is forwarded based on information associated with the label.

The packet is then forwarded to the next router in the LSP. This router and all subsequent routers in the LSP do not examine any of the IP routing information in the labeled packet. Rather, they use the label to look up information in their label forwarding table. They then replace the old label with a new label and forward the packet to the next router in the path.

When the packet reaches the egress router, the label is removed, and the packet again becomes a native IP packet and is again forwarded based on its IP routing information.

Types of LSPs

There are three types of LSPs:

- Static LSPs—For static paths, you must manually assign labels on all routers involved (ingress, transit, and egress). No signaling protocol is needed. This procedure is similar to configuring static routes on individual routers. Like static routes, there is no error reporting, liveliness detection, or statistics reporting.
- LDP-signaled LSPs—The Label Distribution Protocol (LDP) is a protocol for distributing labels in non-traffic-engineered applications. LDP allows routers to establish label-switched paths (LSPs) through a network by mapping network-layer routing information directly to data link layer-switched paths.

These LSPs might have an endpoint at a directly attached neighbor (comparable to IP hop-by-hop forwarding), or at a network egress node, enabling switching through all intermediary nodes. LSPs established by LDP can also traverse traffic-engineered LSPs created by RSVP.

LDP associates a forwarding equivalence class (FEC) with each LSP it creates. The FEC associated with an LSP specifies which packets are mapped to that LSP. LSPs are extended through a network as each router chooses the label advertised by the next hop for the FEC and splices it to the label it advertises to all other routers. This process forms a tree of LSPs that converge on the egress router.

- RSVP-signaled LSPs—For signaled paths, RSVP is used to set up the path and dynamically assign labels. (RSVP signaling messages are used to set up signaled paths.) You configure only the ingress router. The transit and egress routers accept signaling information from the ingress router, and they set up and maintain the LSP cooperatively. Any errors encountered while establishing an LSP are reported to the ingress router for diagnostics. For signaled LSPs to work, a version of RSVP that supports tunnel extensions must be enabled on all routers.

There are two types of RSVP-signaled LSPs:

- Explicit-path LSPs—All intermediate hops of the LSP are manually configured. The intermediate hops can be strict, loose, or any combination of the two. Explicit path LSPs provide you with complete control over how the path is set up. They are similar to static LSPs but require much less configuration.
- Constrained-path LSPs—The intermediate hops of the LSP are automatically computed by the software. The computation takes into account information provided by the topology information from the IS-IS or OSPF link-state routing protocol, the current network resource utilization determined by RSVP, and the resource requirements and constraints of the LSP. For signaled constrained-path LSPs to work, either the IS-IS or OSPF protocol and the IS-IS or OSPF traffic engineering extensions must be enabled on all routers.

Scope of LSPs

For constrained-path LSPs, the LSP computation is confined to one IGP domain, and cannot cross any AS boundary. This prevents an AS from extending its IGP into another AS.

Explicit-path LSPs, however, can cross as many AS boundaries as necessary. Because intermediate hops are manually specified, the LSP does not depend on the IGP topology or a local forwarding table.

Constrained-Path LSP Computation

The Constrained Shortest Path First (CSPF) algorithm is an advanced form of the shortest-path-first (SPF) algorithm used in OSPF and IS-IS route computations. CSPF is used in computing paths for LSPs that are subject to multiple constraints. When computing paths for LSPs, CSPF considers not only the topology of the network, but also the attributes of the LSP and the links, and it attempts to minimize congestion by intelligently balancing the network load.

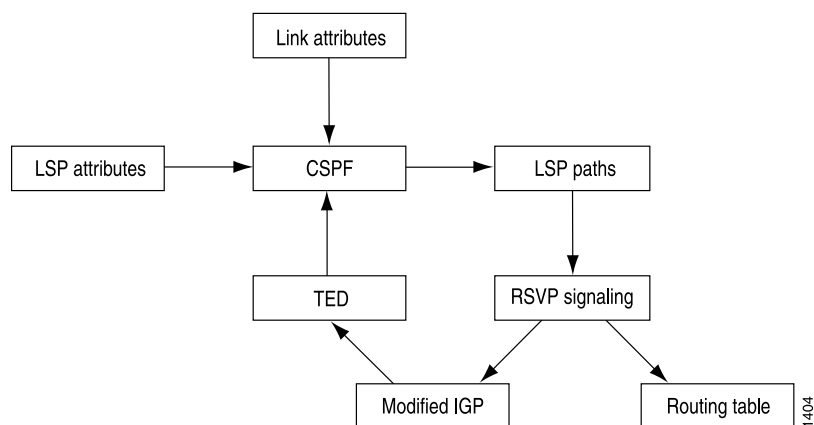
The constraints that CSPF considers include:

- LSP attributes
 - Administrative groups (that is, link color requirements)
 - Bandwidth requirements
 - Explicit route (strict or loose)
 - Hop limitations
 - Priority (setup and hold)
- Link attributes
 - Administrative groups (that is, link colors assigned to the link)
 - Reservable bandwidth of the links (static bandwidth minus the currently reserved bandwidth)

The data that CSPF considers comes from the following sources:

- Traffic engineering database—Provides CSPF with up-to-date topology information, the current reservable bandwidth of links, and the link colors. For the CSPF algorithm to perform its computations, a link-state IGP (such as OSPF or IS-IS) with special extensions is needed. For CSPF to be effective, the link-state IGP on all routers must support the special extensions. While building the topology database, the extended IGP must take into consideration the current LSPs and must flood the route information everywhere. Because changes in the reserved link bandwidth and link color cause database updates, an extended IGP tends to flood more frequently than a normal IGP. See [Figure 125 on page 1700](#) for a diagram of the relationships between these components.
- Currently active LSPs—Includes all the LSPs that should originate from the router and their current operational status (up, down, or timeout).

Figure 125: CSPF Computation Process



How CSPF Selects a Path

To select a path, CSPF follows certain rules. The rules are as follows:

1. Computes LSPs one at a time, beginning with the highest priority LSP (the one with the lowest setup priority value). Among LSPs of equal priority, CSPF services the LSPs in alphabetical order of the LSP names.
2. Prunes the traffic engineering database of all the links that are not full duplex and do not have sufficient reservable bandwidth.
3. If the LSP configuration includes the **include** statement, prunes all links that do not share any included colors.
4. If the LSP configuration includes the **exclude** statement, prunes all links that contain excluded colors. If the link does not have a color, it is accepted.
5. If several paths have equal cost, chooses the one whose last-hop address is the same as the LSP's destination.

6. If several equal cost paths remain, selects the one with the fewest number of hops.
7. If several equal-cost paths remain, applies the CSPF load-balancing rule configured on the LSP (least fill, most fill, or random).

CSPF finds the shortest path toward the LSP's egress router, taking into account explicit-path constraints. For example, if the path must pass through Router A, two separate SPF computations are performed, one from the ingress router to Router A, the other from Router A to the egress router. All CSPF rules are applied to both computations.

CSPF Path Selection Tie-Breaking

If more than one path is still available after the CSPF rules have been applied, a tie-breaking rule is applied to choose the path for the LSP. The rule used depends on the configuration. There are three tie-breaking rules:

- Random—One of the remaining paths is picked at random. This rule tends to place an equal number of LSPs on each link, regardless of the available bandwidth ratio. This is the default behavior.
- Least fill—The path with the largest minimum available bandwidth ratio is preferred. This rule tries to equalize the reservation on each link.
- Most fill—The path with the smallest minimum available bandwidth ratio is preferred. This rule tries to fill a link before moving on to alternative links.

The following definitions describe how a figure for minimum available bandwidth ratio is derived for the least fill and most fill rules:

- Reservable bandwidth = bandwidth of link x subscription factor of link
- Available bandwidth = reservable bandwidth – (sum of the bandwidths of the LSPs traversing the link)
- Available bandwidth ratio = available bandwidth/reservable bandwidth
- Minimum available bandwidth ratio (for a path) = the smallest available bandwidth ratio of the links in a path



NOTE: For the least fill or most fill behaviors to be used, the paths must have their bandwidth (specified using the `bandwidth` statement at the `[edit protocols mpls label-switched-path lsp-name]` hierarchy level) or minimum bandwidth (specified using the `minimum-bandwidth` statement at the `[edit protocols mpls label-switched-path lsp-name auto-bandwidth]` hierarchy level) configured to a value greater than 0. If the bandwidth or minimum bandwidth for the paths is either not configured or configured as 0, the minimum available bandwidth cannot be calculated and the random path selection behavior is used instead.

Computing CSPF Paths Offline

The Junos OS provides online, real-time CSPF computation only; each router performs CSPF calculations independent of the other routers in the network. These calculations are based on currently available topology information—information that is usually recent, but not completely accurate. LSP placements are locally optimized, based on current network status.

To optimize links globally across the network, you can use an offline tool to perform the CSPF calculations and determine the paths for the LSPs. You can create such a tool yourself, or you can modify an existing network design tool to perform these calculations. You should run the tool periodically (daily or weekly) and download the results into the router. An offline tool should take the following into account when performing the optimized calculations:

- All the LSP's requirements
- All link attributes
- Complete network topology

MPLS and RSVP Overview

MPLS provides a mechanism for engineering network traffic patterns that is independent of routing tables. MPLS assigns short labels to network packets that describe how to forward them through the network. MPLS is independent of any routing protocol and can be used for unicast packets.

In the traditional Level 3 forwarding paradigm, as a packet travels from one router to the next, an independent forwarding decision is made at each hop. The IP network layer header is analyzed, and the next hop is chosen based on this analysis and on the information in the routing table. In an MPLS environment, the analysis of the packet header is performed just once, when a packet enters the MPLS cloud. The packet is then assigned to a stream, which is identified by a *label*, which is a short (20-bit), fixed-length value at the front of the packet. Labels are used as lookup indexes for the label forwarding table. For each label, this table stores forwarding information. You can associate additional information with a label—such as class-of-service (CoS) values—that can be used to prioritize packet forwarding.

Packets traveling along an LSP are identified by a label—a 20-bit, unsigned integer in the range 0 through 1,048,575. For push labels on ingress routers, no labels in this range are restricted. For incoming labels on the transit static LSP, the label value is restricted to 1,000,000 through 1,048,575.

On MX Series, PTX Series, and T Series routers, the value for entropy and flow labels is restricted to 16 through 1,048,575.

In the Junos OS, label values are allocated per router. The display output shows only the label (for example, **01024**). Labels for multicast packets are independent of those for unicast packets. Currently, the Junos OS does not support multicast labels.

Labels are assigned by downstream routers relative to the flow of packets. A router receiving labeled packets (the next-hop router) is responsible for assigning incoming labels. A received packet containing a label that is unrecognized (unassigned) is dropped. For unrecognized labels, the router does not attempt to unwrap the label to analyze the network layer header, nor does it generate an Internet Control Message Protocol (ICMP) destination unreachable message.

A packet can carry a number of labels, organized as a last-in, first-out stack. This is referred to as a *label stack*. At a particular router, the decision about how to forward a labeled packet is based exclusively on the label at the top of the stack.

Figure 126 on page 1703 shows the encoding of a single label. The encoding appears after data link layer headers, but before any network layer header.

Figure 126: Label Encoding

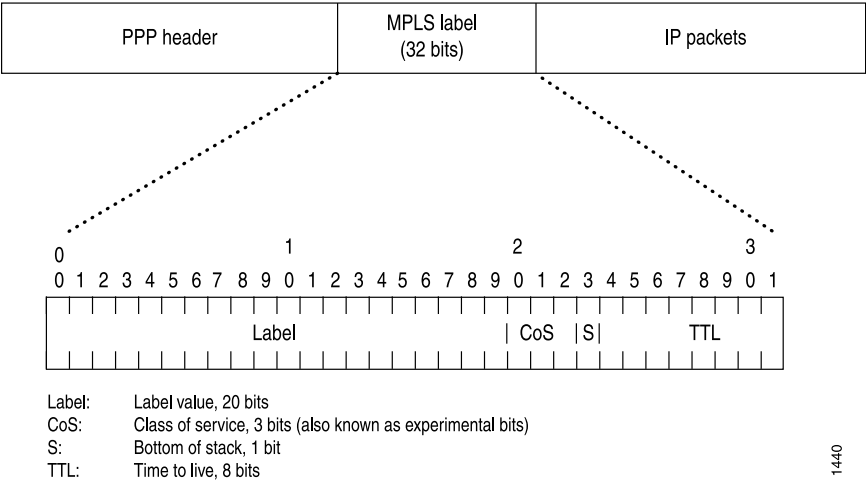
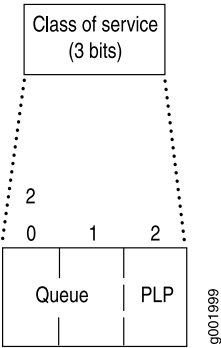


Figure 127 on page 1703 illustrates the purpose of the class-of-service bits (also known as the EXP or experimental bits). Bits 20 and 21 specify the queue number. Bit 22 is the packet loss priority (PLP) bit used to specify the random early detection (RED) drop profile.

Figure 127: Class-of-Service Bits



RSVP Overview

RSVP is a resource reservation setup protocol that is used by both network hosts and routers. Hosts use RSVP to request a specific class of service (CoS) from the network for particular application flows. Routers use RSVP to deliver CoS requests to all routers along the data path. RSVP also can maintain and refresh states for a requested CoS application flow.

RSVP treats an application flow as a simplex connection. That is, the CoS request travels only in one direction—from the sender to the receiver. RSVP is a transport layer protocol that uses IP as its network layer. However, RSVP does not transport application flows. Rather, it is more of an Internet control protocol, similar to the Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP). RSVP runs as a separate software process in the Junos OS and is not in the packet forwarding path.

RSVP is not a routing protocol, but rather is designed to operate with current and future unicast and multicast routing protocols. The routing protocols are responsible for choosing the routes to use to forward packets, and RSVP consults local routing tables to obtain routes. RSVP only ensures the CoS of packets traveling along a data path.

The receiver in an application flow requests the preferred CoS from the sender. To do this, the receiver issues an RSVP CoS request on behalf of the local application. The request propagates to all routers in reverse direction of the data paths toward the sender. In this process, RSVP requests might be merged, resulting in a protocol that scales well when there are a large number of receivers.

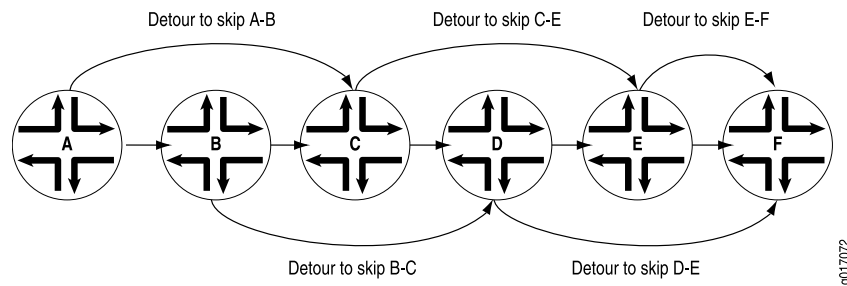
Because the number of receivers in an application flow is likely to change and the flow of delivery paths might change during the life of an application flow, RSVP takes a soft-state approach in its design, creating and removing the protocol states in routers and hosts incrementally over time. RSVP sends periodic refresh messages to maintain its state and to recover from occasional lost messages. In the absence of refresh messages, RSVP states automatically time out and are deleted.

Related •
Documentation

Fast Reroute Overview

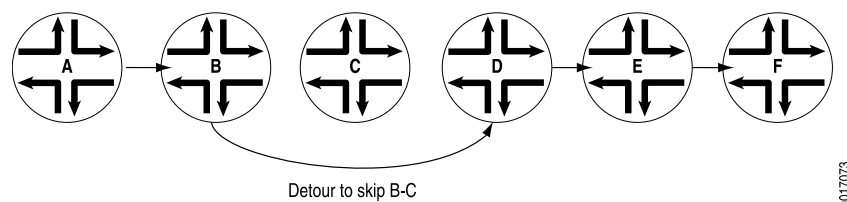
Fast reroute provides redundancy for an LSP path. When you enable fast reroute, detours are precomputed and preestablished along the LSP. In case of a network failure on the current LSP path, traffic is quickly routed to one of the detours. [Figure 128 on page 1705](#) illustrates an LSP from Router A to Router F, showing the established detours. Each detour is established by an upstream node to avoid the link toward the immediate downstream node and the immediate downstream node itself. Each detour might traverse through one or more label-switched routers (or switches) that are not shown in the figure.

Fast reroute protects traffic against any single point of failure between the ingress and egress routers (or switches). If there are multiple failures along an LSP, fast reroute itself might fail. Also, fast reroute does not protect against failure of the ingress or egress routers.

Figure 128: Detours Established for an LSP Using Fast Reroute

If a node detects that a downstream link has failed (using a link-layer-specific liveness detection mechanism) or that a downstream node has failed (for example, using the RSVP neighbor hello protocol), the node quickly switches the traffic to the detour and, at the same time, signals the ingress router about the link or node failure.

[Figure 129 on page 1705](#) illustrates the detour taken when the link between Router B and Router C fails.

Figure 129: Detour After the Link from Router B to Router C Fails

If the network topology is not rich enough (there are not enough routers with sufficient links to other routers), some of the detours might not succeed. For example, the detour from Router A to Router C in [Figure 128 on page 1705](#) cannot traverse link A-B and Router B. If such a path is not possible, the detour does not occur.

Note that after the node switches traffic to the detour, it might switch the traffic again to a newly calculated detour soon after. This is because the initial detour route might not be the best route. To make rerouting as fast as possible, the node switches traffic onto the initial detour without first verifying that the detour is valid. Once the switch is made, the node recomputes the detour. If the node determines that the initial detour is still valid, traffic continues to flow over this detour. If the node determines that the initial detour is no longer valid, it again switches the traffic to a newly computed detour.



NOTE: If you issue `show` commands after the node has switched traffic to the initial detour, the node might indicate that the traffic is still flowing over the original LSP. This situation is temporary and should correct itself quickly.

The time required for a fast-rerouting detour to take effect depends on two independent time intervals:

- Amount of time to detect that there is a link or node failure—This interval depends greatly on the link layer in use and the nature of the failure. For example, failure detection

on an SONET/SDH link typically is much faster than on a Gigabit Ethernet link, and both are much faster than detection of a router failure.

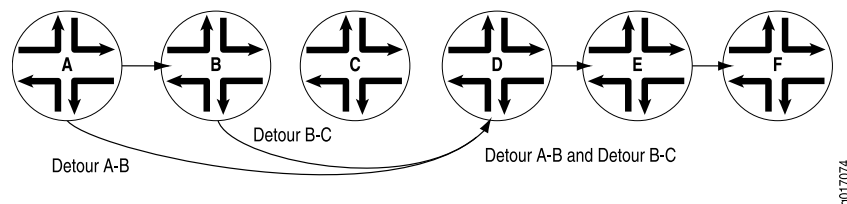
- Amount of time required to splice the traffic onto the detour—This operation is performed by the Packet Forwarding Engine, which requires little time to splice traffic onto the detour. The time needed can vary depending on the number of LSPs being switched to detours.

Fast reroute is a short-term patch to reduce packet loss. Because detour computation might not reserve adequate bandwidth, the detours might introduce congestion on the alternate links. The ingress router is the only router that is fully aware of LSP policy constraints and, therefore, is the only router able to come up with adequate long-term alternate paths.

Detours are created by use of RSVP and, like all RSVP sessions, they require extra state and overhead in the network. For this reason, each node establishes at most one detour for each LSP that has fast reroute enabled. Creating more than one detour for each LSP increases the overhead, but serves no practical purpose.

To reduce network overhead further, each detour attempts to merge back into the LSP as soon as possible after the failed node or link. If you can consider an LSP that travels through n router nodes, it is possible to create $n - 1$ detours. For instance, in [Figure 130 on page 1706](#), the detour tries to merge back into the LSP at Router D instead of at Router E or Router F. Merging back into the LSP makes the detour scalability problem more manageable. If topology limitations prevent the detour from quickly merging back into the LSP, detours merge with other detours automatically.

Figure 130: Detours Merging into Other Detours



Point-to-Multipoint LSPs Overview

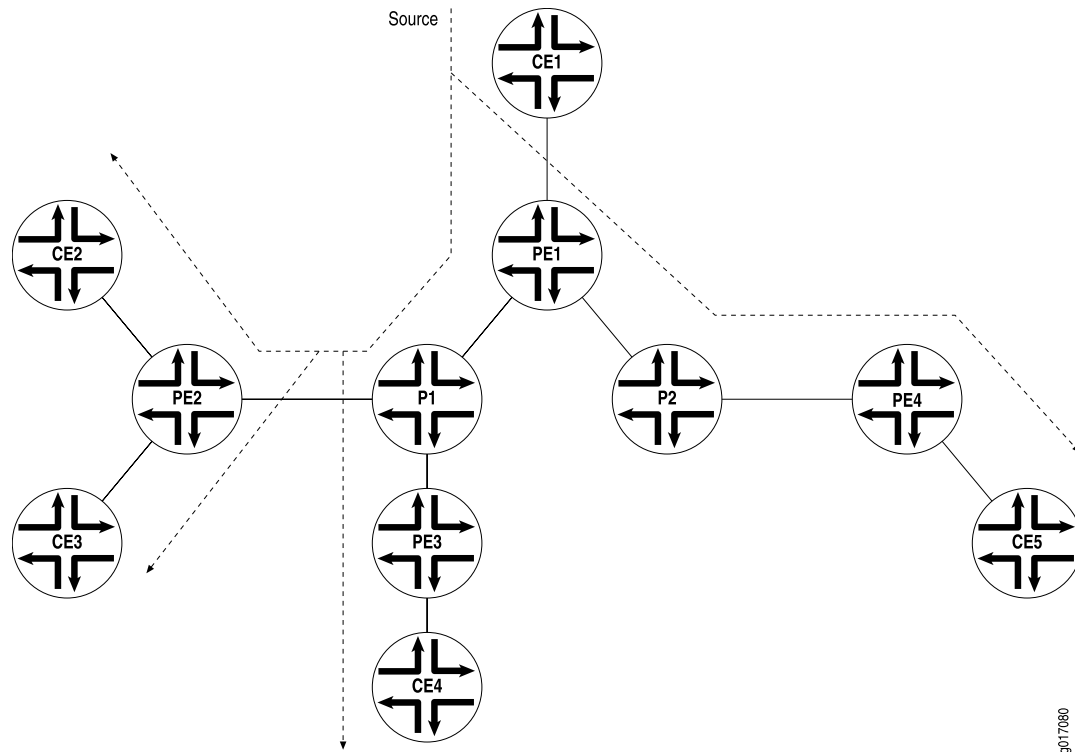
A point-to-multipoint MPLS LSP is an LSP with a single source and multiple destinations. By taking advantage of the MPLS packet replication capability of the network, point-to-multipoint LSPs avoid unnecessary packet replication at the ingress router. Packet replication takes place only when packets are forwarded to two or more different destinations requiring different network paths.

This process is illustrated in [Figure 131 on page 1707](#). Router PE1 is configured with a point-to-multipoint LSP to Routers PE2, PE3, and PE4. When Router PE1 sends a packet on the point-to-multipoint LSP to Routers P1 and P2, Router P1 replicates the packet and forwards it to Routers PE2 and PE3. Router P2 sends the packet to Router PE4.

This feature is described in detail in the Internet drafts [draft-raggarwa-mpls-p2mp-te-02.txt](#) (expired February 2004), *Establishing Point to Multipoint MPLS TE LSPs*, [draft-ietf-mpls-rsvp-te-p2mp-02.txt](#), *Extensions to Resource*

Reservation Protocol-Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label-Switched Paths (LSPs), and RFC 6388, Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths (only point-to-multipoint LSPs are supported).

Figure 131: Point-to-Multipoint LSPs



The following are some of the properties of point-to-multipoint LSPs:

- A point-to-multipoint LSP enables you to use MPLS for point-to-multipoint data distribution. This functionality is similar to that provided by IP multicast.
- You can add and remove branch LSPs from a main point-to-multipoint LSP without disrupting traffic. The unaffected parts of the point-to-multipoint LSP continue to function normally.
- You can configure a node to be both a transit and an egress router for different branch LSPs of the same point-to-multipoint LSP.
- You can enable link protection on a point-to-multipoint LSP. Link protection can provide a bypass LSP for each of the branch LSPs that make up the point-to-multipoint LSP. If any of the primary paths fail, traffic can be quickly switched to the bypass.
- You can configure branch LSPs either statically, dynamically, or as a combination of static and dynamic LSPs.
- You can enable graceful Routing Engine switchover (GRES) and graceful restart for point-to-multipoint LSPs at ingress and egress routers. The point-to-multipoint LSPs must be configured using either static routes or circuit cross-connect (CCC). GRES and graceful restart allow the traffic to be forwarded at the Packet Forwarding Engine

based on the old state while the control plane recovers. Feature parity for GRES and graceful restart for MPLS point-to-multipoint LSPs on the Junos Trio chipset is supported in Junos OS Releases 11.1R2, 11.2R2, and 11.4.

RSVP Operation Overview

A Resource Reservation Protocol (RSVP) label-switched path (LSP) tunnel enables you to send RSVP LSPs inside other RSVP LSPs. This enables a network administrator to provide traffic engineering from one end of the network to the other. A useful application for this feature is to connect customer edge (CE) routers with provider edge (PE) routers by using an RSVP LSP, and then tunnel this edge LSP inside a second RSVP LSP traveling across the network core.

You should have a general understanding of MPLS and label switching concepts. For more information about MPLS, see the *Junos MPLS Applications Configuration Guide*.

An RSVP LSP tunnel adds the concept of a forwarding adjacency, similar to the one used for generalized Multiprotocol Label Switching (GMPLS).

The forwarding adjacency creates a tunneled path for sending data between peer devices in an RSVP LSP network. Once a forwarding adjacency LSP (FA-LSP) has been established, other LSPs can be sent over the FA-LSP by using Constrained Shortest Path First (CSPF), Link Management Protocol (LMP), Open Shortest Path First (OSPF), and RSVP.

To enable an RSVP LSP tunnel, the Junos OS uses the following mechanisms:

- LMP—Originally designed for GMPLS, LMP establishes forwarding adjacencies between RSVP LSP tunnel peers, and maintains and allocates resources for traffic engineering links.
- OSPF extensions—OSPF was designed to route packets to physical and logical interfaces related to a Physical Interface Card (PIC). This protocol has been extended to route packets to virtual peer interfaces defined in an LMP configuration.
- RSVP-TE extensions—RSVP-TE was designed to signal the setup of packet LSPs to physical interfaces. The protocol has been extended to request path setup for packet LSPs traveling to virtual peer interfaces defined in an LMP configuration.

The following limitations exist for LSP hierarchies:

- Circuit cross-connect (CCC)-based LSPs are not supported.
- Graceful restart is not supported.
- Link protection is not available for FA-LSPs or at the egress point of the forwarding adjacency.
- Point-to-multipoint LSPs are not supported across FA-LSPs.

RSVP creates independent sessions to handle each data flow. A session is identified by a combination of the destination address, an optional destination port, and a protocol. Within a session, there can be one or more senders. Each sender is identified by a

combination of its source address and source port. An out-of-band mechanism, such as a session announcement protocol or human communication, is used to communicate the session identifier to all senders and receivers.

A typical RSVP session involves the following sequence of events:

1. A potential sender starts sending RSVP path messages to the session address.
2. A receiver, wanting to join the session, registers itself if necessary. For example, a receiver in a multicast application would register itself with IGMP.
3. The receiver receives the path messages.
4. The receiver sends appropriate Resv messages toward the sender. These messages carry a flow descriptor, which is used by routers along the path to make reservations in their link-layer media.
5. The sender receives the Resv message and then starts sending application data.

This sequence of events is not necessarily strictly synchronized. For example, receivers can register themselves before receiving path messages from the sender, and application data can flow before the sender receives Resv messages. Application data that is delivered before the actual reservation contained in the Resv message typically is treated as best-effort, non-real-time traffic with no CoS guarantee.

RSVP Hello Packets and Timers

RSVP monitors the status of the interior gateway protocol (IGP) (IS-IS or OSPF) neighbors and relies on the IGP protocols to detect when a node fails. If an IGP protocol declares a neighbor down (because hello packets are no longer being received), RSVP also brings down that neighbor. However, the IGP protocols and RSVP still act independently when bringing a neighbor up.

In the Junos OS, RSVP typically relies on IGP hello packet detection to check for node failures. RSVP sessions are kept up even if RSVP hello packets are no longer being received, so long as the router continues to receive IGP hello packets. RSVP sessions are maintained until either the router stops receiving IGP hello packets or the RSVP Path and Resv messages time out. Configuring a short time for the IS-IS or OSPF hello timers allows these protocols to detect node failures quickly.

RSVP hellos can be relied on when the IGP does not recognize a particular neighbor (for example, if IGP is not enabled on the interface) or if the IGP is RIP (not IS-IS or OSPF). Also, the equipment of other vendors might be configured to monitor RSVP sessions based on RSVP hello packets. This equipment might also take an RSVP session down due to a loss of RSVP hello packets.

We do not recommend configuring a short RSVP hello timer. If quick discovery of a failed neighbor is needed, configure short IGP (OSPF or IS-IS) hello timers.

OSPF and IS-IS have infrastructure to manage rapid hello message sending and receiving reliably, even if the routing protocols or some other process are straining the processing capability of the router. Under the same circumstances, RSVP hellos might time out prematurely even though the neighbor is functioning normally.

RSVP Message Types

RSVP uses the following types of messages to establish and remove paths for data flows, establish and remove reservation information, confirm the establishment of reservations, and report errors:

- [Path Messages on page 1710](#)
- [Resv Messages on page 1710](#)
- [PathTear Messages on page 1710](#)
- [ResvTear Messages on page 1711](#)
- [PathErr Messages on page 1711](#)
- [ResvErr Messages on page 1711](#)
- [ResvConfirm Messages on page 1711](#)

Path Messages

Each sender host transmits path messages downstream along the routes provided by the unicast and multicast routing protocols. Path messages follow the exact paths of application data, creating path states in the routers along the way, thus enabling routers to learn the previous-hop and next-hop node for the session. Path messages are sent periodically to refresh path states.

The refresh interval is controlled by a variable called the **refresh-time**, which is the periodical refresh timer expressed in seconds. A path state times out if a router does not receive a specified number of consecutive path messages. This number is specified by a variable called **keep-multiplier**. Path states are kept for $(\text{keep-multiplier} + 0.5) \times 1.5 \times \text{refresh-time}$ seconds.

Resv Messages

Each receiver host sends reservation request (Resv) messages upstream toward senders and sender applications. Resv messages must follow exactly the reverse path of path messages. Resv messages create and maintain a reservation state in each router along the way.

Resv messages are sent periodically to refresh reservation states. The refresh interval is controlled by the same refresh time variable, and reservation states are kept for $(\text{keep-multiplier} + 0.5) \times 1.5 \times \text{refresh-time}$ seconds.

PathTear Messages

PathTear messages remove (tear down) path states as well as dependent reservation states in any routers along a path. PathTear messages follow the same path as path messages. A PathTear typically is initiated by a sender application or by a router when its path state times out.

PathTear messages are not required, but they enhance network performance because they release network resources quickly. If PathTear messages are lost or not generated, path states eventually time out when they are not refreshed, and the resources associated with the path are released.

ResvTear Messages

ResvTear messages remove reservation states along a path. These messages travel upstream toward senders of the session. In a sense, ResvTear messages are the reverse of Resv messages. ResvTear messages typically are initiated by a receiver application or by a router when its reservation state times out.

ResvTear messages are not required, but they enhance network performance because they release network resources quickly. If ResvTear messages are lost or not generated, reservation states eventually time out when they are not refreshed, and the resources associated with the reservation are released.

PathErr Messages

When path errors occur (usually because of parameter problems in a path message), the router sends a unicast PathErr message to the sender that issued the path message. PathErr messages are advisory; these messages do not alter any path state along the way.

ResvErr Messages

When a reservation request fails, a ResvErr error message is delivered to all the receivers involved. ResvErr messages are advisory; these messages do not alter any reservation state along the way.

ResvConfirm Messages

Receivers can request confirmation of a reservation request, and this confirmation is sent with a ResvConfirm message. Because of the complex RSVP flow-merging rules, a confirmation message does not necessarily provide end-to-end confirmation of the entire path. Therefore, ResvConfirm messages are an indication, not a guarantee, of potential success.

Juniper Networks routers never request confirmation using the ResvConfirm message; however, a Juniper Networks router can send a ResvConfirm message if it receives a request from another vendor's equipment.

MTU Signaling in RSVP

The maximum transmission unit (MTU) is the largest size packet or frame, in bytes, that can be sent in a network. An MTU that is too large might cause retransmissions. Too small an MTU might cause the router to send and handle relatively more header overhead and acknowledgments. There are default values for MTUs associated with various protocols. You can also explicitly configure an MTU on an interface.

When an LSP is created across a set of links with different MTU sizes, the ingress router does not know what the smallest MTU is on the LSP path. By default, the MTU for an LSP is 1,500 bytes.

If this MTU is larger than the MTU of one of the intermediate links, traffic might be dropped, because MPLS packets cannot be fragmented. Also, the ingress router is not aware of this type of traffic loss, because the control plane for the LSP would still function normally.

To prevent this type of packet loss in MPLS LSPs, you can configure MTU signaling in RSVP. This feature is described in RFC 3209. Juniper Networks supports the Integrated Services object for MTU signaling in RSVP. The Integrated Services object is described in RFCs 2210 and 2215. MTU signaling in RSVP is disabled by default.

To avoid packet loss due to MTU mismatches, the ingress router needs to do the following:

- Signal the MTU on the RSVP LSP—To prevent packet loss from an MTU mismatch, the ingress router needs to know what the smallest MTU value is along the path taken by the LSP. Once this MTU value is obtained, the ingress router can assign it to the LSP.
- Fragment packets—Using the assigned MTU value, packets that exceed the size of the MTU can be fragmented into smaller packets on the ingress router before they are encapsulated in MPLS and sent over the RSVP-signaled LSP.

Once both MTU signaling and packet fragmentation have been enabled on an ingress router, any route resolving to an RSVP LSP on this router uses the signaled MTU value.

The following are limitations to MTU signaling in RSVP:

- Changes in the MTU value might cause a temporary loss of traffic in the following situations:
 - For link protection and node protection, the MTU of the bypass is only signaled at the time the bypass becomes active. During the time it takes for the new path MTU to be propagated, packet loss might occur because of an MTU mismatch.
 - For fast reroute, the MTU of the path is updated only after the detour becomes active, causing a delay in an update to the MTU at the ingress router. Until the MTU is updated, packet loss might occur if there is an MTU mismatch.

In both cases, only packets that are larger than the detour or bypass MTU are lost.

- When an MTU is updated, it triggers a change in the next hop. Any change in the next hop causes the route statistics to be lost.
- The minimum MTU supported for MTU signaling in RSVP is 1,488 bytes. This value prevents a false or incorrectly configured value from being used.
- For single-hop LSPs, the MTU value displayed by the **show** commands is the RSVP-signaled value. However, this MPLS value is ignored and the correct IP value is used.

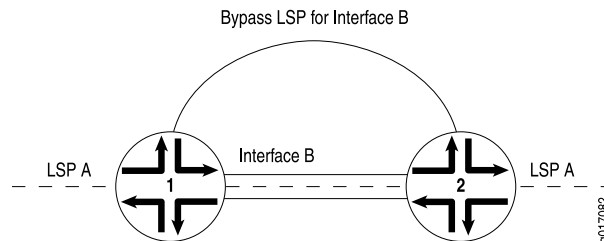
Link Protection and Node Protection

Link protection helps to ensure that traffic going over a specific interface to a neighboring router or switch can continue to reach this router (switch) if that interface fails. When link protection is configured for an interface and an LSP that traverses this interface, a bypass LSP is created that will handle this traffic if the interface fails. The bypass LSP uses a different interface and path to reach the same destination. The path used can be configured explicitly, or you can rely on CSPF. The RSVP metric for the bypass LSP is set in the range of 20,000 through 29,999 (this value is not user configurable).

If a link-protected interface fails, traffic is quickly switched to the bypass LSP. Note that a bypass LSP cannot share the same egress interface with the LSPs it monitors.

In [Figure 132 on page 1713](#), link protection is enabled on Interface B between Router 1 and Router 2. It is also enabled on LSP A, an LSP that traverses the link between Router 1 and Router 2. If the link between Router 1 and Router 2 fails, traffic from LSP A is quickly switched to the bypass LSP generated by link protection.

Figure 132: Link Protection Creating a Bypass LSP for the Protected Interface



Although LSPs traversing an interface can be configured to take advantage of link protection, it is important to note that it is specifically the interface that benefits from link protection. If link protection is enabled on an interface but not on a particular LSP traversing that interface, then if the interface fails, that LSP will also fail.



NOTE: Link protection does not work on unnumbered interfaces.

Node Protection

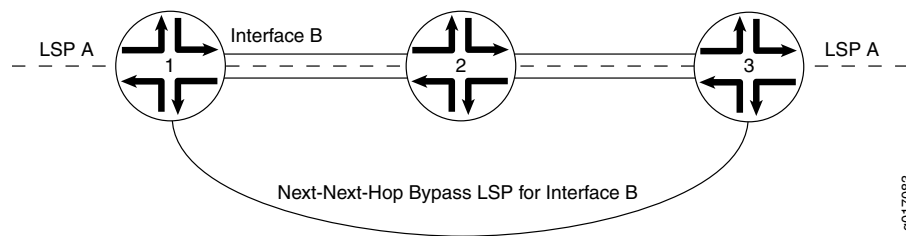
Node protection extends the capabilities of link protection. Link protection helps to ensure that traffic going over a specific interface to a neighboring router can continue to reach this router if that interface fails. Node protection ensures that traffic from an LSP traversing a neighboring router can continue to reach its destination even if the neighboring router fails.

When you enable node protection for an LSP, you must also enable link protection. Once enabled, node protection and link protection establish the following types of bypass LSPs:

- Next-hop bypass LSP—Provides an alternate route for an LSP to reach a neighboring router. This type of bypass LSP is established when you enable either node protection or link protection.
- Next-next-hop bypass LSP—Provides an alternate route for an LSP to get around a neighboring router en route to the destination router. This type of bypass LSP is established exclusively when node protection is configured. If a next-next-hop bypass LSP cannot be created, an attempt is made to signal a next-hop bypass LSP.

In [Figure 133 on page 1714](#), node protection is enabled on Interface B on Router 1. Node protection is also enabled on LSP A, an LSP that traverses the link transiting Router 1, Router 2, and Router 3. If Router 2 suffers a hardware or software failure, traffic from LSP A is switched to the next-next-hop bypass LSP generated by node protection.

Figure 133: Node Protection Creating a Next-Next-Hop Bypass LSP



The time needed by node protection to switch traffic to a next-next-hop bypass LSP can be significantly longer than the time needed by link protection to switch traffic to a next-hop bypass LSP. Link protection relies on a hardware mechanism to detect a link failure, allowing it to quickly switch traffic to a next-hop bypass LSP.

Node failures are often due to software problems on the node router. Node protection relies on the receipt of hello messages from a neighboring router to determine whether it is still functioning. The time it takes node protection to divert traffic partly depends on how often the node router sends hello messages and how long it takes the node-protected router to react to having not received a hello message. However, once the failure is detected, traffic can be quickly diverted to the next-next-hop bypass LSP.



NOTE:

Node protection provides traffic protection in the event of an error or interruption of the physical link between two routers. It does not provide protection in the event of control plane errors. The following provides an example of a control plane error:

- A transit router changes the label of a packet due to a control plane error.
- When the ingress router receives the packet, it considers the label change to be a catastrophic event and deletes both the primary LSP and the associated bypass LSP.

LSP Protection Overview

RSVP-TE extensions establish backup label-switched path (LSP) tunnels for local repair of LSP tunnels. These mechanisms enable immediate re-direction of traffic onto backup LSP tunnels, in the event of a failure.

RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*, describes two different types of traffic protection for RSVP-signaled LSPs:

- One-to-one backup—In this method, detour LSPs for each protected LSP is created at each potential point of local repair.
- Facility backup—In this method, a bypass tunnel is created to protect a set of LSPs that have similar backup constraints at a potential failure point, by taking advantage of the MPLS label stacking.

The one-to-one backup and the facility backup methods protect links and nodes during network failure, and can co-exist in a mixed network.

LSP Protection Types Comparison

In the Junos OS, the one-to-one backup of traffic protection is provided by fast reroute. Each LSP requires a protecting LSP to be signaled at each hop except the egress router. This method of LSP protection cannot be shared.

In the facility backup method, the LSP traffic protection is provided on the node and link. Each LSP requires a protecting LSP to be signaled at each hop except the egress router. Unlike fast reroute, this protecting LSP can be shared by other LSPs.

Table 248 on page 1715 summarizes the traffic protection types.

Table 248: One-to-One Backup Compared with Facility Backup

Comparison	One-to-One Backup	Facility Backup
Name of the protecting LSP	Detour LSP	Bypass LSP
Sharing of the protecting LSP	Cannot be shared	Can be shared by multiple LSPs
Junos configuration statements	fast-reroute	node-link-protection and link-protection

One-to-One Backup Implementation

In the one-to-one backup method, the points of local repair maintain separate backup paths for each LSP passing through a facility. The backup path terminates by merging back with the primary path at a node called the merge point. In this approach, the merge point can be any node downstream from the protected facility.

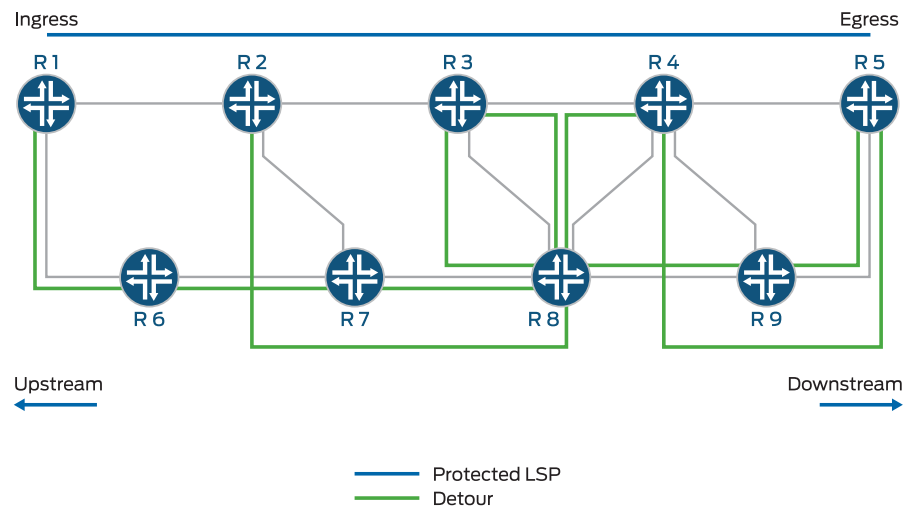
In the one-to-one backup method, an LSP is established that intersects the original LSP downstream of the point of link or node failure. A separate backup LSP is established for each LSP that is backed up.

One-to-one backup is appropriate under the following circumstances:

- Protection of a small number of LSPs relative to the total number of LSPs.
- Path selection criteria, such as bandwidth, priority, and link coloring for detour paths is critical.
- Control of individual LSPs is important.

In Figure 134 on page 1716, Routers R1 and R5 are the ingress and egress routers, respectively. A protected LSP is established between the two routers transiting Routers R2, R3, and R4. Router R2 provides user traffic protection by creating a partial backup LSP that merges with the protected LSP at Router R4. This partial one-to-one backup LSP is called a detour. Detours are always calculated to avoid the immediate downstream link and node, providing against both link and node failure.

Figure 134: One-to-One Backup



In the example, the protected LSP is **R1-R2-R3-R4-R5**, and the following detours are established:

- Router R1—**R1-R6-R7-R8-R3**
- Router R2—**R2-R7-R8-R4**
- Router R3—**R3-R8-R9-R5**
- Router R4—**R4-R9-R5**

To protect an LSP that traverses **N** nodes fully, there can be as many as **(N - 1)** detours. The point of local repair sends periodic refresh messages to maintain each backup path, as a result maintaining state information for backup paths protecting individual LSPs is a significant resource burden for the point of local repair. To minimize the number of LSPs in the network, it is desirable to merge a detour back to its protected LSP, when feasible. When a detour LSP intersects its protected LSP at an LSR with the same outgoing interface, it is merged.

Facility Backup Implementation

In the facility backup approach, a point of local repair maintains a single backup path to protect a set of primary LSPs traversing the point of local repair, the facility, and the merge point. The facility backup is based on interface rather than on LSP. While fast reroute protects interfaces or nodes along the entire path of a LSP, the facility backup protection can be applied on interfaces as needed. As a result, fewer states need to be maintained and refreshed which results in a scalable solution. The facility backup method is also called many-to-one backup.

The facility backup method takes advantage of the MPLS label stack. Instead of creating a separate LSP for every backed-up LSP, a single LSP is created that serves to back up a set of LSPs. Such an LSP tunnel is called a bypass tunnel. In this method, a router immediately upstream from a link failure uses an alternate interface to forward traffic

to its downstream neighbor, and the merge point should be the node immediately downstream to the facility. This is accomplished by preestablishing a bypass path that is shared by all protected LSPs traversing the failed link. A single bypass path can safeguard a set of protected LSPs. When an outage occurs, the router immediately upstream from the link outage switches protected traffic to the bypass link, then signals the link failure to the ingress router.

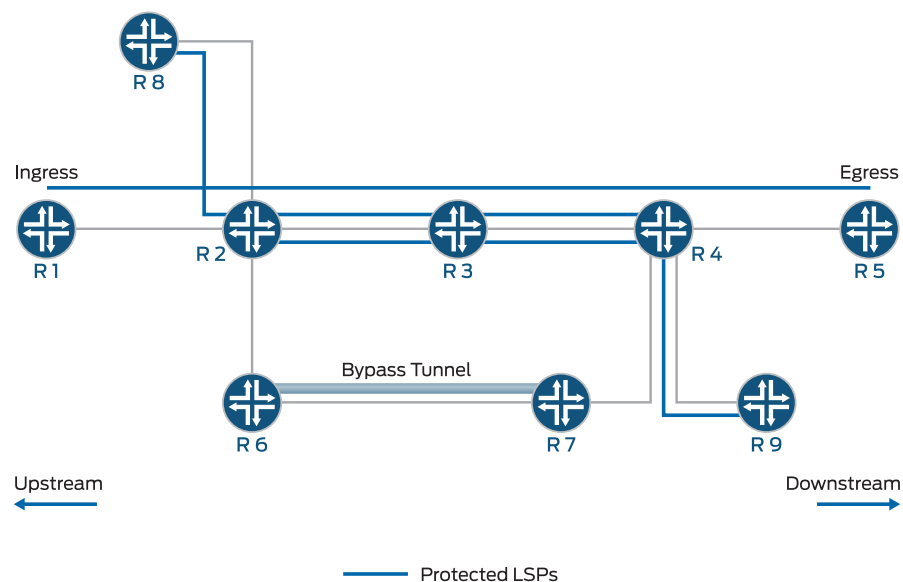
The bypass tunnel must intersect the path of the original LSP(s) somewhere downstream of the point of local repair. This constrains the set of LSPs being backed up through that bypass tunnel to those that pass through some common downstream nodes. All LSPs that pass through the point of local repair and through this common node, and that do not also use the facilities involved in the bypass tunnel are candidates for this set of LSPs.

The facility backup method is appropriate in the following situations:

- The number of LSPs to be protected is large.
- Satisfying path selection criteria (priority, bandwidth, and link coloring) for bypass paths is less critical.
- Control at the granularity of individual LSPs is not required.

In [Figure 135 on page 1717](#), Routers R1 and R5 are the ingress and egress routers, respectively. Router R2 has established a bypass tunnel that protects against the failure of Router R2-R3 link and Router R3 node. A bypass tunnel is established between Routers R6 and R7. There are three different protected LSPs that are using the same bypass tunnel for protection.

Figure 135: Facility Backup



8042700

The facility backup method provides a scalability improvement, wherein the same bypass tunnel is also used to protect LSPs from any of Routers R1, R2, or R8 to any of Routers R4, R5, or R9.

Related •
Documentation

CHAPTER 58

Service Design and Provisioning: Managing and Deploying Tunnel Services

- [Managing Devices and Tunnel Services Overview on page 1719](#)
- [Discovering Tunnel Devices on page 1720](#)
- [Creating an RSVP LSP Service Order on page 1722](#)
- [Viewing the Configured LSP Services on page 1749](#)
- [Modifying an Explicit Path in RSVP LSP Services on page 1751](#)
- [Modifying an RSVP LSP Service on page 1753](#)
- [Viewing LSP Services in Deploy Mode on page 1754](#)
- [Viewing LSP Service Orders in a Table on page 1756](#)
- [Deactivating an LSP Service on page 1757](#)
- [Reactivating an LSP Service on page 1759](#)
- [Force-Deploying an LSP Service on page 1761](#)
- [Viewing Alarms for an LSP Service on page 1763](#)
- [Managing Deployment of LSP Services Configuration to Devices on page 1763](#)
- [Deploying an LSP Service on page 1769](#)
- [Deleting a Partial Configuration of an LSP Service Order on page 1770](#)
- [Deleting an LSP Service Order on page 1772](#)
- [Validating the Pending Configuration of an LSP Service Order on page 1773](#)
- [Viewing the Configuration of a Pending LSP Service Order on page 1774](#)
- [Viewing the Configuration Details of RSVP LSP Services on page 1777](#)
- [Viewing Decommissioned LSP Service Orders on page 1779](#)

Managing Devices and Tunnel Services Overview

The design and provisioning workspaces include tasks that enable you to do the following:

- **Discover LSP Devices**—Discovers Juniper Networks devices that have been discovered in the Junos Space database or resynthesizes LSP and GRE devices that are already discovered. You can discover devices to bring them under the administration and management of Connectivity Services Director by using the Junos Space Network

Management Platform application or by using the Connectivity Services Director application in Device View of Build mode by selecting Device Discovery > Discover Devices from the Tasks pane.

- **Manage LSP Service Orders**—Enables you to manage TA service orders, such as deploying the service orders, viewing pending configuration, deleting partial configuration, and discarding and validating pending configuration using the Manage Service Deployment page (accessible in Deploy mode of Service View by selecting **Service Provisioning > Deploy Services** from the tasks pane).
- **Manage LSP Services**—Enables you to manage services, including actions that let you decommission services, perform functional audits, view functional audit results, and view service configuration changes for TA services using the Manage LSP Services page (accessible in Deploy mode of Service View by selecting **Service Provisioning > Deploy Services** from the tasks pane).

The provisioning workspace allows you, the MPLS LSP service designer to create and manage LSP definitions to use as a starting point for provisioning services. You must have Service Designer privileges to create a tunnel service or LSP service definition. You must first discover Juniper Networks devices that have been configured for MPLS LSPs and create an LSP definition..

Discovering Tunnel Devices

When you start Connectivity Services Director for the first time, the system does not have any devices. The first step is to build your network. Even with large networks, Connectivity Services Director has made this step relatively easy and straightforward. You will add devices to Connectivity Services Director and the database by using a process called *device discovery*. Once a device is discovered, it shows in the interface and Connectivity Services Director begins to monitor the device.

Connectivity Services Director provides a wizard for device discovery. The following example shows the path for device discovery through the wizard. For an alternate path, you can get a step-by-step instruction from the help system.

Before you discover tunneling devices:

- Ensure that the devices that you want to discover are configured for MPLS with the required interface in the Junos OS configuration hierarchy [edit protocols mpls]. See the *Junos Software MPLS Configuration Guide*.

In this example, we provide an IP address range, and Connectivity Services Director populates the database with all supported devices within that range.

1. While in the **Build** mode, select **Device View** or **Custom Group View** from the View selector.
2. To discover physical devices, click **Discover Devices** in the Tasks pane. Each mode has a Tasks Pane that displays the actions you can take while in that mode and that particular network view.

3. (Optional) Type a name for the discovery job. The default name is ND Discovery.
4. Click **Add** in the Device Targets window. You can add a single device IP address, a range of IP addresses, an IP subnet, or a hostname. In this example, we select an IP address range.
5. Provide the initial or the lowest IP address value and the ending or highest IP address value for the range and click **Add**. You can have up to 1024 devices in a range. After you click Add, the address range is listed in the Device Targets window.
6. Click **Next** or click **Discovery Options** to proceed to specify the device credentials and method of discovery.
7. Click **Add** in the Device Credentials window and enter the username and password assigned for administrative access.
8. Select **Ping**, **SNMP**, or both as the method of device discovery. Selecting both is the preferred method if the device is configured for SNMP.

If you select SNMP, the Add SNMP Settings dialog box is displayed. In this example, because we run SNMP version 2, we need to provide the community string. Click **Add** to save the setting.



NOTE: You cannot choose a method for device discovery for virtual network discovery.

9. Click **Next** or **Schedule Options** to proceed to schedule the time when discovery is run.



NOTE: Scheduling options are not available for virtual network discovery.

10. Indicate whether to run the device discovery now or set up a schedule to minimize network traffic. In this example, we set the schedule to run during off hours.
11. Click **Review** to review the settings before you exit the wizard.
12. Click **Finish** to complete the discovery setup and to save the settings.
13. Click **View Discovery Status** to view all scheduled and completed jobs. After a job completes, you can click **Show Details** to view further information on any unexpected results.

Creating an RSVP LSP Service Order

The service designer is responsible for creating and managing service definitions and the service provisioner uses these definitions as the basis for creating a service order. You can create a service definition that specifies attributes that are common to a group of service orders with similar service requirements, and a service order, which is an implementation object or a derivative of a service definition. For RSVP label-switched path (LSP) services, a service order can be directly created but a customized service definition cannot be created independently.

You can create MPLS RSVP LSP (also called RSVP LSP) service orders that you can use as a starting point for provisioning LSP services. For RSVP LSP service orders, unlike the framework that is available for network services, such as point-to-point, VPLS, and Layer 3 VPN protocols, in which a service definition is created independently as a separate item and a service order can be created, based on a service definition, a service order is created, independent of a service definition. You can, however, select a customized predefined service definition during the creation of an RSVP LSP service order. When you select such a predefined service definition, the parameters that are contained in it are populated in the corresponding fields of the service order creation wizard.

A wizard is available to create and modify a service order. The settings that you configure in the service order are organized in separate pages of the wizard, which you can launch by clicking the appropriate buttons at the top of the Create or Edit a Service Order page. Alternatively, you can proceed to the corresponding setting-related pages by clicking the Back and Next buttons in the wizard at any point during the creation of the service order.

To create an RSVP LSP service order, you must first discover devices that have been configured for the RSVP LSP.

1. [Configuring LSP Order General Settings on page 1722](#)
2. [Configuring LSP Service Order Advanced Settings on page 1726](#)
3. [Creating a Name Pattern for LSPs in the Service Order on page 1738](#)
4. [Configuring Node Settings for LSPs in the Service Order on page 1740](#)
5. [Configuring MPLS Path Settings on page 1741](#)
6. [Configuring LSP Primary Path Settings on page 1745](#)
7. [Configuring LSP Secondary Path Settings on page 1747](#)
8. [Reviewing the Configured Settings on page 1748](#)

Configuring LSP Order General Settings

As the service activator, you can configure an RSVP LSP based on a predefined RSVP LSP service definition. Alternatively, you can create an RSVP LSP service order without basing it on a service definition, and use the service order as a starting point for provisioning LSP services. The service activator can configure LSP settings that the service designer specified to be editable.

To create an RSVP LSP service order, configure the general settings.

1. Select **Service View** from the View selector.

The workspaces that are applicable to routing and tunneling services are displayed.

2. From the Junos Space user interface, click the **Deploy** icon on the Connectivity Services Director banner.

The functionalities that you can configure in this mode are displayed in the Tasks pane of the GUI window.

3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.

The different network service types that you can configure, such as point-to-point, VPLS, and L3VPN, are displayed.

4. From the Service View pane, click the plus sign (+) sign next to Tunnels, and select RSVP LSPs.

The RSVP LSPs node is expanded and displayed in the View pane.

5. From the task pane, select **Service Provisioning > Manage LSP**.

The Manage Network Services page is displayed in on the top right main display area, and the Manage Service Deployment window is displayed on the bottom of the main display area.

Name	Service Type	State	FA Status	Fault Status	PM Status	Activation Date	Last Modified Date
LSP_50	LSP	DeploymentPending	Pending	None	None	September 5, 2015, 1...	September 5, 2015, 1...
Test11	LSP	Deployed-Active	Pending	Up	None	August 30, 2015, 7.1...	August 30, 2015, 7.1...
fm_path	LSP	DeploymentPending	Pending	None	None	August 30, 2015, 3.5...	August 30, 2015, 3.5...
p2p_predefined	LSP	DeploymentPending	Pending	None	None	August 30, 2015, 3.5...	August 30, 2015, 3.5...
fm_csp10	LSP	DeploymentPending	Pending	None	None	August 30, 2015, 3.4...	August 30, 2015, 3.4...
p2p_csp10	LSP	DeploymentPending	Pending	None	None	August 30, 2015, 3.4...	August 30, 2015, 3.4...
R1_R4	LSP	Deployed-Active	Up	Up	None	August 29, 2015, 10...	August 29, 2015, 10...
R4-R1	LSP	Deployed-Active	Pending	Down	None	August 29, 2015, 10...	August 29, 2015, 10...
FM_PL_Node_mod2	LSP	DeploymentPending	Pending	None	None	August 28, 2015, 11.0...	August 28, 2015, 11.0...
FM_PL_Node_mod1	LSP	Deployed-Active	Pending	Up	None	August 28, 2015, 11.0...	August 28, 2015, 11.0...
Fullmesh	LSP	Deployed-Active	Up	Up	None	August 28, 2015, 10...	August 28, 2015, 10...
fulmesh_mod	LSP	Deployed-Active	Pending	None	None	August 28, 2015, 10...	August 28, 2015, 10...
P2P2	LSP	DeploymentPending	Pending	None	None	August 28, 2015, 10...	August 28, 2015, 10...

Page 1 of 1 | Displaying 1 - 13 of 13 | Show 25 items

Manage LSP Deployment

6. Click the down arrow on the **New** menu and select **RSVP LSPs** from the drop-down menu.

The wizard to create an RSVP LSP is displayed.

On the General Settings page of the wizard, the Service Details pane is displayed on the left, which contains the Basic and Advanced tabs.

7. Click the **Basic** tab.

The general settings are displayed.

Create RSVP LSP Service Order.

General Settings > Node Parameters > Path Settings > Review

You are here: General Settings

Service Details

Basic

Order Name: LSP_SO

LSP Configuration: ☒ Create Custom ☐ Import Existing

LSP Type: RSVP

Topology: ☒ P2P ☐ P2MP ☒ Full Mesh

Path Selection Type: ☒ CSPF ☐ Explicit Path

LSP Protection Type: Path Protection Only

Local Protection Type: Link Protection

LSP Pattern Details

Name: Full Mesh Default Pattern

Pattern: \$Name_SIngressRouter_to_SEgressLoopbackAddress

8. Configure the settings on the Basic tab as indicated in the following table.

Item	Action
Service Name	Type a name that identifies the LSP service order. A service order name cannot exceed 50 characters and can contain only letters, numbers, and some special characters. The special characters allowed are hyphen (-), underscore (_), and period (.)

Item	Action
LSP Configuration	<p>Perform either of the following actions to specify the method to be used for creating an LSP order:</p> <ul style="list-style-type: none"> • Select the Create Custom option button to create a service order as an entirely new one. • Select the Import Existing option button to select an available LSP service definition that you created and published, and select a predefined service definition from the drop-down list. The LSP service definition on the LSP Definition drop-down menu is available for selection only if you published the service definition. <p>The following are the predefined RSVP LSP service definitions:</p> <ul style="list-style-type: none"> • RSVP LSP with BFD - Path Protection—Creates an RSVP LSP service order that protects the LSP primary path by establishing a secondary path with BFD as the signaling protocol • RSVP LSP with BFD - P2MP Topology—Creates an RSVP LSP service order with BFD as the signaling protocol and a point-to-multipoint topology • RSVP LSP with Path Protection—Creates an RSVP LSP service order that protects the primary path by establishing a secondary path • RSVP LSP with Node Link Protection—Creates an RSVP LSP service order that bypasses a node or link for redundancy. • FullMesh LSP with Node Link Protection—Creates an RSVP LSP service order in a full-mesh topology that bypasses a node or link for redundancy. <p>The parameters on the different pages of the wizard are filled out with the values of parameters retrieved from the service definition you selected. You can modify them as needed.</p>
Topology	<p>Select the LSP transport topology from the list:</p> <ul style="list-style-type: none"> • P2P—Provides a point-to-point connectivity between the selected endpoints • P2MP—Provides a point-to-multipoint connectivity between the selected endpoints • Full Mesh—Provides any-to-any unidirectional MPLS connectivity among all the selected provider edge router
Path Selection Type	<p>From this list, select either CSPF or Explicit Path. In Constrained Shortest Path First (CSPF) LSPs, the intermediate hops of the LSP are automatically computed by the software. If you select CSPF, Junos OS calculates the best path for you. In explicit-path LSPs, all intermediate hops of the LSP are manually configured. The intermediate hops can be strict, loose, or any combination of the two.</p>
LSP Protection Type	<p>Select the type of protection you want to configure.</p> <p>Path Protection Only—Protects the LSP primary path by establishing a secondary path.</p> <p>Fast reroute can be applied to the LSP if you are selecting Path Protection Only. On the Advanced page, specify the protection type as Path Protection Only and select the Enable Fast Reroute check box in the Common Settings section on the Advanced tab.</p> <p>Local Protection Only—Provides local repair procedures that ensure faster restoration by establishing local protection as close to a failure as possible. Configuring only local protection for the ingress router of the primary LSP causes RSVP-traffic engineering to indicate to LSP setup that the primary LSP needs local protection. When there is only one path for the LSP, you can specify either link protection or node-link protection.</p> <p>Path and Local Protection—Provides redundancy using a combination of path protection and local protection options. The primary path is protected and local repair procedures for faster redundancy is achieved using this methodology.</p>

Item	Action
Local Protection Type	<p>Specify the type of protection:</p> <p>Link Protection—Provides backup support for a single link.</p> <p>Node-Link Protection—Can bypass a node or a link to provide redundancy.</p> <p>NOTE: This drop-down list is unavailable if the LSP Protection Type is Path Protection Only.</p>

- Click the **Advanced** tab.

The advanced settings that you can configure for the LSP service order are displayed.

Configuring LSP Service Order Advanced Settings

On the left of the General Settings page of the wizard, the Service Details pane contains the Basic and Advanced tabs.

To configure the settings that are globally applicable throughout the LSP in the LSP service order:

- Click the **Advanced** tab on the General Settings page of the wizard to create an RSVP LSP.

The global or system-wide settings are displayed.

The screenshot shows the 'Create RSVP LSP Service Order' wizard. At the top, there's a title bar 'Create RSVP LSP Service Order.' with a help icon. Below it are four tabs: 'General Settings' (active), 'Node Parameters', 'Path Settings', and 'Review'. Below the tabs, it says 'You are here: General Settings'. The main area is divided into two sections. The top section is 'Service Details' with two sub-tabs: 'Basic' and 'Advanced' (active). Under the 'Advanced' tab, there's a heading 'These are optional configuration settings, expand respective fieldsets to configure them.' followed by three expandable sections: 'Common Settings', 'Path Settings', and 'BFD Settings'. The bottom section is 'LSP Pattern Details' with two fields: 'Name' (set to 'Full Mesh Default Pattern') and 'Pattern' (set to '\$Name_SIngressRouter_to_\$EgressLoopbackAddress'). There are 'Select' and 'Create' buttons next to the 'Name' field. At the bottom right, there are four buttons: 'Back', 'Next', 'Done', and 'Cancel'.

- You can specify the following types of settings from the Advanced tab of the LSP service order creation wizard:
 - Common Settings**—Configure the LSP retry limit, retry timer (seconds), LDP tunneling settings, auto-bandwidth settings, protections settings, and BFD settings. See [“Configuring Common LSP Settings” on page 1727](#) for details

- b. Path Settings—Configure the primary and secondary paths on one point-to-point or several point-to-multiple-point branches. Specify the primary path to use for an LSP. You can configure only one primary path. You can optionally specify the preference, CoS, and bandwidth values for the primary path, which override any equivalent values that you configure for the LSP. See [“Configuring MPLS Path Settings” on page 1741](#) for details.
- c. BFD Settings—Configure a Bidirectional Forwarding Detection (BFD) protocol on MPLS IPv4 LSPs. BFD is used as a periodic Operation, Administration, and Maintenance (OAM) feature for LSPs to detect LSP data plane faults. You can configure a BFD protocol for LSPs that use RSVP as the signaling protocol. See [“Configuring BFD Settings for LSPs in the Service Order” on page 1735](#) for details.

The following sections describe the advanced settings you can configure for the LSP service order:

- [Configuring Common LSP Settings on page 1727](#)
- [Configuring LSP Path Settings in the Service Order on page 1730](#)
- [Configuring BFD Settings for LSPs in the Service Order on page 1735](#)

[Configuring Common LSP Settings](#)

You can use the **Common LSP Settings** page to view or configure the LSP retry limit, retry timer (seconds), LDP tunneling settings, auto-bandwidth settings, protections settings, and BFD settings.

Each LSP has a bandwidth value. This value is included in the sender's Tspec field in RSVP path setup messages. You can specify a bandwidth value in bits per second. If you configure more bandwidth for an LSP, it should be able to carry a greater volume of traffic. The default bandwidth is 0 bits per second.

The ingress router might make many attempts to connect and reconnect to the egress router using the primary path. You can control how often the ingress router tries to establish a connection using the primary path and how long it waits between retry attempts. The retry timer configures how long the ingress router waits before trying to connect again to the egress router using the primary path. The default retry time is 30 seconds. The time can be from 1 through 600 seconds. To modify this value, include the retry timer parameter in the service order.

Automatic bandwidth allocation allows an MPLS tunnel to automatically adjust its bandwidth allocation based on the volume of traffic flowing through the tunnel. You can configure an LSP with minimal bandwidth; this feature can dynamically adjust the LSP's bandwidth allocation based on current traffic patterns. The bandwidth adjustments do not interrupt traffic flow through the tunnel. You set a sampling interval on an LSP configured with automatic bandwidth allocation. The average bandwidth is monitored during this interval. At the end of the interval, an attempt is made to signal a new path for the LSP with the bandwidth allocation set to the maximum average value for the preceding sampling interval. If the new path is successfully established and the original path is removed, the LSP is switched over to the new path. If a new path is not created, the LSP continues to use its current path until the end of the next sampling interval, when another attempt is made to establish a new path. Note that you can set minimum and

maximum bandwidth values for the LSP. During the automatic bandwidth allocation interval, the router might receive a steady increase in traffic (increasing bandwidth utilization) on an LSP, potentially causing congestion or packet loss. To prevent this, you can define a second trigger to prematurely expire the automatic bandwidth adjustment timer before the end of the current adjustment interval.

To configure common settings that are applicable to all LSPs in the service order:

1. On the Advanced pane of the General Settings page, click the plus sign beside the **Common Settings** section.

The parameters that are applicable to all the LSPs are available for configuration.

2. Fill in the parameters as indicated in the table.

Item	Action
Retry limit	<p>Specify the number of times an ingress router can attempt to establish or reestablish a connection to the egress router by using the primary path. This counter is reset each time a primary path is created successfully. When the limit is exceeded, no more connection attempts are made. Intervention is then required to restart the connection.</p> <p>Range: 0 through 10,000</p> <p>Default: No limit is set.</p>
Retry timer	<p>Specify how long the ingress router waits before trying to connect again to the egress router by using the primary path.</p> <p>Range: 1 through 600 seconds</p> <p>Default: 30 seconds</p>

Item	Action
Bandwidth (Kbps)	<p>Specify the bandwidth in Kbps.</p> <p>A nonzero bandwidth requires that transit and egress routers reserve capacity along the outbound links for the path. The RSVP scheme is used to reserve this capacity. Any failure in bandwidth reservation (such as failures at RSVP policy control or admission control) might cause the LSP setup to fail. If there is insufficient bandwidth on the interfaces for the transit or egress routers, the LSP is not established.</p> <p>Range: Any positive integer</p> <p>Default: 0 (No bandwidth is reserved.)</p>
Enable LDP tunneling	<p>Select this check box to enable LSP for LDP tunneling. That is, if you are using RSVP for traffic engineering, you can run LDP simultaneously to eliminate the distribution of external routes in the core network. The LSPs established by LDP are tunneled through the LSPs established by RSVP. LDP effectively treats the traffic-engineered LSPs as single hops. When you configure the router to run LDP across RSVP-established LSPs, LDP automatically establishes sessions with the router at the other end of the LSP. LDP control packets are routed hop by hop, rather than carried through the LSP. This routing allows you to use simplex (one-way) traffic-engineered LSPs. Traffic in the opposite direction flows through LDP-established LSPs that follow unicast routing rather than through traffic-engineered tunnels.</p>
Enable fast reroute	<p>Select this check box to enable fast reroute. If you enable the fast reroute, the ingress router signals all the downstream routers that fast reroute is enabled on the LSP, and each downstream router does its best to set up detours for the LSP. If a downstream router does not support fast reroute, it ignores the request to set up detours and continues to support the LSP. A router that does not support fast reroute will cause some of the detours to fail, but otherwise has no impact on the LSP.</p>

Item	Action
Auto Bandwidth	<p>Select this check box to allow an MPLS tunnel to automatically adjust its bandwidth allocation based on the volume of traffic flowing through the tunnel.</p> <ol style="list-style-type: none"> 1. In the Adjust Interval field, specify the bandwidth reallocation interval. Range: 300 through 4,294,967,295 seconds. Default: 86,400 seconds. 2. In the Maximum Bandwidth (Kbps) field, specify the maximum bandwidth in Kbps or an LSP with automatic bandwidth allocation enabled. You can maintain the LSP's bandwidth between minimum and maximum bounds by specifying values. The default value is 10000 Kbps. The range is 1 through 2147483 Kbps. 3. In the Minimum Bandwidth (Kbps) field, specify the minimum bandwidth in Kbps or an LSP with automatic bandwidth allocation enabled. The default value is 1000 Kbps. The range is 1 through 2147483 Kbps. You must enter the minimum bandwidth to be lower than the maximum bandwidth.

3. Click the plus sign beside the **Path Settings** section to configure the path specifications for the LSP.

The Path Settings section is expanded and displayed.

Configuring LSP Path Settings in the Service Order

When IP traffic enters an LSP tunnel, the ingress router marks all packets with a CoS value, which is used to place the traffic into a transmission priority queue. On the router, for SDH/SONET and T3 interfaces, each interface has four transmit queues. The CoS value is encoded as part of the MPLS header and remains in the packets until the MPLS header is removed when the packets exit from the egress router. The routers within the LSP use the CoS value set at the ingress router. The CoS value is encoded by means of the CoS bits (also known as the EXP or experimental bits). MPLS class of service works in conjunction with the router's general CoS functionality. If you do not configure any CoS features, the default general CoS settings are used. For MPLS class of service, you might want to prioritize how the transmit queues are serviced by configuring weighted round-robin, and to configure congestion avoidance using random early detection (RED).

When there is insufficient bandwidth to establish a more important LSP, you might want to tear down a less important existing LSP to free the bandwidth. You do this by preempting the existing LSP. Whether an LSP can be preempted is determined by two properties associated with the LSP:

- Setup priority—Determines whether a new LSP that preempts an existing LSP can be established. For preemption to occur, the setup priority of the new LSP must be higher

than that of the existing LSP. Also, the act of preempting the existing LSP must produce sufficient bandwidth to support the new LSP. That is, preemption occurs only if the new LSP can be set up successfully.

- **Reservation priority**—Determines the degree to which an LSP holds on to its session reservation after the LSP has been set up successfully. When the reservation priority is high, the existing LSP is less likely to give up its reservation, and hence it is unlikely that the LSP can be preempted.

You cannot configure an LSP with a high setup priority and a low reservation priority, because permanent preemption loops might result if two LSPs are allowed to preempt each other. You must configure the reservation priority to be higher than or equal to the setup priority. The setup priority also defines the relative importance of LSPs on the same ingress router. When the software starts, when a new LSP is established, or during fault recovery, the setup priority determines the order in which LSPs are serviced. Higher-priority LSPs tend to be established first and hence enjoy more optimal path selection.

To configure LSP path settings in the service order:

1. On the Advanced pane of the General Settings page, click the plus sign beside the **Path Settings** section.

The LSP path parameters that are applicable to all the LSPs are available for configuration.

The screenshot shows the 'Create RSVP LSP Service Order' configuration page. The top navigation bar includes tabs for 'General Settings', 'Node Parameters', 'Path Settings', and 'Review'. Below the navigation bar, a breadcrumb indicates 'You are here: General Settings'. The main content area is divided into two sections: 'Service Details' and 'LSP Pattern Details'. The 'Service Details' section has two tabs: 'Basic' and 'Advanced'. The 'Advanced' tab is selected, and the 'Path Settings' section is expanded. The 'Path Settings' section contains the following configuration options:

- Common Settings:**
 - Class Of Service:** Best Effort (dropdown menu)
 - Hop Limit:** 255 (spin box)
 - Bandwidth (Kbps):** 2 (spin box)
 - ☐ Standby (enable switchover)
 - ☐ Adaptive
- Priority:**
 - Setup Priority:** 7 (spin box)
 - Hold Priority:** 0 (spin box)
- BFD Settings:** (collapsed)

The 'LSP Pattern Details' section at the bottom contains the following configuration options:

- Name:** Full Mesh Default Pattern (text field) with 'Select' and 'Create' buttons.
- Pattern:** \$Name_SingressRouter_to_EgressLoopbackAddress (text field)

At the bottom right of the page, there are four buttons: 'Back', 'Next', 'Done', and 'Cancel'.

2. Fill in the parameters as indicated in the following table.

Item	Action
Hop limit	<p>Specify the hop limit of the LSP.</p> <p>Range: 2 through 255. A path with two hops consists of the ingress and egress routers only.</p> <p>Default: Each LSP can traverse a maximum of 255 hops, including the ingress and egress routers.</p>
Class of service	<p>Specify a decimal number. This number corresponds to a 3-bit binary number. The high-order 2 bits of the CoS value select which transmit queue to use on the outbound interface card. The low-order bit of the CoS value is treated as the packet loss priority (PLP) bit and is used to select the random early detection (RED) drop profile to use on the output queue. If the low-order bit is 0, the non-PLP drop profile is used, and if the low-order bit is 1, the PLP drop profile is used. Typically, RED aggressively drops packets that have the PLP bit set. For more information about RED and drop profiles, see the <i>Junos OS Class of Service Configuration Guide</i>.</p> <p>Range: A decimal number from 0 through 7</p> <p>This field is not applicable for local-protection type of LSPs.</p>
Bandwidth (Kbps)	<p>Specify a bandwidth in Kbps for an LSP. Each LSP has a bandwidth value. This value is included in the sender's Tspec field in RSVP path setup messages. The ingress router uses the traffic specification (Tspec) object to specify the parameters for the traffic it is going to send. You can specify a bandwidth value in bits per second. If you configure more bandwidth for an LSP, it should be able to carry a greater volume of traffic. The default bandwidth is 0 bits per second.</p>
Standby (enable switchover)	<p>Select this check box to have the path remain up at all times to provide immediate switchover if connectivity problems occur.</p> <p>This field is displayed only for secondary paths.</p>

Item	Action
Adaptive	<p>Select this check box if you want to configure an LSP to be adaptive when it is attempting to reroute itself. When it is adaptive, the LSP holds onto existing resources until the new path is successfully established and traffic has been switched over to the new LSP. To retain its resources, an adaptive LSP does the following:</p> <ul style="list-style-type: none">• Maintains existing paths and allocated bandwidths—This ensures that the existing path is not torn down prematurely and allows the current traffic to continue flowing while the new path is being set up.• Avoids double-counting for links that share the new and old paths—Double-counting occurs when an intermediate router does not recognize that the new and old paths belong to the same LSP and counts them as two separate LSPs, requiring separate bandwidth allocations. If some links are close to saturation, double-counting might cause the setup of the new path to fail. <p>By default, adaptive behavior is disabled.</p> <p>You can include the adaptive statement in two different hierarchy levels. If you specify the adaptive statement at the LSP hierarchy levels, the adaptive behavior is enabled on all primary and secondary paths of the LSP. This means both the primary and secondary paths share the same bandwidth on common links.</p> <p>This check box is not available for P2MP topology and also when the path selection type is explicit path.</p>
Priority	<p>Configure the LSP's preemption properties by selecting a value from the Setup Priority and Hold riority lists.</p>

Item	Action
Setup Priority	<p>Specify a priority value, which determines whether a new LSP that preempts an existing LSP can be established. For preemption to occur, the setup priority of the new LSP must be higher than that of the existing LSP. Also, the act of preempting the existing LSP must produce sufficient bandwidth to support the new LSP. That is, preemption occurs only if the new LSP can be set up successfully. The setup priority also defines the relative importance of LSPs on the same ingress router. When the software starts, when a new LSP is established, or during fault recovery, the setup priority determines the order in which LSPs are serviced. Higher-priority LSPs tend to be established first and hence enjoy more optimal path selection.</p> <p>This field cannot be configured for local-protection type of LSPs.</p> <p>Range: Both setup-priority and reservation-priority can be a value from 0 through 7, where 0 is the highest priority and 7 is the lowest priority.</p> <p>Default: An LSP has a setup priority of 7 (that is, it cannot preempt any other LSPs) and a reservation priority of 0 (that is, other LSPs cannot preempt it). These defaults prevent preemption. When you are configuring these values, make sure that the setup priority value is lower than or equal to the hold priority value.</p>
Hold Priority	<p>Specify a hold priority value. The hold priority determines the degree to which an LSP holds onto its session reservation of the LSP that has been set up successfully. When the hold priority is high, the existing LSP is less likely to give up its reservation and, therefore, it is unlikely that the LSP can be preempted. You must configure the hold priority to be greater than or equal to the setup priority.</p> <p>This field cannot be configured for local-protection type of LSPs.</p> <p>Range: 0 through 7, where 0 is the highest priority and 7 is the lowest priority.</p> <p>NOTE: If traffic engineering admission control determines that there are insufficient resources to accept a request to set up a new LSP, the setup priority is evaluated against the hold priority of existing LSPs. An LSP with a hold priority lower than the setup priority of the new LSP can be preempted. The existing LSP is terminated to make room (that is, resources are freed) for the new LSP.</p>

- Click the plus sign beside the **BFD Settings** section to configure the BFD parameters for the LSP.

The BFD Settings section is expanded and displayed.

Configuring BFD Settings for LSPs in the Service Order

BFD for RSVP supports unicast IPv4 LSPs. When BFD is configured for an RSVP LSP on the ingress router, it is enabled on the primary path and on all standby secondary paths for that LSP. The source IP address for outgoing BFD packets from the egress side of an MPLS BFD session is based on the outgoing interface IP address. You can enable BFD for all LSPs on a router or for specific LSPs. If you configure BFD for a specific LSP, whatever values configured globally for BFD are overridden. The BFD sessions originate only at the ingress router and terminate at the egress router.

The BFD failure detection timers are adaptive and can be adjusted to be more or less aggressive. For example, the timers can adapt to a higher value if the adjacency fails, or a neighbor can negotiate a higher value for a timer than the configured value. The timers adapt to a higher value when a BFD session flap occurs more than three times in a span of 15 seconds. A back-off algorithm increases the receive (Rx) interval by two if the local BFD instance is the reason for the session flap. The transmission (Tx) interval is increased by two if the remote BFD instance is the reason for the session flap.

To configure BFD settings for RSVP LSPs in the service order:

1. On the Advanced pane of the General Settings page, click the plus sign beside the **BFD Settings** section.

The parameters that are applicable to all of the LSPs are available for configuration.

The screenshot displays the 'Create RSVP LSP Service Order' configuration interface. At the top, a blue header bar contains the title and a help icon. Below the header, a navigation bar shows four tabs: 'General Settings' (selected), 'Node Parameters', 'Path Settings', and 'Review'. A breadcrumb trail indicates 'You are here: General Settings'.

The main configuration area is divided into two sections. The top section, 'Service Details', has a left sidebar with 'Basic' and 'Advanced' tabs. The 'Advanced' tab is active, showing the 'Path Settings' section. Within 'Path Settings', the 'BFD Settings' section is expanded, revealing a list of configuration parameters:

- BFD Detection:** A dropdown menu set to 'This LSP'.
- Minimum Interval:** A numeric input field set to 300.
- Minimum Receive Interval:** A numeric input field set to 50.
- Multiplier:** A numeric input field set to 3.
- No Adaption:** An unchecked checkbox.
- Transmit Minimum Interval:** A numeric input field set to 50.
- Transmit Threshold:** A numeric input field.
- Detection Threshold:** A numeric input field.
- Failure Action:** Two radio buttons, 'Teardown' (selected) and 'Make Before Break'.

The bottom section, 'LSP Pattern Details', contains:

- Name:** A text input field with 'Full Mesh Default Pattern' and a 'Select' button.
- Pattern:** A text input field with the value '\$Name_SingressRouter_to_\$EgressLoopbackAddress' and a 'Create' button.

At the bottom right of the interface, there is a row of four buttons: 'Back', 'Next', 'Done', and 'Cancel'.

2. Fill in the parameters as indicated in the following table:

Field	Action
BFD Detection	<p>Select the BFD setting type:</p> <ul style="list-style-type: none"> • This LSP—Configure BFD settings for all of the specific LSP. • Primary Path—Configure BFD settings for the primary path of the specific LSP. • Secondary Path—Configure BFD settings for the secondary path of the specific LSP. • None—Do not configure BFD settings. By default, BFD is not configured. <p>NOTE: The primary path and the secondary path are listed on BFD Detection menu only if you have configured the primary and secondary paths.</p> <p>You can modify the BFD Detection settings in a service.</p>
Minimum Interval	<p>Specify the minimum transmit and receive interval. This value represents the minimum interval at which the local routing device transmits hello packets as well as the minimum interval that the routing device expects to receive a reply from a neighbor with which it has established a BFD session.</p> <p>Range: 1 through 255000 milliseconds</p> <p>Default: 50</p>
Minimum Receive Interval	<p>Specify the minimum receive interval. This value represents the minimum interval at which the peer must receive a reply from a peer with which it has established a BFD session.</p> <p>Range: 1 through 255000 milliseconds</p> <p>Default: 50</p>
Multiplier	<p>Specify the detection time multiplier. This value represents the number of hello packets not received by the neighbor before BFD declares that the neighbor is down.</p> <p>Range: 1 through 255</p> <p>Default: 3</p>
No adaptation	<p>Select this check box to disable adaptation.</p> <p>You can configure an LSP to be adaptive when it is attempting to reroute itself. When it is adaptive, the LSP holds onto existing resources until the new path is successfully established and traffic has been switched over to the new LSP. To retain its resources, an adaptive LSP does the following:</p> <ul style="list-style-type: none"> • Maintains existing paths and allocated bandwidths—This ensures that the existing path is not torn down prematurely and allows the current traffic to continue flowing while the new path is being set up. • Avoids double-counting for links that share the new and old paths—Double-counting occurs when an intermediate router does not recognize that the new and old paths belong to the same LSP and counts them as two separate LSPs, requiring separate bandwidth allocations. If some links are close to saturation, double-counting might cause the setup of the new path to fail. <p>By default, adaptive behavior is disabled.</p>

Field	Action
Transmit Minimum Interval	<p>Specify the minimum transmit interval at which the local routing device transmits hello packets to a neighbor with which it has established a BFD session. The negotiated transmit interval for a peer is the interval between the sending of BFD packets to peers. The receive interval for a peer is the minimum time that it requires between packets sent from its peer; the receive interval is not negotiated between peers. To determine the transmit interval, each peer compares its configured minimum transmit interval with its peer's minimum receive interval. The larger of the two numbers is accepted as the transmit interval for that peer.</p> <p>Range: 1 through 255000 milliseconds</p> <p>Default: 50 milliseconds</p>
Transmit Threshold	<p>Specify the high transmit interval triggering a trap.</p> <p>The threshold is used for detecting the adaptation of the transmit interval. When the BFD session transmit interval adapts to a value greater than the threshold, a single trap and a single system message are sent.</p> <p>Range: 51 through 4,294,967,295</p> <p>Default: None</p>
Detection Threshold	<p>Specify the maximum time at which to trigger a trap.</p> <p>Specify the threshold for the adaptation of the BFD session detection time. When the detection time adapts to a value equal to or greater than the threshold, a single trap and a single system log message are sent.</p> <p>Range: 0 through 4,294,967,295</p> <p>Default: None</p>
Failure Action	<p>Select an action to take when a BFD session for an RSVP LSP goes down:</p> <ul style="list-style-type: none"> • Teardown—Causes the LSP path to be taken down and resigned immediately. • Make Before Break—Attempts to signal a new LSP path before tearing down the old LSP path. <p>When the BFD session for an RSVP LSP goes down, the LSP is torn down and resigned. Traffic can be switched to a standby LSP, or you can simply tear down the LSP path. Any actions performed are logged. When a BFD session for an RSVP LSP path goes down, you can configure the Junos OS to resignal the LSP path or to simply disable the LSP path. A standby LSP path could be configured to handle traffic while the primary LSP path is unavailable. The router can automatically recover from LSP failures that can be detected by BFD. By default, if a BFD session fails, the event is simply logged.</p>
Teardown Timeout	<p>Specify a time to wait before the LSP path is taken down and resigned. If you specify a value of 0 for the teardown-timeout interval, the LSP is taken down and resigned immediately.</p> <p>Range: 0 through 30 seconds</p> <p>Default: None</p>

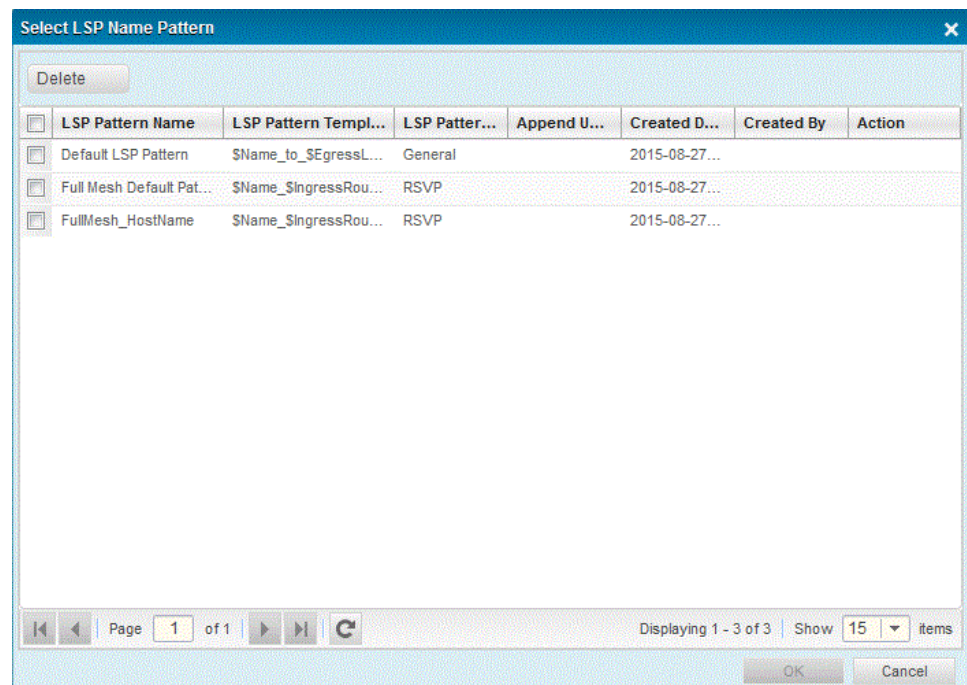
3. Specify the LSP pattern settings. See [“Creating a Name Pattern for LSPs in the Service Order” on page 1738](#) for details.

Creating a Name Pattern for LSPs in the Service Order

Instead of using an existing predefined pattern of label-switched path (LSP) names, you can also create an LSP name of your preference or convention. The customized LSP name includes a set of common variables and supported special characters. The Transport Activate software appends a unique number to these customized name to avoid conflicts.

To specify a name pattern for LSPs in the service order:

1. On the General Settings page, with either the Advanced or Basic tab selected, click the plus sign (+) next to LSP Pattern Details at the bottom of the page to expand the section.



2. Click **Select** adjacent to the Name field to select a pattern from the list of available patterns.

The Select LSP Name pattern dialog box appears. The dialog box displays a table, which includes the following patterns:

- Default LSP pattern—Uses the default LSP name pattern for a point-to-point and point-to-multipoint topology
- Full-mesh default pattern—Uses the default LSP name pattern for a full-mesh topology
- User-defined RSVP patterns—Creates an LSP name of your preference or convention

3. Select the check box next to the pattern to be used in the LSP service order.

4. Click **OK** to save the selection.

You are returned to the LSP Pattern Details section of the General Settings page of the wizard.

5. In the Pattern field, view the name of the selected pattern. For example, the pattern of Default LSP Pattern is Service Order Name_to_Egress Loopback Address.

Alternatively, to create a new name pattern, click the **Create** button adjacent to the Name field.

The Create LSP Name Pattern dialog box appears.

6. From the Name list, select one of the following:

- **RSVP**—Name pattern for RSVP LSPs.
- **General**—Name pattern for general LSPs.
- **Static**—Name pattern for static LSPs.

The specified name pattern for the type of LSP you want to configure is selected.

7. Specify the name of the pattern in the **Name** box.

8. In the LSP Pattern Details section, select the **Select Variable** option button to select an existing variable from the Variable drop-down list. The predefined variables are listed in the Variable drop-down list.

Alternatively, select the **Add Text** option button to add a new variable.

The Variable field is available for specifying the variable.

9. Click **Add** to add the variable to the pattern.

The variable you add is displayed in pattern name of the Pattern field.



NOTE: You can select any of the predefined variables from the Variable drop-down list. The variables in the Variable drop-down list are based on the **Pattern Type** you select.

Alternatively, click **Clear** to remove the variable from the Variables drop-down list.

The variable is deleted from the pattern name in the Pattern field.

10. Select the **Append unique number** check box to append a unique number to these customized names you create to avoid conflicts.

11. Click **Create** to add the name pattern to the LSP service.

You are returned to the General Settings page of the wizard and the pattern name appears in the Patterns field.

The pattern is also added to the Select LSP Name Patterns inventory page, which you can open by clicking **Select** beside the Name field in the LSP Pattern Details section. You can select this pattern name in the service order from the Select LSP Name Patterns inventory page.



NOTE: You can view the details of a pattern on the Select LSP Name Patterns inventory page. You cannot modify an existing pattern.

12. On the General Settings page of the wizard, click **Next** to proceed to the next step of the wizard, which is to define the node or endpoint settings.

The Node Settings page of the wizard is displayed.

Configuring Node Settings for LSPs in the Service Order

On the **Node Settings** page, you can configure the endpoints or nodes for the LSP service order.

Only fields that correspond to the type of topology that you selected on the General Settings page of the wizard are displayed on the Node Settings page.

Create RSVP LSP Service Order. ⓘ

General Settings > **Node Parameters** > Path Settings > Review

You are here: Node Parameters

Topology: Full Mesh

Select Devices

+ Add - Delete

<input type="checkbox"/>	Name	IpAddress	State	Managed State	Platform	OS Version	Roles
<input type="checkbox"/>	480R4_SV_Alb...	10.102.162.222	■ Up	In Sync	MX480	15.1-20150121...	N_PE
<input type="checkbox"/>	960R1_SV_Alb...	10.102.163.58	■ Up	In Sync	MX960	15.1-20150121...	N_PE

No data to display | Show 20 Items

⏪ Back ⏩ Next ⏹ Done ⏴ Cancel

1. Fill in the parameters as described in the following table:

Item	Action
Ingress Router	<ol style="list-style-type: none"> 1. Click Select beside the field to open the Select device dialog box. 2. Select the check box next to an available router that must function as the ingress router. The local router is always considered to be the ingress router, which is the beginning of the LSP. The software automatically determines the correct outgoing interface and IP address to use to reach the next router in an LSP. By default, the router ID is chosen as the address of the ingress router. MPLS-signaled label-switched paths (LSPs) run from a specific ingress router to a specific egress router. For basic MPLS-signaled LSP function, you must configure the ingress router, but do not have to configure any other routers. This field is unavailable if the selected LSP service definition is a full-mesh RSVP definition.
Egress Router	<ol style="list-style-type: none"> 1. Click Select beside the field to open the Select Device dialog box. The Select button is available only for P2P topology. 2. Select an available router that must function as the egress router in the LSP connection established using the primary path from the ingress router. For a point-to-point topology, select one egress router. 3. If the topology is a point-to-multipoint LSP topology, click Add in the Egress Routers table to open the Select Device dialog box. NOTE: The Egress Routers table is available only for P2MP topology. Select multiple routers to function as egress routers for the point-to-multiple-point topology. <p>To delete an egress router added to the LSP service, select the device, and click Delete above the table of listed egress routers.</p>
Select Devices	<p>This field is available only for full-mesh LSP topology.</p> <ol style="list-style-type: none"> 1. If the topology is a full-mesh LSP topology, click Add in the Egress Routers table to open the Select Device dialog box. The Egress Routers table is available only for P2MP topology. Select multiple routers to function as egress routers for the point-to-multiple-point topology. 2. To delete an egress router added to the LSP service, select the device, and click Delete above the table of listed egress routers.

2. Click **Next** to proceed to the next page of the wizard, which is to configure path settings.

The Path Settings page of the wizard is displayed.

Configuring MPLS Path Settings

The **Path Settings** page of the service order creation wizard enables you to view existing paths or add, edit, or delete new paths.

1. Fill in the parameters as indicated in the following table under the Primary and Secondary tabs of the Path Parameters page.

Item	Action
Path Name	Define the path to be either automatic path selection or a new path name. If you do not configure both primary and secondary paths for an LSP, MPLS uses an automatic path selection algorithm.
Automatic	(Optional) Select this option from the Path Name list for an automatic path to be used for the LSP.
Create New	<p>(Optional) Click this button create a new path.</p> <p>The Create MPLS Path dialog box is displayed.</p> <p>To add one or more new paths:</p> <ol style="list-style-type: none"> 1. Type a name in the Path Name text box. 2. Select whether you want the LSP path to be Loose or Strict. <p>To configure complete path information, specify every router hop between the ingress and egress routers, preferably by selecting the Strict attribute. To configure incomplete path information, specify only a subset of router hops. Select the Loose attribute in places where the path is incomplete. For incomplete paths, the MPLS routers complete the path by querying the local routing table. This query is performed on a hop-by-hop basis, and each router can obtain only enough information to reach the next explicit hop. It might be necessary to traverse a number of routers to reach the next (loose) explicit hop.</p> 3. Type an IP address in the IP address text box. 4. Click Add to add the path to the table that displays all the configured paths. Alternatively, select a path from the table and click Delete to remove the path for the LSP.

Item	Action
Hop limit	<p>Specify the hop limit of the LSP.</p> <p>Range: 2 through 255. A path with two hops consists of the ingress and egress routers only.</p> <p>Default: Each LSP can traverse a maximum of 255 hops, including the ingress and egress routers.</p>
Class of service	<p>Select one of the following values to specify the class of service (CoS) type for the LSP:</p> <ul style="list-style-type: none"> • Background—Background type applications such as e-mail and FTP; has a CoS value of 1 • Best Effort—Traffic to be transmitted as a best-effort type; has a CoS value of 0 • Excellent Effort—Traffic to be transmitted as an excellent-load type; has a CoS value of 3 • Critical Applications—Traffic to ensure a high-quality user experience for users of business-critical applications; has a CoS value of 2 • Video < 100 ms—Streaming type applications such as video on demand and multimedia messaging; has a CoS value of 5 • Voice < 10 ms—Voice messaging such as VoIP; has a CoS value of 6 • Internetwork Control—Packets with internetwork control precedence; has a CoS value of 4 • Network Control—Packets with network control precedence; has a CoS value of 7. <p>CoS enables both subscribers and services to be differentiated from each other. Premium subscribers can be prioritized over basic subscribers, while real-time services can be prioritized over non-real-time services. The importance of QoS increases during periods of congestion. An unloaded network can meet the needs of all subscribers and services. However, as the network load increases, the prioritization of traffic determines whether performance for subscribers and services can be maintained or be degraded.</p> <p>The high-order 2 bits of the CoS value select which transmit queue to use on the outbound interface card. The low-order bit of the CoS value is treated as the PLP bit and is used to select the RED drop profile to use on the output queue. If the low-order bit is 0, the non-PLP drop profile is used, and if the low-order bit is 1, the PLP drop profile is used. Typically, RED aggressively drops packets that have the PLP bit set. For more information about RED and drop profiles, see the <i>Junos OS Class of Service Configuration Guide</i>.</p> <p>This field is not applicable for local-protection type of LSPs.</p>
Bandwidth (Kbps)	<p>Specify a bandwidth in Kbps for an LSP. Each LSP has a bandwidth value. This value is included in the sender's Tspec field in RSVP path setup messages. You can specify a bandwidth value in bits per second. If you configure more bandwidth for an LSP, it should be able to carry a greater volume of traffic. The default bandwidth is 0 bits per second.</p>
Standby (enable switchover)	<p>Select this check box to have the path remain up at all times to provide immediate switchover if connectivity problems occur.</p> <p>This check box is displayed only for secondary paths.</p>

Item	Action
Adaptive	<p>Select this check box if you want to configure an LSP to be adaptive when it is attempting to reroute itself. When it is adaptive, the LSP holds onto existing resources until the new path is successfully established and traffic has been cut over to the new LSP. To retain its resources, an adaptive LSP does the following:</p> <ul style="list-style-type: none"> • Maintains existing paths and allocated bandwidths—This ensures that the existing path is not torn down prematurely and allows the current traffic to continue flowing while the new path is being set up. • Avoids double-counting for links that share the new and old paths—Double-counting occurs when an intermediate router does not recognize that the new and old paths belong to the same LSP and counts them as two separate LSPs, requiring separate bandwidth allocations. If some links are close to saturation, double-counting might cause the setup of the new path to fail. <p>By default, adaptive behavior is disabled.</p> <p>You can include the adaptive statement in two different hierarchy levels. If you specify the adaptive statement at the LSP hierarchy levels, the adaptive behavior is enabled on all primary/secondary paths of the LSP. This means both the primary and secondary paths share the same bandwidth on common links.</p> <p>This check box cannot be selected for P2MP topology and also when the path selection type is explicit path.</p>
Priority	Configure the LSP's preemption properties by selecting a value from the Setup Priority and Hold Priority lists.
Setup Priority	<p>Specify a priority value, which determines whether a new LSP that preempts an existing LSP can be established. For preemption to occur, the setup priority of the new LSP must be higher than that of the existing LSP. Also, the act of preempting the existing LSP must produce sufficient bandwidth to support the new LSP. That is, preemption occurs only if the new LSP can be set up successfully. The setup priority also defines the relative importance of LSPs on the same ingress router. When the software starts, when a new LSP is established, or during fault recovery, the setup priority determines the order in which LSPs are serviced. Higher-priority LSPs tend to be established first and hence enjoy more optimal path selection.</p> <p>This field cannot be configured for local-protection type of LSPs.</p> <p>Range: Both setup-priority and reservation-priority can be a value from 0 through 7, where 0 is the highest priority and 7 is the lowest priority.</p> <p>Default: An LSP has a setup priority of 7 (that is, it cannot preempt any other LSPs) and a reservation priority of 0 (that is, other LSPs cannot preempt it). These defaults prevent preemption. When you are configuring these values, make sure that the setup priority value is lower than or equal to the hold priority value.</p>
Hold Priority	<p>Specify a hold priority value.</p> <p>This field cannot be configured for local-protection type of LSPs.</p> <p>Range: 0 through 7, where 0 is the highest priority and 7 is the lowest priority.</p> <p>The hold priority determines the degree to which an LSP holds onto its session reservation of the LSP that has been set up successfully. When the hold priority is high, the existing LSP is less likely to give up its reservation and, therefore, it is unlikely that the LSP can be preempted. You must configure the hold priority to be greater than or equal to the setup priority.</p> <p>NOTE: If traffic engineering admission control determines that there are insufficient resources to accept a request to set up a new LSP, the setup priority is evaluated against the hold priority of existing LSPs. An LSP with a hold priority lower than the setup priority of the new LSP can be preempted. The existing LSP is terminated to make room (that is, resources are freed) for the new LSP.</p>

2. View any administrative groups that are configured on the device. You can configure any new administrative groups.

Administrative groups, also known as link coloring or resource class, are manually assigned attributes that describe the color of links, such that links with the same color conceptually belong to the same class. You can use administrative groups to implement a variety of policy-based LSP setups. Administrative groups are meaningful only when constrained-path LSP computation is enabled (CSPF, instead of Explicit Path).

You can assign up to 32 names and values (in the range 0 through 31), which define a series of names and their corresponding values. The administrative names and values must be identical across all routers within a single domain.

If all interfaces are set to green or yellow, they are all appropriate to be used. The primary path must transit green or yellow links and must stay away from red links. The primary path is periodically recomputed and reoptimized. Finally, this path always keeps the secondary path in hot-standby state for quick failover. You can exclude the red interfaces or links from being part of the LSP.

Fill in the parameters as indicated in the following table under the Admin Groups table of the Path Parameters page.

Field	Action
Include-all	Select an administrative group from the menu to specify that the LSP must traverse links that include all of the defined administrative groups.
Include-any	Select an administrative group from the menu to define the administrative groups to include in an LSP or a path's primary and secondary paths.
Exclude	Select an administrative group from the menu to define the administrative groups to exclude from an LSP or a path's primary and secondary paths.

3. Click **Next** to proceed to the final step of the wizard, which is to review the configured settings.

The **Review** page of the wizard is displayed.

Alternatively, click the **Primary** tab to define the primary path settings of the LSP.

Configuring LSP Primary Path Settings

This page is unavailable if the value in the **LSP protection type** field is **Local Protection Only**.

On the Path Settings page, click the **Primary** tab. The **LSP Primary Path Settings** page enables you to configure primary paths on one point-to-point or several point-to-multiple-point branches. Specify the primary path to use for an LSP. You can configure only one primary path. You can optionally specify the preference, CoS, and bandwidth values for the primary path, which override any equivalent values that you configure for the LSP.

Create RSVP LSP Service Order.

General Settings > Node Parameters > **Path Settings** > Review

You are here: Path Settings

LSPs

name
480R4_SV_Alok_re->960R1_SV_Alok_re
960R1_SV_Alok_re->480R4_SV_Alok_re

Configuration for LSP:

Primary Secondary

Path name: Automatic View Create

Path Settings

Class Of Service: [dropdown]

Hop Limit: 255

Bandwidth (Kbps): [dropdown]

☐ Standby (enable switchover)

☐ Adaptive

Priority: [dropdown]

Admin Groups

Existing Admin Groups on Router Y

Name	Group Name
Admin Groups	
Include-all:	[dropdown]
Include-any:	[dropdown]
Exclude:	[dropdown]

Back Next Done Cancel

The settings that you configured in the selected LSP service definition populate the fields on this page. If you chose to create a custom LSP service order on the General Settings page of the wizard, the fields are not populated.

1. Fill in the parameters as indicated in the following table.

Item	Action
Primary Path	<p>Select a primary path from the LSPs pane on the left. Based on the Topology type, the paths are listed in the following pattern:</p> <ul style="list-style-type: none"> • P2P topology <i>Ingress router-> Egress router</i> • P2MP topology <i>Ingress router-> Egress router 1</i> <i>Ingress router->Egress router 2</i> • Full Mesh topology <i>Router 1-> Router 2</i> <i>Router 2-> Router 1</i>
Path Name	<p>From the list, select the path name that you want. This is a required field.</p> <p>For a primary path <i>Ingress router-> Egress router</i> , the Path Name list contains the paths on the ingress router.</p>

Configure any primary path setting that you selected in the LSP service definition to be editable in the LSP service order. You cannot change any setting that you configured in the LSP service definition to not be editable.

2. Click the **Secondary** tab on the Node Settings page.

The **LSP Secondary Path Settings** page appears.

Configuring LSP Secondary Path Settings

This page is unavailable if the value in the **LSP protection type** field is **Local protection only**, or if the value in the **Topology** field is **P2MP**.

On the Path Settings page, click the **Secondary** tab. The **LSP Secondary Path Settings** page enables you to configure primary paths on one point-to-point or several point-to-multiple-point branches. The settings that you configured in the selected LSP service definition populate the fields on this page. The fields are not populated with values if you chose to create a custom LSP service order on the General Settings page of the wizard.

Create RSVP LSP Service Order.

General Settings

Node Parameters

Path Settings

Review

You are here: Review

Service Details

Basic

Advanced

LSP Type:

Topology:

Path Selection Type:

LSP Protection Type:

RSVP

Full Mesh

CSPF

Path Protection

Pattern Details

Order Name:

Pattern Name:

LSP_SO

Full Mesh Default Pattern

Back

Next

Done

Cancel

1. Fill in the parameters as indicated in the following table.

Item	Action
Secondary Path	<div>Select a secondary path from the LSPs pane on the left. Based on the Topology type, the paths are listed in the following pattern:</div> <div><div><div>• P2P topology</div><div><i>Ingress router</i>→ <i>Egress router</i></div></div><div><div>• Full Mesh topology</div><div><i>Router 1</i>→ <i>Router 2</i></div><div><i>Router 2</i>→ <i>Router 1</i></div></div></div>
Path Name	<div>From the list, select the path name that you want. This is a required field.</div> <div>For a primary path <i>Ingress router</i>→ <i>Egress router</i> , the Path Name list contains the paths on the ingress router.</div>

Configure any secondary path setting that you selected in the predefined LSP service definition to be editable in the LSP service order.

2. Click **Next** to proceed to the final step of the wizard, which is to review the configured settings.

The **Review** page of the wizard is displayed.

Reviewing the Configured Settings

The Review page of the service definition or service order creation and modification wizards enable you to view and evaluate the service parameters and components you configured in the preceding steps or on the preceding pages of the wizard. This page provides a comprehensive, single-page view of all the service elements configured using the different pages of the wizard. You can either click the buttons corresponding to the various settings at the top of the wizard page to directly traverse to the page you want to modify or click the navigation buttons at the bottom of the wizard page to go to the different pages of the wizard.

To examine the configured settings, and modify them as needed:

1. Click **Review** to view the defined parameters.

You can examine and modify the created service order parameters. Alternatively, click the corresponding buttons at the top of the wizard page to navigate to the specific pages that pertain to the settings you want to modify.

Create RSVP LSP Service Order.

General Settings > Node Parameters > Path Settings > **Review**

You are here: Review

- Service Details
- Pattern Details
- Node Parameters** Edit
 - Topology: Full Mesh
 - Full Mesh**

Name	IpAddress	State	Managed S...	Platform	OS Version	Roles
480R4_SV_...	10.102.162.222	up	In Sync	MX480	15.1-201501...	N_PE
960R1_SV_...	10.102.163.58	up	In Sync	MX960	15.1-201501...	N_PE
- Path Settings** Edit
 - Path Settings**

Source	Destination	LSP Path Name
480R4_SV_Alok_re	960R1_SV_Alok_re	480R4_SV_Alok_re->960R1_SV_A...
960R1_SV_Alok_re	480R4_SV_Alok_re	960R1_SV_Alok_re->480R4_SV_A...

Page 1 of 1

Back Next Done Cancel

2. Click **Edit** beside any of the sections to modify the parameters corresponding to that section.

You are taken to the page pertaining to the parameter in the wizard.

3. Click **Finish** to save the service order.
4. Click **Back** to return to the previous page of the wizard; otherwise, click **Cancel** to discard the changes.

The service order inventory window appears.

Viewing the Configured LSP Services

To view and determine the status of LSP services in a tabular form:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Build** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the View pane, click the plus sign (+) to expand the tree and select the type of service.
4. In the Network Services > Tunnel task pane, select **Service Provisioning > View LSPs**.

The View LSP Services page is displayed with a table of services on the system appears in the bottom pane of the main display area. The following fields are displayed on this page:

[Table 114 on page 808](#) describes the fields in the View LSP Services table.

Table 249: Fields in the Services Table

Field	Description
Name	Name of the service order assigned during service creation or edit.
Service Type	Label-switched path (LSP)
State	State of the service: <ul style="list-style-type: none"> • Active—Denotes a service that has been deployed and is in an active state (enabled). • Inactive—Denotes a service that has been deployed and is in a deactivated state (disabled). • Pending—Denotes a service for which deployment of the service to a device is pending to be performed. • Failed—An attempt to modify the service failed.
FA Status	Status of functional audit of the service.

Table 249: Fields in the Services Table (continued)

Field	Description
Fault Status	Fault management status of the service.
SLA Status	Service-level agreement status of the service. If data exceeds the threshold value specified in the Threshold Alarm Profile, the system generates a threshold alarm. The value in the SLA Status column changes to SLA Violated. If the data does not cross the threshold value specified in the Threshold Alarm Profile, the value in the SLA Status column changes to SLA Violation Cleared.
PM Status	Performance management status of the service.
Definition	Name of the service definition upon which the service order is based.
Activation Date	Date and time at which the service order was last activated.
Last Modified Time	Date and time at which the profile was last updated.

In the View pane, if you select the Tunnel item in the tree under Network Services, without expanding the tree and selecting a specific service type, such as RSVP LSPs, the top pane displays a set of five pie charts that enable you to view the different service orders configured, and their associated audit and monitoring statuses. The FA Status chart displays the functional audit status for the service orders. The Device State graph displays the statuses of devices on which services are being provisioned and commissioned. The Fault Status chart displays the connectivity fault management details for the service orders. The SLA Status chart displays the service-level agreement details for the service orders. The PM Status chart displays the performance management details for the service orders. The count or percentage of service orders in the pie chart segments sum up to the total number of configured service orders. Mouse over each segment of the pie to view the number corresponding to the percentage of service orders for each of the charts. These charts provide a visual overview of customers and service orders on your network, and enables you to quickly access related and commonly needed information. For example, you can check for failed service orders and then access a list of failed requests so you can begin to take restoration measure.

5. To view details of a specific service, double-click the table row that summarizes the service.

Modifying an Explicit Path in RSVP LSP Services

In explicit routing, the route the label-switched path (LSP) takes is defined by the ingress node. The path consists of a series of hops defined by the ingress label-switching router (LSR). Each hop can be a traditional interface, an autonomous system, or an LSP. You can choose a new explicit path from the existing paths, create and map a new explicit path, and delete the explicit path associated with RSVP service. When explicit-path LSPs are configured, the LSP is established along the path you specified.

The **Path Settings** page of the service order modification wizard enables you to view existing paths or add, edit, or delete paths.

To configure an explicit-path LSP:

1. Select **Service View** from the View selector.
The workspaces that are applicable to routing and tunneling services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon on the Connectivity Services Director banner.
The functionalities that you can configure in this mode are displayed in the Tasks pane of the GUI window.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. From the Service View pane, click the plus sign (+) sign next to Tunnels, and select RSVP LSPs.
5. From the Tasks pane, select **Service Provisioning > Manage LSP**. The Manage Network Services page is displayed in on the top right main display area, and the Manage Service Deployment window is displayed on the bottom of the main display area.
6. Select an RSVP service and click **Modify**. The Modify LSP service wizard appears.



NOTE: You can modify the primary path or the secondary path of an RSVP service only.

7. Navigate to the Path Settings page of the wizard.

This page is unavailable if the **LSP protection type** is **Local Protection Only**.

From the Path Settings page, click the **Primary** tab. The **LSP Primary Path Settings** page enables you to configure primary paths on one point-to-point or several point-to-multiple-point branches. Specify the primary path to use for an LSP. You

can configure only one primary path. You can optionally specify preference, CoS, and bandwidth values for the primary path, which override any equivalent values that you configure for the LSP.

From the Path Settings page, click the **Secondary** tab. The **LSP Secondary Path Settings** page enables you to configure primary paths on one point-to-point or several point-to-multiple-point branches. The settings that you configured in the selected LSP service definition populate the fields on this page. The fields are not populated with values if you chose to create a custom LSP service order in the General Settings page of the wizard.

8. Modify the primary and secondary path.

To modify the primary or secondary path:

- a. Select a primary path or secondary path from the LSPs pane on the left. Based on the **Topology** type, the paths are listed in the following pattern:

- **P2P** topology

Ingress router—> Egress router

- **Full Mesh** topology

Router 1—> Router 2

Router 2—> Router 1

- b. Select the **Automatic** radio button for an automatic path to be used for the LSP for the primary path or secondary path.

9. Create a new path.

To create a new primary or secondary path:

- a. Select the **Create New** radio button to create a new path. The fields to create a new path are displayed in the Path Name section.

- b. Specify the following fields:

- **Path Name**—Name of the new path
- **IP address**—IP address of the new path
- **Loose/Strict**—Explicit Route Objects (EROs) type.

EROs limit LSP routing to a specified list of LSRs. By default, RSVP messages follow a path that is determined by the network IGP's shortest path. However, in the presence of a configured ERO, the RSVP messages follow the path specified. EROs consist of two types of instructions: loose hops and strict hops.

When a loose hop is configured, the hop denotes one or more transit LSRs through which the LSP must be routed. The network IGP determines the exact route from the inbound router to the first loose hop, or from one loose hop to the next. The loose hop specifies only that a particular LSR be included in the LSP.

When a strict hop is configured, the hop identifies an exact path through which the LSP must be routed. Strict-hop EROs specify the exact order of the routers through which the RSVP messages are sent.

- c. Click **Add** to add the new path.

The new path now appears in the primary and secondary paths list.

10. Click **Modify**.

Connectivity Services Director modifies the explicit path of a RSVP LSP service. If the path is topologically not feasible, either because the network is partitioned or insufficient resources are available along some parts of the path, the LSP fails. No alternative paths can be used.

If the setup succeeds, the LSP stays on the defined path indefinitely.



NOTE: Select the View Deployment Jobs option on the tasks pane in Deploy mode to check whether the deployment jobs completed successfully.

Modifying an RSVP LSP Service

You can modify the name of a RSVP LSP service. After modifying a service, the configuration audit and functional audit information is cleared and the functional audit status is set to pending.

To modify the attributes of a service:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon on the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. From the Service View pane, click the plus sign (+) sign next to Tunnels, and select RSVP LSPs.
5. From the task pane, select **Service Provisioning > Manage LSP**. The Manage Network Services window is displayed in the top part of the right pane, and the Manage Service Deployment window is displayed in the bottom part of the right pane.
6. Select an RSVP service, and click **Modify**. The Modify LSP service wizard appears.



NOTE: You can modify the primary path or the secondary path of an RSVP service only.

7. Modify the fields.

For example, you can enable or disable BFD for a BFD LSP service.



NOTE: You can modify only those fields, which are editable in the service order.

The **Full Mesh** template implementation supports the generic attributes (at device level) that are common across LSPs.



NOTE: You cannot assign specific values to each of the LSPs, because the **Full Mesh** template design does not support such a modification.

For a RSVP LSP service, you can also modify the primary and secondary path. For more information on modifying the paths, see [“Modifying an Explicit Path in RSVP LSP Services” on page 1751](#).

For a full mesh RSVP service you can add or delete the devices.

8. Click **Modify**.

The software modifies the service.

9. Use the Jobs workspace to check for successful completion of the action.

Viewing LSP Services in Deploy Mode

To view and determine the status of LSP services in a tabular form:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the View pane, click the plus sign (+) to expand the tree and select the type of service.
4. In the Network Services > Tunnel task pane, select **Service Provisioning > Deploy Services**.

The Manage LSP Services page is displayed in the upper half of the window.

A table of services on the system appears in the main display area. The following fields are displayed on this page:

In the top half of the window on the right pane, the Manage Network Services page presents information on existing services in a table.

The **Manage LSP Services** page provides the following information about each service:

[Table 114 on page 808](#) describes the fields in the service orders table.

Table 250: Fields in the Services Table

Field	Description
Name	Name of the service order assigned during service creation or edit.
Service Type	Label-switched path (LSP)
Customer	Name of the enterprise customer who placed an order for the service.
Deployment State	State of the service: <ul style="list-style-type: none"> • Active—Denotes a service that has been deployed and is in an active state (enabled). • Inactive—Denotes a service that has been deployed and is in a deactivated state (disabled). • Pending—Denotes a service for which deployment of the service to a device is pending to be performed. • Failed—An attempt to modify the service failed.
FA Status	Status of functional audit of the service.
Fault Status	Fault management status of the service.
SLA Status	Service-level agreement status of the service. If data exceeds the threshold value specified in the Threshold Alarm Profile, the system generates a threshold alarm. The value in the SLA Status column changes to SLA Violated. If the data does not cross the threshold value specified in the Threshold Alarm Profile, the value in the SLA Status column changes to SLA Violation Cleared.
PM Status	Performance management status of the service.
Definition	Name of the service definition upon which the service order is based.
Activation Date	Date and time at which the service order was last activated.
Last Modified Time	Date and time at which the profile was last updated.

From this page, you can create a service order, modify the properties of the service order, conduct a functional or configuration audit, deploy or deactivate the service

order, and view alarms associated with a particular service order for debugging and corrective action.

5. To view details of a specific service, double-click the table row that summarizes the service.

Viewing LSP Service Orders in a Table

To view and determine the status of RSVP LSP service orders in a tabular form:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the View pane, click the plus sign (+) to expand the Network Services > Tunnel > RSVP LSPs tree and select the type of service.
4. in the Network Services > Tunnel > RSVP LSPs View pane, select **Service Provisioning > Manage LSP**.

The Manage LSP Deployment page is displayed on the right pane.

Name	Service Type	State	Latest Job	Created Date	Created By
p2plspd	LSP	Completed	196650	2015-09-01T10:43:06.0...	super

A table of service orders on the system appears in the main display area. The following fields are displayed on this page:

- Name—Unique name assigned to the service.
- Customer—Name of the customer for which the service is provided.
- State:

- Completed—Service order has been successfully deployed.
- Failed—Device is down or the Connectivity Services Director application was unable to push the service configuration to a device configured for the service.
- In-progress—Connectivity Services Director application is in the process of deploying the service.
- Requested—Service provisioner has created the service order, but has not yet attempted to deploy it or schedule it for deployment.
- Scheduled—Service provisioner has scheduled the service order for deployment.
- Invalid—Service order contains invalid data.
- Validated—When all the information in the service order is successfully validated, the service order transitions to the Validated state.
- Service Type:
 - LSP (Label-switched path)
- Latest Job—Unique identifier assigned by the system for a deployment job. Click the link in the job ID to open the CSD Deployment Jobs. The table on that page lists configuration deployment jobs.
- Signaling Type:
 - BGP
 - LDP
- Created By—The screen name of the user who created the service order
- Created Date—The date and when you created the service order.

From this page, you can create a service order, modify the properties of the service order, conduct a functional or configuration audit, deploy or deactivate the service order, and view alarms associated with a particular service order for debugging and corrective action.

5. To view details of a specific service order, double-click the table row that summarizes the service order.

Deactivating an LSP Service

This procedure disables a service for a particular protocol that you have previously created on the network. By disabling a service, the traffic processing for the traversed packets is impacted. In certain network topologies, you might require a service-related settings to be disabled for a certain period to perform troubleshooting or modification to the traffic-handling method, and you might want to reactivate a disabled service later when you have completed network maintenance and analysis work. In such a case, it might be beneficial to use the deactivation functionality for a service order. When you disable a service, the configuration attributes associated with such a service are deactivated and commented out in the device settings. The deactivated service is propagated to the

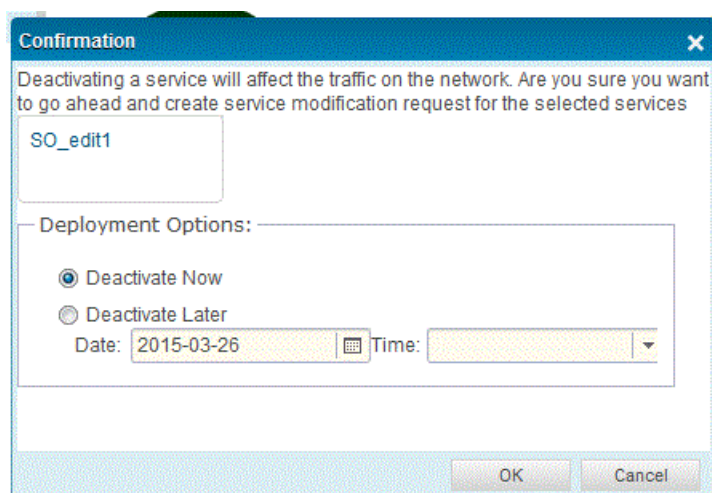
devices associated with the service. To disable a service, the service must not contain any pending or uncommitted changes. Also, the service must be in the Deployed or Re-Activated state.



NOTE: To modify a service order, it must not be in the Deactivated state.

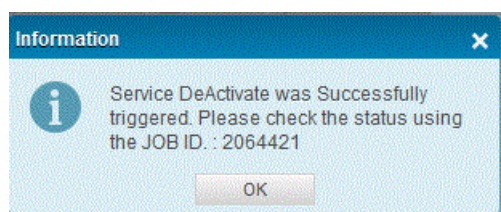
To deactivate a service:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside Tunnel to view services based on protocols, and expand the **RSVP LSPs** tree to select an LSP service.
5. From the task pane, select **Service Provisioning > Manage LSP**. The top part of the right pane displays the Manage LSP Network Services page, with the table of services, and the bottom part of the right pane displays the Manage LSP Service Deployment page, with the table of service orders.
6. From the Manage Network Services page, select the check box next to the service you want to deactivate.
7. Click the down arrow on the **Action** menu, above the table of listed services, and select **Deactivate** to disable the selected service. A dialog box is displayed prompting you to confirm your action.



8. Do one of the following in the Confirmation dialog box:

- To deactivate the service immediately, select Deactivate now, and click Yes. If you click Yes, a pending change request is created for each selected service. Alternatively, if you click No, the deactivate operation is discarded.
- To deactivate the service at a later time, select Deactivate later, and select a date and time for deployment, then click OK. The time field specifies the time kept by the server, but in the time zone of the client. After scheduling the service order for deactivation, the provisioning software begins validating the service order.



9. Use the Jobs workspace to monitor the outcome of the deployment.

Related Documentation

- [Reactivating a Service on page 862](#)
- [Force-Deploying a Service on page 864](#)
- [Decommissioning a Service on page 868](#)

Reactivating an LSP Service

After you disable a service to deactivate the configuration settings on devices mapped to the service, you might require the service settings to be reenabled after you have modified the service parameters, either directly on the device or using the Connectivity Services Director application. In such a case, you can use the reactivation functionality to revive and activate the service properties on devices. To disable a service, the service

must not contain any pending or uncommitted changes. Also, the service must be in the Deactivated state.

To reactivate a service:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside **Tunnel** to view services based on protocols, and expand the **RSVP LSPs** tree to select an LSP service.
5. From the task pane, select **Service Provisioning > Manage LSP**. The top part of the right pane displays the Manage LSP Network Services page, with the table of services, and the bottom part of the right pane displays the Manage LSP Service Deployment page, with the table of service orders.
6. From the Manage Network Services page, select the check box next to the service you want to reactivate.
7. Click the down arrow on the Action menu, above the table of listed service orders, and select Reactivate to reenable the selected service order. A dialog box is displayed prompting you to confirm your action.
8. Do one of the following in the Confirmation dialog box:
 - To reactivate the service immediately, select Reactivate now, and click Yes. If you click Yes, the selected service is activated immediately. Alternatively, if you click No, the deactivate operation is discarded.
 - To reactivate the service at a later time, select Reactivate later, and select a date and time for reactivating, then click OK. The time field specifies the time kept by the server, but in the time zone of the client.
9. Use the Jobs workspace to monitor the outcome of the deployment.

**Related
Documentation**

- [Reactivating a Service on page 862](#)
- [Force-Deploying a Service on page 864](#)
- [Decommissioning a Service on page 868](#)

Force-Deploying an LSP Service

When a service fails a configuration audit because configuration changes on a PE device do not match the configuration required for the service, you can force-deploy the service to push the configuration to the device.

Force deployment pushes the same configuration to the device that was pushed during the deployment of the service, thus allowing the operator to recover from a state in which the configuration on the device was lost or changed out-of-band.

The validation before generating the configuration for a force-deployed service order will be performed against the current configuration on the device and the configuration is not pushed if the validation fails. If the forced deployment is unable to push the configuration again, then you might need to manually configure the device.

This procedure forces deployment of a service on the network.

You cannot force-deploy an invalid service order.

To schedule a service for forced deployment:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside Tunnel to view services based on protocols, and expand the **RSVP LSPs** tree to select an LSP service.
5. From the task pane, select **Service Provisioning > Manage LSP**. The top part of the right pane displays the Manage LSP Network Services page, with the table of services, and the bottom part of the right pane displays the Manage Service Deployment page, with the table of service orders.
6. From the Manage LSP Network Services page, select the check box next to the service you want to forcibly deploy.

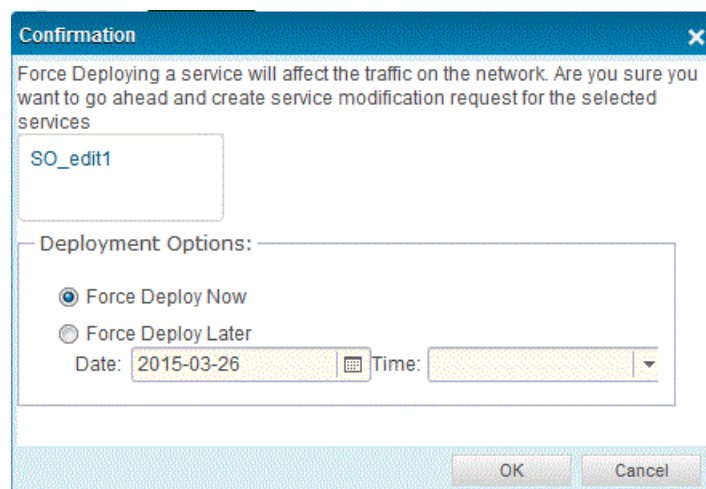
The top pane displays information about the services that have been previously created, such as the name of the service, the functional audit status, the performance management status, and the deployment state of the service. You can modify the properties of the service, conduct a functional or configuration audit, force-deploy or

deactivate the service, and view alarms associated with a particular service order for debugging and corrective action. Services can be in one of the following service states:

- **Completed**—The service order has been successfully deployed.
- **Scheduled for deployment**—The service provisioner has scheduled the service order for deployment.
- **Deployment Failed**—An attempted service deployment was not successfully completed or failed an audit.
- **In Progress**—The Connectivity Services Director application is in the process of deploying the service.
- **Requested**—The service provisioner has created the service order, but has not yet attempted to deploy it or schedule it for deployment.
- **Invalid**—The service order is not valid.

7. Open the **Actions** menu and click **Force Deploy Service**.

The **Schedule Force Deployment** window appears.



8. To deploy the service immediately, select **Force deploy now**, and click **OK**.

To deploy the service at a later time, select **Force deploy later**, select a date and time for deployment, then click **OK**.

The time field specifies the time kept by the server, but in the time zone of the client.

After scheduling the service order for deployment, the provisioning software begins validating the service order.

9. Use the Jobs workspace to monitor the outcome of the forced deployment.

Related Documentation

- [Deactivating a Service on page 860](#)
- [Reactivating a Service on page 862](#)

- [Decommissioning a Service on page 868](#)

Viewing Alarms for an LSP Service

Activity on a network device consists of a series of events. A software component on the network device, called an entity, is responsible for running the Simple Network Management Protocol (SNMP) to log and monitor these events. You can view the details of alarms and events generated for a particular service order to examine and diagnose the problems that are generating the alarms. These alarms provide essential and cohesive information about system conditions, any discrepancies and malfunctioning, and protocols or components that need to be examined and debugged for better efficiency and working capacity.

To view alarm and event details for a service:

1. Select Service View from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Build** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. Click the plus sign (+) beside Tunnel to view services based on protocols, and expand the **RSVP LSPs** tree to select an LSP service.
4. From the task pane, select **Service Provisioning > Manage LSP**. The top part of the right pane displays the Manage Network Services page, with the table of services, and the bottom part of the right pane displays the Manage Service Deployment page, with the table of service orders.
5. Select the check box next to the service for which you want to view alarm details.
6. Click the **View Alarms** button, above the table of listed services.
The Alarm Detail dialog box is displayed.
7. Click **Close** after you finish evaluating the information to return to the Manage Network Services page.

Related Documentation

- [Alarm Detail Monitor \(Service View\) on page 1280](#)

Managing Deployment of LSP Services Configuration to Devices

When you make configuration changes in Build mode, the changes are not deployed to devices automatically. You must manually deploy the changes to devices in Deploy mode.

To start deploying configuration changes:

1. From the View selector, select **Service View**. The workspaces that are applicable to this view are displayed.
2. Click **Deploy** in the Connectivity Services Director banner.
3. Click the plus sign (+) beside Tunnel to expand the tree in the View pane and view the list of service types.
4. Expand the RSVP LSPs tree to view the list of LSPs.
5. In the Tasks pane, select **Service Provisioning > Manage LSP**. The Manage LSP Service Deployment window is displayed in the bottom part of the right pane.



TIP: From Build mode of Service View, in the View pane, if you select the Connectivity item in the tree under Network Services, without expanding the tree and selecting a specific service type, such as P2P Services, L3VPN Services, or VPLS Services, the top pane displays a set of five pie charts that enable you to view the different service orders configured, and their associated audit and monitoring statuses. The FA Status chart displays the functional audit status for the service orders. The Device State graph displays the statuses of devices on which services are being provisioned and commissioned. The Fault Status chart displays the connectivity fault management details for the service orders. The SLA Status chart displays the service-level agreement details for the service orders. The PM Status chart displays the performance management details for the service orders. The count or percentage of service orders in the pie chart segments sum up to the total number of configured service orders. Mouse over each segment of the pie to view the number corresponding to the percentage of service orders for each of the charts. These charts provide a visual overview of customers and service orders on your network, and enables you to quickly access related and commonly needed information. For example, you can check for failed service orders and then access a list of failed requests so you can begin to take restoration measure.

In Build mode of Service View, from the View pane, if you select the Network Services node and do not expand the Network Services > Connectivity tree, the top pane displays a pie chart that enables you to view and examine the different services configured for devices, and the types of service protocols configured. The Services by Type graph displays the count of services for each type of service definition. Mouse over each segment of the pie to view the number corresponding to the percentage of service orders for each of the charts. This chart provides a visual overview of customers and service orders on your network, and enables you to quickly access related and commonly needed information. For

example, you can check for failed service orders and then access a list of failed requests so you can begin to take restoration measure.

.....
The following fields are displayed in this window:

- Name—Unique name assigned to the service.
- Customer—Name of the customer for which the service is provided.
- State—State of the service order. Service orders can be one of the following states:
 - Completed—The service order has been successfully deployed.
 - Scheduled for deployment—The service provisioner has scheduled the service order for deployment.
 - Deployment Failed—An attempted service deployment was not successfully completed or failed an audit.
 - In Progress—The Connectivity Services Director application is in the process of deploying the service.
 - Requested—The service provisioner has created the service order, but has not yet attempted to deploy it or schedule it for deployment.
 - Invalid—The service order is not valid.
- Signaling—Type of signaling, namely, BGP or LDP.
- Created By—Name of the user that created the service order.
- Created Date—Date and time at which the service order was created.

This topic describes:

- [Selecting Configuration Deployment Options on page 1765](#)
- [Discarding the Pending Configurations on page 1766](#)
- [Deploying Service Configuration Changes to Devices Immediately on page 1767](#)
- [Scheduling Configuration Deployment of Services on page 1768](#)
- [Specifying Configuration Deployment Scheduling Options on page 1768](#)

Selecting Configuration Deployment Options

Based on the approval mode, you can choose to deploy the device configuration changes in the following ways:

- When you select the auto approval mode, the page Devices with Pending Changes open. From the Devices with Pending Changes page, you can:

- Deploy configuration changes immediately by selecting one or more devices and clicking Deploy Now. For more information, see [“Deploying Configuration Changes to Devices Immediately” on page 759](#).
- Schedule configuration deployment by selecting one or more devices and clicking Schedule Deploy. For more information, see [“Scheduling Configuration Deployment” on page 759](#).
- View configuration changes that are pending on a device by clicking View in the Configuration Changes column.
- Validate that the pending changes for a device are compatible with the device’s configuration by selecting up to ten devices and clicking Validate Pending Configuration Changes.
- Discard the pending configuration changes. For more information, see [“Discarding the Pending Configurations” on page 757](#).

Discarding the Pending Configurations

Use the Discard Local Configuration Changes Results window to discard all the pending configurations that were made on a device. Once you discard the local configuration changes on a device, the configuration state of the device changes to In Sync or Out of Sync based on the system of record (SOR) mode set for the Junos Space Network Management Platform. If the SOR mode is set to Network as system of record (NSOR), then the configuration state changes to In Sync and if the SOR mode is set to Junos Space as system of record (SSOR), then the configuration state changes to Out of Sync.

To discard the configuration changes:

1. From the View selector, select **Service View**. The workspaces that you can configure in this view are displayed.
2. Click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that are applicable to this lifecycle mode are displayed.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside Tunnel to expand the tree in the View pane and click **RSVP LSPs** to view the list of LSP services.
5. From the task pane, select **Service Provisioning > Manage LSP**. The top part of the right pane displays the Manage Network Services page, with the table of services, and the bottom part of the right pane displays the Manage Service Deployment page, with the table of service orders.

6. From the Manage Service Deployment page, select the services for which you want to discard the pending configuration and click **Discard Pending Configuration** from the Actions menu.

The Discard Local Configuration Changes Results window opens displaying the status of the discard pending configuration job.

7. To discard the pending changes of the service immediately, select **Partial delete now**, and click **OK**. To discard the pending changes of the service at a later time, select **Partial delete later**, select a date and time for deletion, then click **OK**. The time field specifies the time kept by the server, but in the time zone of the client. After scheduling the service order for deployment, the provisioning software begins validating the service order.
8. Click **Close** to close the Discard Local Configuration Changes Results window.

Deploying Service Configuration Changes to Devices Immediately

To deploy service configuration changes to devices immediately:

1. From the View selector, select **Service View**. The workspaces that you can configure in this view are displayed.
2. Click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that are applicable to this lifecycle mode are displayed.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside Tunnel to expand the tree in the View pane and click **RSVP LSPs** to view the list of LSP services.
5. From the task pane, select **Service Provisioning > Manage LSP**. The top part of the right pane displays the Manage Network Services page, with the table of services, and the bottom part of the right pane displays the Manage Service Deployment page, with the table of service orders.
6. Select the check box next to the service you want to deploy from the Manage Service Deployment page.
7. Click **Deploy Now**.
The Deploy Options window opens.
8. In the Deploy Options window, enter a job name in the Deployment Job Name field, then click **OK**.

The configuration deployment job runs. The Deploy Configuration window opens and shows the results of the deployment job.

Scheduling Configuration Deployment of Services

To schedule the services configuration deployment to devices:

1. From the View selector, select **Service View**. The workspaces that you can configure in this view are displayed.
2. Click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that are applicable to this lifecycle mode are displayed.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside Tunnel to expand the tree in the View pane and click **RSVP LSPs** to view the list of LSP services.
5. From the task pane, select **Service Provisioning > Manage LSP**. The top part of the right pane displays the Manage Network Services page, with the table of services, and the bottom part of the right pane displays the Manage Service Deployment page, with the table of service orders.
6. Select the check box next to the service you want to deploy from the Manage Service Deployment page.
7. Click **Schedule Deploy**.
The Deploy Options window opens.
8. Use the Deploy Options window to schedule the configuration deployment. See [“Specifying Configuration Deployment Scheduling Options” on page 760](#) for a description of the window.

Specifying Configuration Deployment Scheduling Options

Use the Deploy Options window to schedule configuration deployment jobs. [Table 98 on page 760](#) describes the actions for the fields in this window.

Table 251: Deploy Options Window

Field	Action
Deployment Job Name	Enter a job name.
Date and Time	Enter the job's start date and time.

Table 251: Deploy Options Window (continued)

Field	Action
OK	Click to accept changes and exit the window.
Cancel	Click to cancel changes and exit the window.

Deploying an LSP Service

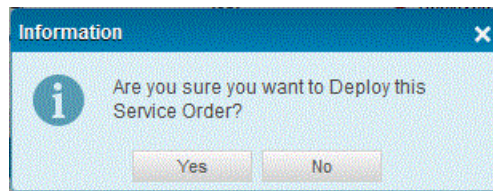
This procedure schedules a service for deployment on the network. Use this procedure to perform the following tasks:

- Deploy a new service.
- Deploy a modified service.
- Redeploy a service order that failed deployment.

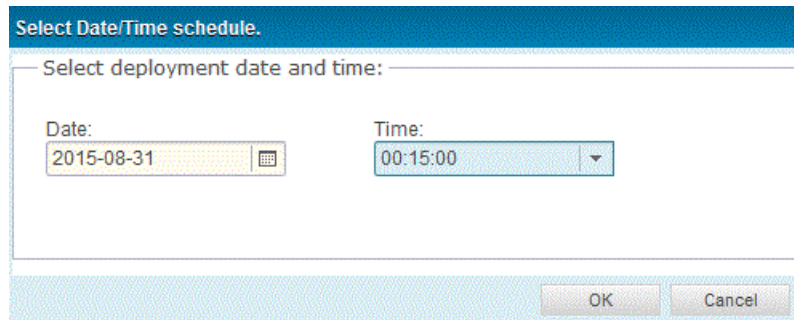
You cannot deploy an invalid service order.

To schedule a service for deployment:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. Click the plus sign (+) beside Tunnel to expand the tree in the View pane and view the list of service types.
4. Expand the RSVP LSPs tree to view the list of LSP services.
5. From the **Network Services > Tunnel** task pane, select **Service Provisioning > Manage LSP**. The Manage Service Deployment page is displayed on the right pane.
6. In the **Manage Service Deployment** page, select the service order that you want to deploy.
7. Click the **Deploy Service Order** button at the top of the page.
The **Deploy Service** window appears.
8. To deploy the service immediately, select **Deploy now**, and click **OK**.



To deploy the service at a later time, select **Schedule Deploy**, and select a date and time for deployment, then click **OK**.



The time field specifies the time kept by the server, but in the time zone of the client.

After scheduling the service order for deployment, the provisioning software begins validating the service order.

9. Use the Jobs workspace to monitor the outcome of the deployment.

Related Documentation

- [Validating the Pending Configuration of a Service Order on page 1018](#)
- [Viewing the Configuration of a Pending Service Order on page 1020](#)

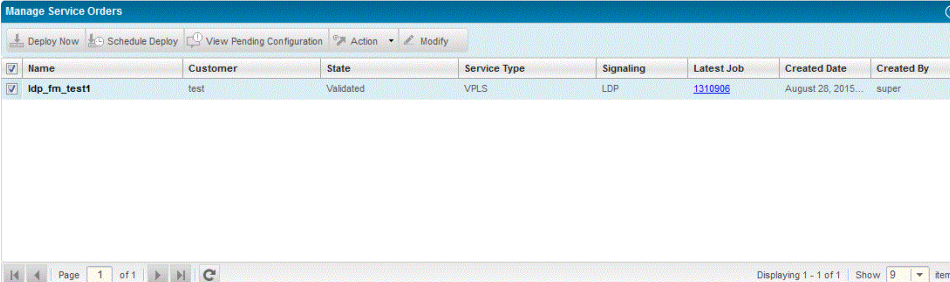
Deleting a Partial Configuration of an LSP Service Order

A failed service order of type Provisioning can leave parts of the service configuration on the devices. To remove this partial configuration:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.

4. Click the plus sign (+) beside Tunnel to expand the tree in the View pane and view the list of service types.
5. Expand the RSVP LSPs tree to view the list of LSP services.
6. From the **Network Services > Tunnel** task pane, select **Service Provisioning > Manage LSP > *service order name***. The top part of the right pane displays the Manage Network Services page, with the table of services, and the bottom part of the right pane displays the Manage Service Deployment page, with the table of service orders.
7. In the **Manage Service Deployment** page, select the failed service order for which you want to delete the partial configuration.
8. Open the **Actions** menu and select **Delete Partial Configuration**.
9. To delete the pending changes of the service immediately, select **Partial Delete Now**, and click **OK**. To discard the pending changes of the service at a later time, select **Partial Delete Later**, select a date and time for deletion, then click **OK**. The time field specifies the time kept by the server, but in the time zone of the client. After scheduling the service order for deployment, the provisioning software begins validating the service order.

Figure 136: Delete Partial Configuration Confirmation



The screenshot shows the 'Manage Service Orders' interface. At the top, there are buttons for 'Deploy Now', 'Schedule Deploy', 'View Pending Configuration', 'Action', and 'Modify'. Below these is a table with the following columns: Name, Customer, State, Service Type, Signaling, Latest Job, Created Date, and Created By. The table contains one row with the following data: Name: ldp_fm_test1, Customer: test, State: Validated, Service Type: VPLS, Signaling: LDP, Latest Job: 1310906, Created Date: August 28, 2015..., Created By: super. At the bottom of the table, there is a pagination bar showing 'Page 1 of 1' and 'Displaying 1 - 1 of 1' items.

Name	Customer	State	Service Type	Signaling	Latest Job	Created Date	Created By
ldp_fm_test1	test	Validated	VPLS	LDP	1310906	August 28, 2015...	super

You are returned to the Manage Service Orders page.

Related Documentation

- [Managing Service Configuration Deployment Jobs on page 1003](#)
- [Deploying Services Configuration to Devices on page 1005](#)
- [Deploy Configuration Window on page 764](#)
- [Managing Jobs on page 118](#)

Deleting an LSP Service Order

You can delete a service order that is in the requested state, the scheduled state, the invalid state, or the failed deployment state. To correct a service order in the invalid state, you must delete it and then recreate it; the Connectivity Services Director application does not support modifying the service order directly.

To delete a service order from the database:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. Click the plus sign (+) beside Tunnel to expand the tree in the View pane and view the list of service types.
4. Expand the RSVP LSPs tree to view the list of LSP services.
5. From the **Network Services > Tunnel** task pane, select **Service Provisioning > Manage LSP**.
6. In the **Manage Service Deployment** page, select the service order to be deleted from the Connectivity Services Director application database.
7. Open the **Actions** menu and select **Delete Service Order**.
A pop-up window appears requesting confirmation.
8. Click **Delete**.

The **Manage Service Deployment** page reappears with the deleted service orders removed.

Related Documentation

- [Creating a Point-to-Point Service Order on page 829](#)
- [Creating a Multipoint-to-Multipoint VPLS Service Order on page 881](#)
- [Creating a Point-to-Multipoint VPLS Service Order on page 905](#)

Validating the Pending Configuration of an LSP Service Order

This procedure validates a service order but does not push the configuration to the device. Use this procedure to perform the following tasks:

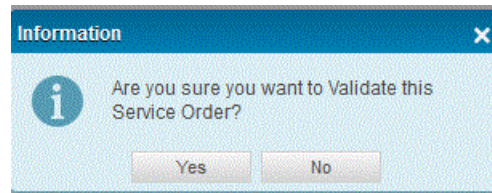
- Validate a service request in the REQUESTED state.
- Validate a service request in the INVALID state after making necessary configuration changes on one or more PE devices associated with the service order.

When you create a service order, it is automatically validated in Connectivity Services Director. However, if subsequent changes to service configuration attributes and settings have occurred for the devices or endpoints to which they are associated, you can use the functionality to validate pending service order configuration. You can validate the configuration of a service order that is in the requested state, the scheduled state, the invalid state, or the failed deployment state

To schedule a service order for validation, follow these steps:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside Tunnel to expand the tree in the View pane and view the list of service types.
5. Expand the RSVP LSPs tree to view the list of LSP services.
6. From the task pane, select **Service Provisioning > Manage LSP**. The top part of the right pane displays the Manage Network Services page, with the table of services, and the bottom part of the right pane displays the Manage Service Deployment page, with the table of service orders.
7. From the Manage Service Deployment page, select the service order you want to validate and save.
8. Open the **Actions** menu and click **Validate Pending Configuration**.

The **Schedule Service Request Validation** window appears.



9. You can validate a service now or at some future time:
 - To validate the service immediately, select **Validate now**, and click **OK**.
 - To validate the service at a later time, select **Validate later**, select a date and time for deployment, and then click **OK**.



NOTE: When specifying a time to validate the service, the time field specifies the time kept by the server, but in the time zone of the client.

After scheduling the service order for validation, the provisioning software begins validating the service order.

10. You can use the **Job Management** window to view details about the service validation.

Related Documentation

- [Deleting a Partial Configuration of an LSP Service Order on page 1014](#)
- [Deleting a Service Order on page 1015](#)
- [Deploying a Service on page 1016](#)

Viewing the Configuration of a Pending LSP Service Order

You can view the configuration of a service order that is in the requested state, the scheduled state, the invalid state, or the failed deployment state.

To view the configuration of such pending service orders:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. Click the plus sign (+) beside Tunnel to expand the tree in the View pane and view the list of service types.
4. Expand the RSVP LSPs tree to view the list of LSP services.

5. From the **Network Services > Tunnel** task pane, select **Service Provisioning > Manage LSP**. The Manage Service Deployment page is displayed on the bottom part of the right pane.
6. Select a service order that is in either of the following states:
 - Requested
 - Invalid
 - Scheduled
 - Failed deployment

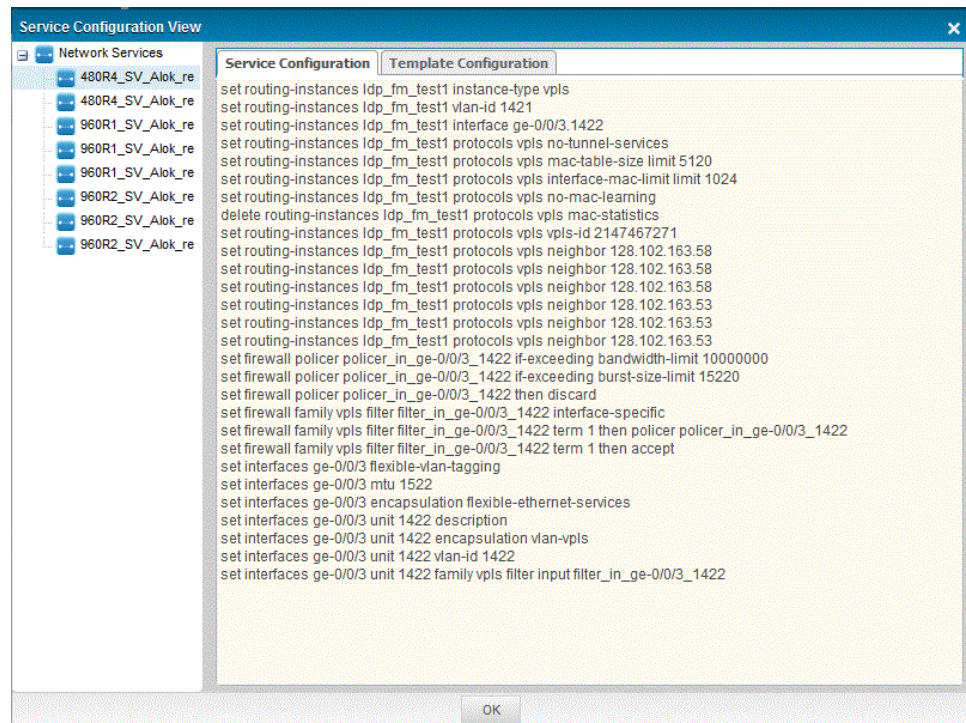


NOTE: The Order State column displays the state of the service order.

7. Select the service order for which you want to view the configuration details.
8. Click the **View Pending Order Configuration** button at the top of the table of listed service orders. The **Service Configuration View** window is displayed. The configuration is displayed in CLI format.



NOTE: The View Pending Order Configuration button on the Manage Service Orders page appears to be dimmed if the service order state is Completed.



9. Select a device to view the configuration details. You can also view the template configuration if a template is attached to the service order.

Based on the application's settings, the configuration is displayed in xml format or in set format. To view the configuration in set format:

1. Select **Platform > Administration > Applications > Connectivity Services Director**.
2. Right-click the Connectivity Services Director application and select **Modify Application Settings**. The Modify Connectivity Services Director Settings window is displayed.
3. Select the **show configuration in set format** check box.

Related Documentation

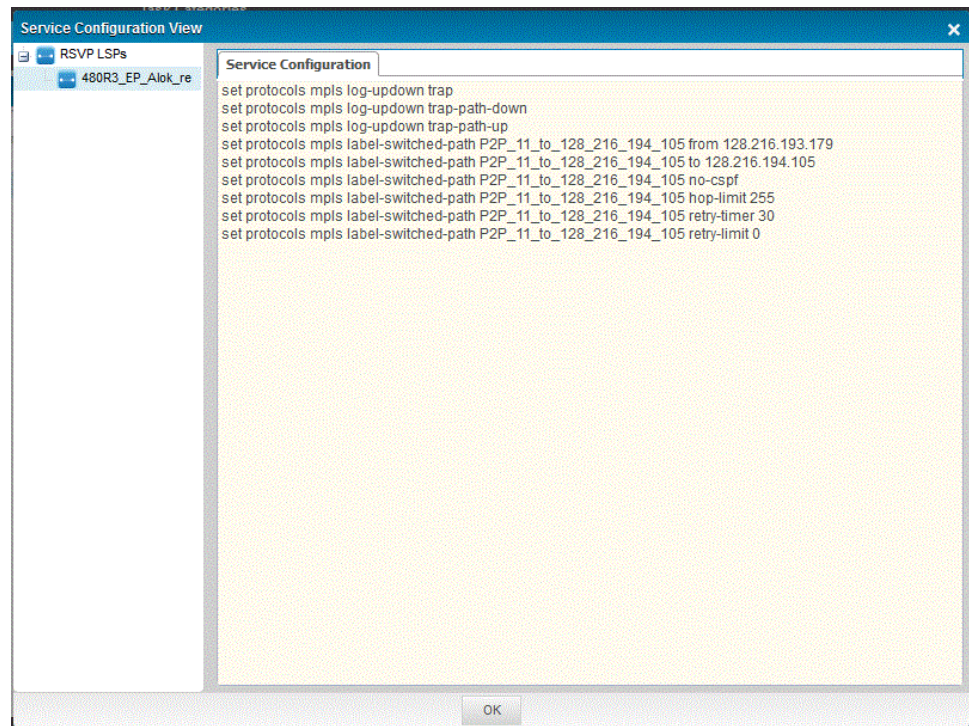
- [Deleting a Partial Configuration of an LSP Service Order on page 1014](#)
- [Deleting a Service Order on page 1015](#)
- [Deploying a Service on page 1016](#)
- [Validating the Pending Configuration of a Service Order on page 1018](#)

Viewing the Configuration Details of RSVP LSP Services

You can view the configuration of an RSVP LSP tunnel service, which enables you to see the parameters and attributes configured for a service on the associated devices in the form of configuration statements and commands that are displayed in the Junos OS CLI interface. You can use these settings to examine the existing service configuration and modify it as necessary to correct any traffic-handling problems or system discrepancies.

To view the configuration of services:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. Click the plus sign (+) beside Tunnels to view services based on protocols, and select **RSVP LSPs** to view the LSP services.
4. From the **Network Services > Tunnels > RSVP LSPs** task pane, select **Service Provisioning > Manage LSP**. The Manage Network Services page is displayed on the top part of the right pane.
5. Select the check box next to a service for which you want to view the configuration details.
6. Click the **View Configuration** option. The Service Configuration View dialog box is displayed. The configuration is displayed in the CLI interface structure and in the form of configuration stanzas.



The left pane displays a tree of devices associated with the specified service. You can select a Service-name > Device-name in the left pane of the window to view the configuration parameters of the corresponding device on the right pane. The right pane contains two tabs— Service Configuration and Template Configuration. The Service Configuration tab displays the settings specified for the service on the device in CLI format. This tab displays the elements or components specified for a service template in the form of configuration stanzas and hierarchy levels. This display is similar to the show command that you can use at a certain [edit] hierarchy level to view the defined settings. The Template Configuration tab displays the service attributes and options defined in the service template, if any, that is associated with the service.

7. Click **OK** to close the dialog box after you complete viewing the configuration attributes and settings.

Related Documentation

- [Deleting a Partial Configuration of an LSP Service Order on page 1014](#)
- [Deleting a Service Order on page 1015](#)
- [Deploying a Service on page 1016](#)
- [Validating the Pending Configuration of a Service Order on page 1018](#)

Viewing Decommissioned LSP Service Orders

In certain situations, you might decommission a service that a customer no longer needs. You cannot decommission a service if a service order requesting action on that service is in the Requested, Scheduled, In Progress, or Invalid state. You can view the decommissioned service orders in a separate page to determine whether you want to delete it completely.

To view and determine the status of RSVP LSP service orders in a tabular form:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the View pane, click the plus sign (+) to expand the Network Services tree and select the Tunnel node.
4. In the Network Services > Tunnel View pane, select **Service Provisioning > Decommissioned Service Orders**.

The Manage LSP Service Deployment page is displayed on the right pane.

Name	Service Type	State	Latest Job	Created Date	Created By
p2plsp_decommission_2015-09-01 10:25...	LSP	Completed	196547	2015-09-01T10:25:50.0...	-
p2plsp	LSP	Completed	196544 ALL	2015-09-01T10:25:12.0...	super

A table of service orders on the system appears in the main display area. The following fields are displayed on this page:

- Name—Unique name assigned to the service.
- Customer—Name of the customer for which the service is provided.

- State:
 - Deployed-Active—Denotes a service that has been deployed and is in an active state (enabled).
 - Deployed-Inactive—Denotes a service that has been deployed and is in a deactivated state (disabled).
 - Deployment-Pending—Denotes a service for which deployment of the service to a device is pending to be performed.
 - Failed Deploy—An attempt to modify the service failed.
- Service Type:
 - LSP (Label-switched path)
- Latest Job—Unique identifier assigned by the system for a deployment job. Click the link in the job ID to open the CSD Deployment Jobs. The table on that page lists configuration deployment jobs.
- Signaling Type:
 - BGP
 - LDP
- Created By—The screen name of the user who created the service order
- Created Date—The date and when you created the service order.

From this page, you can create a service order, modify the properties of the service order, conduct a functional or configuration audit, deploy or deactivate the service order, and view alarms associated with a particular service order for debugging and corrective action.

5. To view details of a specific service order, double-click the table row that summarizes the service order.

Monitoring and Troubleshooting Tunnel Services

- [Performing a Functional Audit for LSP Services on page 1781](#)
- [Viewing Functional Audit Results for LSP Services on page 1789](#)
- [Examining the LSP Summary Details for Effective Troubleshooting on page 1793](#)
- [Troubleshooting the Endpoints of RSVP LSP Services on page 1796](#)
- [Clearing LSP Statistics on page 1801](#)
- [Monitoring Network Reachability by Using the MPLS Traceroute Capability on page 1803](#)
- [Monitoring Network Reachability by Using the MPLS Ping Capability for RSVP LSPs on page 1806](#)

Performing a Functional Audit for LSP Services

A functional audit determines whether a deployed service instance is functioning. It checks the control plane to ensure connectivity among endpoints and that the UNIs are functioning correctly. It also checks the data plane to verify packet transmission between each valid pair of endpoints in the service.

A functional audit works by running commands that perform verification and reporting relevant information.

The following table shows the commands that are used for each service type:

Service Type	Device Family	XML Commands		CLI Commands	
		Data Plane	Control Plane	Data Plane	Control Plane
RSVP LSP	ACX Series, M Series, MX Series	Not supported.	<pre><get-mpls-lsp-information> <name> <i>lspName</i> </name> <ingress> </ingress> </get-mpls-lsp-information></pre>	Not supported.	<pre>show mpls lsp <i>lspName</i> p2pmxl_to_100_100_20 ingress</pre>
		Where: <i>lspName</i> = Name of the LSP			
	BX7000 Gateway	Not supported.	<pre><get-mpls-tunnel-information> <name> <i>tunnelName</i></name> </get-mpls-tunnel-information></pre>	Not supported.	<pre>show mpls tunnel <i>tunnelName</i></pre>
		Where: <i>tunnelName</i> = Tunnel name			
Static LSP	ACX Series, M Series, MX Series	Not supported.	<pre><get-mpls-static-lsp-information> <name> <i>lspName</i> </name> <ingress></ingress> </get-mpls-static-lsp-information></pre>	Not supported.	<pre>show mpls static-lsp name <i>lspName</i> ingress</pre>
		Where: <i>lspName</i> = Name of the LSP			
	BX7000 Gateway	Not supported.	<pre><get-mpls-tunnel-information> <name> <i>tunnelName</i> </name></pre>	Not supported.	<pre>show mpls tunnel <i>tunnelName</i></pre>
		Where: <i>tunnelName</i> = Tunnel name			
GRE	ACX Series, M Series, MX Series	Not supported.	<pre><get-interface-information> <interface-name> <i>interfaceValue</i> </interface-name> </get-interface-information></pre>	Not supported.	<pre>show interfaces <i>interfaceValue</i></pre>
	BX7000 Gateway				
		Where: <i>interfaceValue</i> = Name of the interface			

For the data plane, the Junos Space software places a static MAC address in the forwarding table of the remote endpoint, which it uses to verify correct packet transfer.

Troubleshooting the RSVP LSP Static LSP, and GRE

From the **Troubleshooting** tab you can check status of the interfaces, LDP sessions, neighbor links, and endpoints of the RSVP LSP Static LSP, and GRE. To select the status you want to check, click the device from the device list on the left, and select the show command from the **Command** list. This figure shows the routing table for the selected device.

Functional Audit Result

Last Run Time: 02-Sep-2015 06:52:14 Status: DONE [Rerun Functional Audit](#) [Reload Result](#) [Troubleshoot](#)

Service Status

Service Name: p2p_deletepc
Service Type: LSP
Operation State: Down

Device Name	Topology	Operation State	Troubleshoot Status
RouterX1-re	LSP2P	Down	Done

The following table shows the commands for RSVP LSP:

Service Type	Device Family	XML Commands	CLI Commands	Category
RSVP LSP	M Series	<get-mpls-lsp-information> <regex> <i>instanceValue</i> </regex> </get-mpls-lsp-information>	show mpls lsp ingress name <i>instanceValue</i>	MPLS
		<get-mpls-lsp-information> <extensive/><regex> <i>instanceValue</i> </regex> </get-mpls-lsp-information>	show mpls lsp name <i>instanceValue</i> extensive	MPLS
		<get-rsvp-session-information> <session-name> <i>instanceValue</i> </session-name/> </get-rsvp-session-information>	show rsvp session name <i>instanceValue</i>	Route
		<get-rsvp-neighbor-information> </get-rsvp-neighbor-information>	show rsvp neighbor	Route
		<get-rsvp-interface-information> </get-rsvp-interface-information>	show rsvp interface	Route
		<get-ospf-neighbor-information> </get-ospf-neighbor-information>	show ospf neighbor	Route
		<get-ldp-session-information> </get-ldp-session-information>	show ldp session	Route
		<get-bfd-session-information> </get-bfd-session-information>	show bfd session	OAM
Where:				
<i>instanceValue</i> = Name of the service				

The following table shows the commands for Static LSP:

Service Type	Device Family	XML Commands	CLI Commands	Category
Single-hop and Multihop LSP	M Series	<get-mpls-static-lsp-information> <name> <i>instanceValue</i> </name> <i>routerType</i> </get-mpls-static-lsp-information>	show mpls static-lsp name <i>instanceValue</i>	MPLS
		<get-mpls-static-lsp-information> <extensive/> <i>routerType</i> <regex> <i>instanceValue</i> </regex> </get-mpls-static-lsp-information>	show mpls static-lsp name <i>instanceValue</i> extensive	MPLS
		<get-ospf-neighbor-information> </get-ospf-neighbor-information>	show ospf neighbor	Route
		Where: <i>instanceValue</i> = Name of the service <i>routerType</i> = Type of the router		

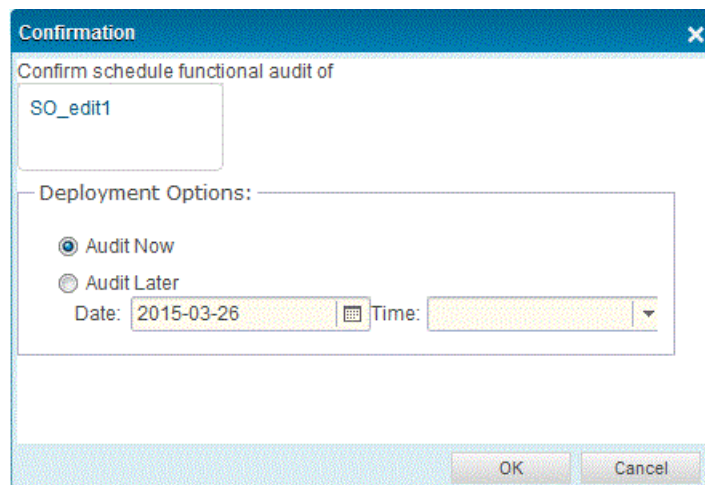
The following table shows the commands for GRE:

Service Type	Device Family	XML Commands	CLI Commands	Category
GRE	ACX Series, M Series, MX Series BX7000 Gateway	<get-interface-information> <terse/> <interface-name> <i>interfaceValue</i> </interface-name> </get-interface-information>	show interface <i>interfaceValue</i> terse	NNI
		<get-ldp-session-information> </get-ldp-session-information>	show ldp session	Route
		<get-ospf-neighbor-information> </get-ospf-neighbor-information>	show ospf neighbor	Route
		Where: <i>interfaceValue</i> = Name of the interface		

Performing the Functional Audit

To perform a functional audit:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. Click the plus sign (+) beside Tunnel to view services based on protocols, and expand the **RSVP LSPs** tree to select an LSP service.
4. In the **Network Services > Tunnel** task pane, select **Audit Results > Functional Audit**. Alternatively, you can select a service order, click the **Audit** button at the top of the table of listed service orders from the Manage Network Services page and select **Run Functional Audit**.



5. In the **Schedule Functional Audit** dialog box, do one of the following:
 - a. Select **Audit Now**, then click **OK**.

The **Job Details** dialog box appears for you to click the Job ID link to see the functional results. The **Job Management** page displays the functional audit details

by job ID, name, percentage complete, state, job type, summary, scheduled start time, user, and recurrence.

ID	Name	Perc...	State	Job Type	Parameters	Summary	Scheduled Start ...	Owner	Recurrence	Refr...
458759	Cloud Infrastructure Event Purge-458759	0.0	Scheduled	Cloud Infrastructure Event Purge			Sep 4, 2015 5:30:00 AM IST		Every 86400000 milliseconds	0
622654	Vpls-Test-scale Deployment	0.0	Cancelled	Deploy Service		Job was cancelled by user super	Sep 3, 2015 9:45:00 PM IST	super		0
622685	Auto Resynchronize devices-622685	0.0	Scheduled	Auto Resynchronize devices	Device(s): junos-ms80-2-space		Sep 3, 2015 3:37:27 PM IST			0
622683	Auto Resynchronize devices-622683	100.0	Failure	Auto Resynchronize devices	Device(s): junos-ms240-space	Number of Reconciled Devices: 1 Number of Reconciled succeeded: 0 Number of Reconciled failed: 1	Sep 3, 2015 3:25:17 PM IST			0
622679	Auto Resynchronize devices-622679	100.0	Failure	Auto Resynchronize devices	Device(s): RouterZ1-re	Number of Reconciled Devices: 1 Number of Reconciled succeeded: 0 Number of Reconciled failed: 1	Sep 3, 2015 3:21:46 PM IST			0
622675	vpls-bgp-res-lst Deployment	100.0	Success	Deploy Service		Deployed On Device [RouterZ1-re] On Device [RouterX1-re] On Device [RouterY1-re] Failed to addNetworkServiceFailure in FM deployment Service monitoring is not working properly	Sep 3, 2015 3:19:08 PM IST	super		0
622674	007_P2P_RESValidate Service Order	100.0	Success	Validate Service		Validated On Device [PE9-re] On Device [480R4_EP_Alok-re] On Device [PE10-re] On Device [480R3_EP_Alok-re]	Sep 3, 2015 3:14:43 PM IST	super		0
622673	006_P2P_RESValidate Service Order	100.0	Success	Validate Service		Validated On Device [PE9-re] On Device [480R4_EP_Alok-re] On Device [480R3_EP_Alok-re] On Device [PE10-re]	Sep 3, 2015 3:11:59 PM IST	super		0
622672	005_P2P_RESValidate Service Order	100.0	Failure	Validate Service		Validating On Device [480R4_EP_Alok-re]Error Downloading Configuration	Sep 3, 2015 3:08:25 PM IST	super		0

- b. Select **Audit Later**, enter a date and time, then click **OK**.

To monitor the progress of an audit after selecting **Audit Later**, after the scheduled time of the audit:

- a. On the Junos Space Network Management Platform user interface, select **Jobs**.
- b. On the **Jobs** statistics page, select the **Functional Audit** segment of the Job Types pie chart.

The **Job Management** page appears filtered by functional audit jobs.

ID	Name	Perc...	State	Job Type	Parameters	Summary	Scheduled Start ...	Owner	Recurrence	Refr...
458759	Cloud Infrastructure Event Purge-458759	0.0	Scheduled	Cloud Infrastructure Event Purge			Sep 4, 2015 5:30:00 AM IST		Every 86400000 milliseconds	0
622654	Vpls-Test-scale Deployment	0.0	Cancelled	Deploy Service		Job was cancelled by user super	Sep 3, 2015 9:45:00 PM IST	super		0
622685	Auto Resynchronize devices-622685	0.0	Scheduled	Auto Resynchronize devices	Device(s): junos-ms80-2-space		Sep 3, 2015 3:37:27 PM IST			0
622683	Auto Resynchronize devices-622683	100.0	Failure	Auto Resynchronize devices	Device(s): junos-ms240-space	Number of Reconciled Devices: 1 Number of Reconciled succeeded: 0 Number of Reconciled failed: 1	Sep 3, 2015 3:25:17 PM IST			0
622679	Auto Resynchronize devices-622679	100.0	Failure	Auto Resynchronize devices	Device(s): RouterZ1-re	Number of Reconciled Devices: 1 Number of Reconciled succeeded: 0 Number of Reconciled failed: 1	Sep 3, 2015 3:21:46 PM IST			0
622675	vpls-bgp-res-lst Deployment	100.0	Success	Deploy Service		Deployed On Device [RouterZ1-re] On Device [RouterX1-re] On Device [RouterY1-re] Failed to addNetworkServiceFailure in FM deployment Service monitoring is not working properly	Sep 3, 2015 3:19:08 PM IST	super		0
622674	007_P2P_RESValidate Service Order	100.0	Success	Validate Service		Validated On Device [PE9-re] On Device [480R4_EP_Alok-re] On Device [PE10-re] On Device [480R3_EP_Alok-re]	Sep 3, 2015 3:14:43 PM IST	super		0
622673	006_P2P_RESValidate Service Order	100.0	Success	Validate Service		Validated On Device [PE9-re] On Device [480R4_EP_Alok-re] On Device [480R3_EP_Alok-re] On Device [PE10-re]	Sep 3, 2015 3:11:59 PM IST	super		0
622672	005_P2P_RESValidate Service Order	100.0	Failure	Validate Service		Validating On Device [480R4_EP_Alok-re]Error Downloading Configuration	Sep 3, 2015 3:08:25 PM IST	super		0

- c. Select the functional audit job that you want.

Summary information about the audit appears in the quick look panel.

- d. In the filter bar, select the table view icon to see additional information about the job. If the service failed the audit, information about the failure appears in the **Summary** field.



NOTE: Functional audit can be run for multiple services from Build mode of Service View of the Connectivity Services Director GUI. From the Manage Network Services page, select the check boxes beside multiple services, and click the Audit/Results button at the top of the table of configured services. When the Audit/Results button is clicked, the Schedule Functional Audit window is displayed, which enables you to perform the audit immediately or schedule it to be run at a later time. You can view detailed, ingrained information about the output of the functional audit that you performed for a service from the Functional Audit Results window. Select the Service-name > Interface-name Device-name > Remote Interface - Remote Device in the left pane of the window. The control plane and data plane statuses are displayed by running service-specific commands in the right pane of the window. Click Rerun Functional Audit at the top-right corner of the window to perform the audit again. If the Status field displays as Completed, an audit can be run again; else, if the Status field displays as Ongoing, it denotes that an audit is currently in progress, you must wait for the running instance to be completed to perform a functional evaluation again.

Click Reload Result at the top-right corner of the window to refresh the results of the audit and display the updated information. You can refresh the results only for completed audit instances. When you select Service-name in the left pane of the window, service status information is displayed in the right pane. The Service Status window displays details such as the operational status of the service, the device name, the topology used in the service are displayed in a tabular format. The number of UNI interfaces and PE devices that are up and down is also shown. When you select Service-name > Interface-name Device-name > Remote Interface - Remote Device in the left pane of the window, endpoint status information is shown in the right pane. The Endpoint Status window displays details of the device name, the topology used in service, remote UNIs status, and device status of the selected service.

The Service Status field corresponding to the service for which polled data is not available is displayed as NA. The Service Status field represents the overall status of a service. To calculate the overall service status, a polling mechanism is used to retrieve data from devices by Connectivity Services Director. Because the overall status of a service involves multiple devices, it is possible to calculate and update service statuses, based on an event from one of the devices because the status of all endpoints of a service needs to be determined to compute the overall service status. It is an expensive

operation to send requests to all endpoints, based on an event from a single device. As a result, a polling method is used to obtain the overall status of the device. Because the polled data represents a snapshot at a point in time, a delay occurs in updating the status of a service. Also, while polling, if service information from one of the devices is not available, the service is marked as down.

6. To view additional details about the functional audit, including results from checking the control plane and the data plane, see *Viewing Functional Audit Results*.

Related Documentation

- [Performing a Configuration Audit on page 1077](#)
- [Troubleshooting N-PE Devices Before Provisioning a Service on page 1080](#)
- [Modifying the Application Settings of Connectivity Services Director on page 1082](#)
- [Troubleshooting the Endpoints of Services on page 1088](#)
- [Viewing Configuration Audit Results on page 1098](#)
- [Viewing Functional Audit Results on page 1102](#)
- [Viewing Functional Audit Results for an Inverse Multiplexing for ATM Service on page 1106](#)

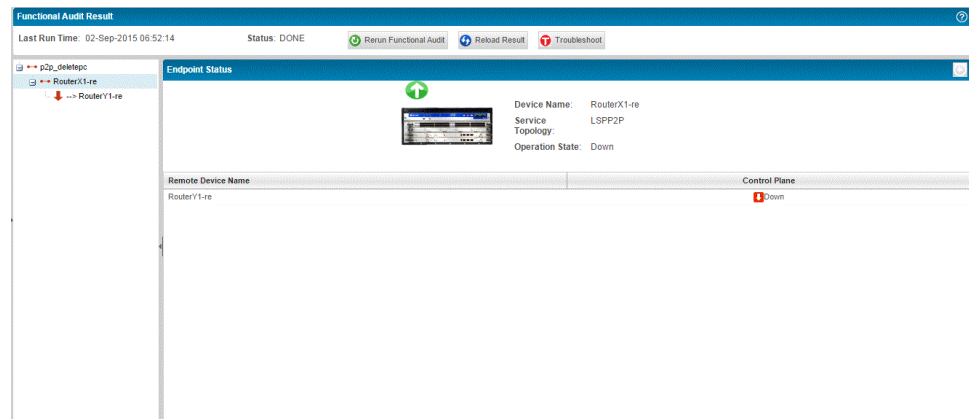
Viewing Functional Audit Results for LSP Services

To view the results of a functional audit of a service, follow this procedure:

After performing a functional audit on a service, look at the functional audit results:

1. From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
2. Click the **Build** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. Click the plus sign (+) beside Tunnel to view services based on protocols, and expand the **RSVP LSPs** tree to select an LSP service.
4. In the **Network Services > Tunnel** task pane, select **Audit Results > Functional Audit**. Alternatively, you can select a service order, click the **Audit** button at the top of the table of listed service orders from the Manage Network Services page.

The **Functional Audit Results** window appears, displaying Service Status in the right panel.



A green up-arrow in the Service Status header bar indicates that the service has passed the functional audit in both the control plane and the data plane. A red down-arrow indicates that the service failed either or both the control plane validation and the data plane validation.

Depending on the type of service, the left panel lists

- The name of the service
- Each endpoint in the service

Icons representing the endpoint indicate its role in the service and its up or down state. [Table 136 on page 1103](#) describes these icons for a service.

Table 252: Service Endpoint Icons



Icon	Meaning
	Hub in a point-to-multipoint service. Endpoint state is up.
	Hub in a point-to-multipoint service. Endpoint state is down.
	Spoke in a point-to-multipoint service. Endpoint state is up.
	Spoke in a point-to-multipoint service. Endpoint state is down.

- Interface name
 - Device name
- To show all endpoints in the service, in the left panel header, select **All**. To display only the endpoints indicating failed validation, select **Failed**. Failed is dimmed if the functional audit returned no validation errors.
 - To view details for an individual interface or endpoint, select it in the left panel. The header bar on the right panel changes to End Point or Interface Status, and details for the selected item are displayed below.

7. Expand each device to show the link from that device to the other N-PE device in the service.

An icon next to each link indicates whether the functional audit commands reported correct functioning of the control plane and data plane. [Table 137 on page 1103](#) describes these icons.

Table 253: Functional Audit Success Status Icons

Icon	Meaning
	Control plane and data plane function correctly.
	Errors were reported in the functioning of either the control plane or the data plane.

8. In the left panel, select a link.

The panel to the right shows the validation results for the control plane validation and data plane validation for the selected link. Icons indicate the success or failure of each set of tests.

The panel to the right shows the validation results for the control plane validation and data plane validation for the selected link. Icons indicate the success or failure of each of these sets of tests. [Table 138 on page 1104](#) describes icons and the textual information provided in the box beside the icon.

Table 254: Control Plane and Data Plane Validation Icons







Icon	Meaning	Explanation
	Control plane up	The text box shows the name of the remote N-PE device and confirms that the data plane is operational.
	Control plane down	The text box shows the name of the configured remote N-PE device and, in the Command status field, explains why the test failed.
	Control plane status unknown	The text box indicates the name of the configured remote N-PE device and, in the Result field, an explanation as to why the functional audit operation was unable to test the control plane—for example, configuration was missing on the device.

Table 254: Control Plane and Data Plane Validation Icons (continued)



Icon	Meaning	Explanation
	Data plane up	The text box indicates the number of packets transmitted and received, and confirms that no data packets were lost during the audit.
	Data plane down	The text box indicates that data packets were lost during the audit.
	Data plane status unknown	The functional audit was unable to complete the data plane test. The Result field in the text box indicates the reason—for example, the platform does not support data plane testing, or the connection to the remote N-PE device is down.

The control plane and data plane validation checks must both show operational status for the link to be considered operational.

- To troubleshoot a service, click the **Troubleshoot** button to open the **Troubleshooting** page. To select the status you want to check, click the device from the device list on the left, and select the show command from the **Command** list.

An icon next to each command indicates whether the command execution is successful or failed. [Table 255 on page 1792](#) describes these icons.

Table 255: Command Status Icons

Icon	Meaning
	Command execution is successful and the command status is up.
	<ul style="list-style-type: none"> Command execution is failed, or, In case of multiple rows, one of the status value is down

**NOTE:**

- Junos OS Release 9.3 and Junos OS Release 9.4 do not support data plane validation. The Functional Audit Results screens do not display data plane validation information if any device in the service is running one of these Junos OS releases.

Examining the LSP Summary Details for Effective Troubleshooting

The LSP Summary page provides a comprehensive and cohesive insight about the configured RSVP LSP service. The status of the LSP and the status of connections between the ingress router and egress routers in an LSP are displayed. The LSP status details are shown for the ingress router. You can also view the ingress, egress, and transit LSP information, such as the primary and secondary states. Ingress information is for the sessions that originate from this router, egress information is for sessions that terminate on this router, and transit information is for sessions that transit through this router. Extensive information about LSPs, including all past state history and the reasons why an LSP might have failed, can also be viewed. This page is beneficial to easily resolve RSVP failures in your network topology by quickly analyzing the LSP status and statistics.

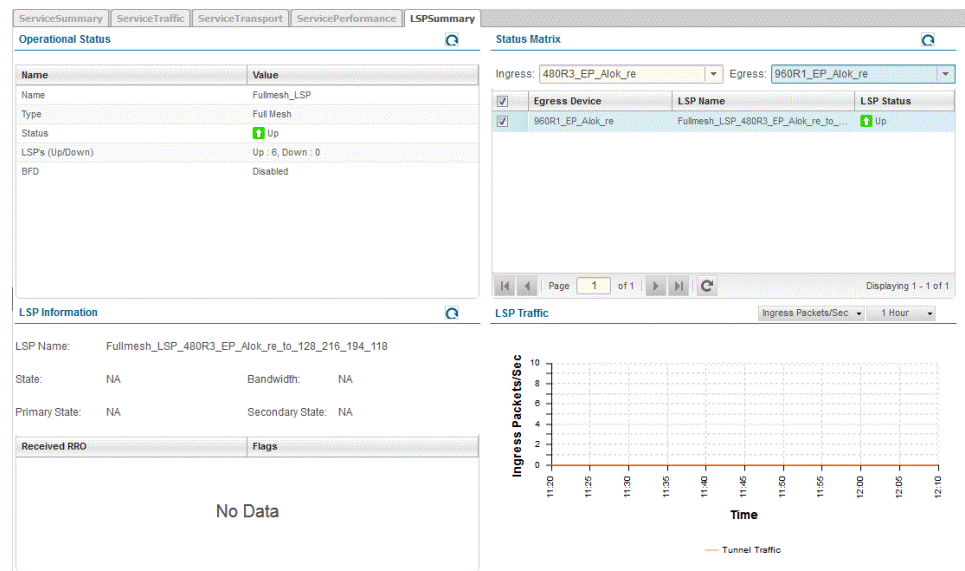


NOTE: The refresh of values and statuses of the parameters displayed in the graphs and tables of different monitors depends on the polling interval configured under the Monitoring tab of the Preferences page (accessible by clicking the down arrow beside the System button in the Connectivity Services Director banner and selecting Preferences).

To view the LSP summary page:

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Monitor** icon in the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside Tunnel to view services based on protocols and expand the **RSVP LSPs** tree to select an LSP service.
5. Click the **LSP Summary** tab. The LSP Summary page is displayed.

Figure 137: LSP Summary Page



This widget provides details on LSP configuration details and statistics of traffic transmitted over the LSP.

- [Operational Status on page 1794](#)
- [Status Matrix on page 1795](#)
- [LSP Information on page 1795](#)
- [LSP Traffic on page 1796](#)

Operational Status

This monitor displays the working status of the LSP service. The following fields are displayed:

- **Name**—Name of the LSP service.
- **Status**—Operational status of the LSP service. A green up arrow indicates the LSP is up, and a red down arrow indicates the LSP is down.
- **Type**—Topology type of the LSP, such as point-to-point, point-to-multipoint, or full-mesh.
- **LSPs Count**—Total number of LSPs configured in the service that are in the up and down states.
- **BFD**—Total number of BFD packets transmitted over the LSP. BFD for RSVP supports unicast IPv4 LSPs. When BFD is configured for an RSVP LSP on the ingress router, it is enabled on the primary path and on all standby secondary paths for that LSP. The source IP address for outgoing BFD packets from the egress side of an MPLS BFD session is based on the outgoing interface IP address.

Status Matrix

This monitor shows the status of connections between the ingress router and egress routers in an LSP. In the tabular view, the egress router, the LSP name, and the LSP status are displayed. From the Ingress list, select the ingress router for the LSP topology. This field is automatically populated for point-to-multipoint LSP topology; you need to select it only for bidirectional P2P LSPs and full-mesh LSPs. From the Egress list, select the output router up to which the LSP runs from an ingress router. This field is applicable for P2P, point-to-multipoint, and full-mesh LSPs.

A green up-arrow in the LSP Status field indicates that the LSP to the destination device is operationally up. A red down-arrow in the LSP Status field indicates that the LSP is down. To filter and sort the display of LSPs, enter the name of the LSP as a match criterion in the Search box and click the Search icon. The page refreshes to display only the LSP names that match with the search term. You can use the paging controls to navigate across multiple pages of LSPs as necessary.

LSP Information

For a destination address that contains LSP names, the corresponding LSP details, such as the name, state, and bandwidth of the LSP, are displayed in this monitor. The following fields are displayed:

- Name— Name of the LSP
- State— State of the LSP handled by this RSVP session: Up, Dn (down), or Restart
- Bandwidth—Specifies the bandwidth in bits per second for the LSP.
- Primary State— State of the LSP that is a primary path: Up, Down, or Restart
- Secondary State— State of the LSP that is a secondary path: Up, Down, or Restart
- Received RRO—(Ingress LSP) Received record route. A series of hops, each with an address followed by a flag. (In most cases, the received record route is the same as the computed explicit route. If Received RRO is different from Computed ERO, there is a topology change in the network, and the route is taking a detour.) The following flags identify the protection capability and status of the downstream node:
 - 0x01—Local protection available. The link downstream from this node is protected by a local repair mechanism. This flag can be set only if the Local protection flag was set in the SESSION_ATTRIBUTE object of the corresponding Path message.
 - 0x02—Local protection in use. A local repair mechanism is in use to maintain this tunnel (usually because of an outage of the link it was routed over previously).
 - 0x03—Combination of 0x01 and 0x02.
 - 0x04—Bandwidth protection. The downstream routing device has a backup path providing the same bandwidth guarantee as the protected LSP for the protected section.
 - 0x08—Node protection. The downstream routing device has a backup path providing protection against link and node failure on the corresponding path section. If the

downstream routing device can set up only a link-protection backup path, the Local protection available bit is set but the Node protection bit is cleared.

- 0x09—Detour is established. Combination of 0x01 and 0x08.
- 0x10—Preemption pending. The preempting node sets this flag if a pending preemption is in progress for the traffic engine LSP. This flag indicates to the ingress legacy edge router (LER) of this LSP that it should be rerouted.
- 0xb—Detour is in use. Combination of 0x01, 0x02, and 0x08.
- Total Packets—Total number of packets and Total number of bytes transmitted over the LSP. This counter is reset to zero whenever the LSP path is optimized (for example, during an automatic bandwidth allocation).
- Total Bytes—Total number of bytes transmitted over the LSP. This counter is reset to zero whenever the LSP path is optimized (for example, during an automatic bandwidth allocation).

LSP Traffic

This monitor displays a line chart with the number of packets or bytes on the y-axis and time on the x-axis to denote the LSP bandwidth utilization. From the Time Interval drop-down box, select 1 Hour, 8 Hours, 1 Day, 1 Week, 1 Month, 3 Months, 6 Months, 1 Year, or Custom to specify the duration for which the data polled from devices needs to be displayed. If you select the Custom option, the Time range popup dialog box is displayed. Specify the date from the calendar, and select the Time From (Start time in the 24-hour time format of collection of data), and Time To (End time in the 24-hour time format of collection of data). Click OK to save the settings. Else, click Cancel to discard the configuration. From the Statistics Type drop-down list, select Packets or Bytes to display metrics corresponding to the selected parameter.

Related Documentation

- [Monitoring the Service Traffic Statistics of P2P Services for Correlating Device Counters on page 1209](#)
- [Monitoring the Service Traffic Statistics of Layer 3 VPN Services for Correlating Device Counters on page 1215](#)
- [Monitoring the Service Transport Details of P2P Services for Easy Analysis on page 1218](#)
- [Monitoring the Service Transport Details of VPLS Services for Easy Analysis on page 1221](#)
- [Monitoring the Service Transport Details of Layer 3 VPN Services for Easy Analysis on page 1225](#)

Troubleshooting the Endpoints of RSVP LSP Services

Junos OS operation (op) scripts automate network and device management and troubleshooting. Op scripts can perform any function available through the remote procedure calls (RPCs) supported by either the Junos XML management protocol or the Junos Extensible Markup Language (XML) API. Op scripts can be executed manually in the CLI or upon user login, or they can be called from another script. They are executed by the Junos OS management (mgd) process.

Op scripts enable you to do the following things:

- Create custom operational mode commands
- Execute a series of operational mode commands
- Customize the output of operational mode commands
- Shorten troubleshooting time by gathering operational information and iteratively narrowing down the cause of a network problem
- Perform controlled configuration changes
- Monitor the overall status of a device by creating a general operation script that periodically checks network warning parameters, such as high CPU usage.

Op scripts are based on the Junos XML management protocol, and the Junos XML API. Op scripts can be written in either the Extensible Stylesheet Language Transformations (XSLT) or Stylesheet Language Alternative Syntax (SLAX) scripting language. Op scripts use XPath to locate the operational objects to be inspected and XSLT constructs to specify the actions to perform on the located operational objects. The actions can change the output or execute additional commands based on the output.

The troubleshooting feature provides an easy and unique way to troubleshoot the services. You do not have to manually login to a device to check the status of services in the Connectivity Services Director application, but you can do the same using the functionality of operational scripts. You do have the flexibility of writing your own scripts to view the results.

Only Juniper Networks devices are supported by this functionality and this is not applicable to the third-party devices.

The operational scripts can either be created or imported to the platform from the local machine before you start troubleshooting the services or you can run the scripts that are of local type directly from the Functional Audit Result window by clicking the **Troubleshoot** button. For op scripts that are not of local type, the op scripts must be imported and staged on to the device using the Junos Space Network Management Platform application before you can run the scripts from within the Connectivity Services Director application for debugging and diagnosing the service endpoints or devices. Currently, you cannot directly add the scripts to the Connectivity Services Director GUI interface. Scripts with execution type as “Local” (@isLocal=true annotation in the SLAX script) are also listed in troubleshooting window. The listing is sorted and filtered based on the context specified for each service.



BEST PRACTICE: We recommend that you configure a script as a local script for effective and optimal debugging and analysis of the configuration settings contained in the script. The main advantage of a local script is that you need not download the script to a device (because a connection is established with the device by the GUI application and the script is run) and you need not remove the script from a device after you decommission a service.

The following table lists the context in which the OP scripts are written for different types of services:

Table 256: OP Scripts Contexts for RSVP LSP Services

Service Type	Context
RSVP LSP LDP	@CONTEXT = "/device/configuration/protocols/mpls/lsp" Example : /device[name="deviceName"]/configuration/protocols/l2circuit/mpls/lsp[name="LSP name"]
Common context for all services	/* @CONTEXT = "/device/configuration/interface/" */ Example: /device[name="device name"]/configuration/ interface[name="interfaceName.unitID"] Example commands:

When you select a single service and from the Network Services > Connectivity task pane, select **Audit Results > Functional Audit** to schedule and perform a functional audit operation, the Functional Audit Results window is displayed after the operation of the selected service is validated. If you have previously run a functional audit already run, the result of the previous audit is displayed. To perform a troubleshooting of the selected service, you must click the **Troubleshoot** button. The troubleshooting task runs as a separate event in Connectivity Services Director, whereas troubleshooting was performed together with functional audit in the Services Activation Director GUI.

- [Troubleshooting Services Using Operational Scripts on page 1798](#)

Troubleshooting Services Using Operational Scripts

The operational scripts or the OP scripts are written to view the statistics of a service in the Connectivity Services Director application. All the commands in the OP scripts are user-defined. To view the contexts for writing OP scripts for different service types, refer [Table 135 on page 1089](#).

To execute the OP scripts and view the status of any service:

1. From the **Network Management Platform** task pane, select **Images and Scripts > Scripts**.
The **Scripts** page that appears displays a list of the existing scripts.
2. From the list of the scripts available in the SLAX format, right-click a script and click **Stage Scripts on Devices** to push the script onto a device.
The **Stage Scripts on Device(s)** page that appears displays a list of the devices associated with the script that you selected.
3. Select the **Select Device Manually** option and select any number of devices to which you want to push the script.

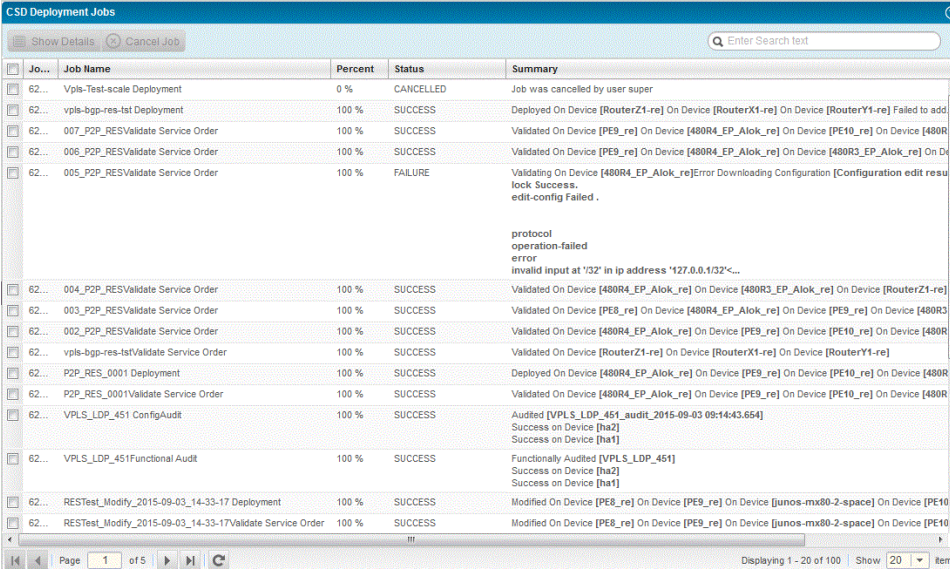


NOTE: The **Enable Scripts on Devices** check box is selected by default.

- Click **Stage** to stage the script on all the devices that you selected.

The **Stage Scripts Information** dialog box confirms the successful staging of scripts onto the selected devices along with the **Job ID**.

- Click **Job ID** to view the status of the job on the **Job Management** page.



Job ID	Job Name	Percent	Status	Summary
62...	Vpls-Test-scale Deployment	0 %	CANCELLED	Job was cancelled by user super
62...	vpls-bgp-res-tst Deployment	100 %	SUCCESS	Deployed On Device [RouterZ1-re] On Device [RouterX1-re] On Device [RouterY1-re] Failed to add...
62...	007_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE9_re] On Device [480R4_EP_Alok_re] On Device [PE10_re] On Device [480R...
62...	006_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE9_re] On Device [480R4_EP_Alok_re] On Device [480R3_EP_Alok_re] On D...
62...	005_P2P_RESValidate Service Order	100 %	FAILURE	Validating On Device [480R4_EP_Alok_re]Error Downloading Configuration [Configuration edit resu lock Success. edit-config Failed . protocol operation-failed error invalid input at '32' in ip address '127.0.0.1/32'<...
62...	004_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [480R3_EP_Alok_re] On Device [RouterZ1-re]
62...	003_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [PE8_re] On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [480R3]
62...	002_P2P_RESValidate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R...
62...	vpls-bgp-res-tstValidate Service Order	100 %	SUCCESS	Validated On Device [RouterZ1-re] On Device [RouterX1-re] On Device [RouterY1-re]
62...	P2P_RES_0001 Deployment	100 %	SUCCESS	Deployed On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R...
62...	P2P_RES_0001Validate Service Order	100 %	SUCCESS	Validated On Device [480R4_EP_Alok_re] On Device [PE9_re] On Device [PE10_re] On Device [480R...
62...	VPLS_LDP_451 ConfigAudit	100 %	SUCCESS	Audited [VPLS_LDP_451_audit_2015-09-03 09:14:43.664] Success on Device [ha2] Success on Device [ha1]
62...	VPLS_LDP_451Functional Audit	100 %	SUCCESS	Functionally Audited [VPLS_LDP_451] Success on Device [ha2] Success on Device [ha1]
62...	RESTest_Modify_2015-09-03_14-33-17 Deployment	100 %	SUCCESS	Modified On Device [PE8_re] On Device [PE9_re] On Device [junos-mx80-2-space] On Device [PE10...
62...	RESTest_Modify_2015-09-03_14-33-17Validate Service Order	100 %	SUCCESS	Modified On Device [PE8_re] On Device [PE9_re] On Device [junos-mx80-2-space] On Device [PE10...

You are redirected to the **Scripts** page.

- From the View selector, select **Service View**. The workspaces that are applicable to routing and tunnel services are displayed.
- Click the **Deploy** icon in the Service View of the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
- Click the plus sign (+) beside Tunnel to view services based on protocols, and expand the **RSVP LSPs** tree to select an LSP service.
- In the **Network Services > Tunnel** task pane, select **Audit Results > Functional Audit**. Alternatively, you can select a service order, click the **Audit** button at the top of the table of listed service orders from the Manage Network Services page.
- In the Schedule Functional Audit dialog box, select **Audit Now**, then click **OK**. After the audit is run, the Functional Audit Results window is displayed.
- From the Functional Audit Results window that displays a list of the devices associated with the service you selected, select the check box next to the device for which you want to diagnose and examine the associated service.
- Click **Troubleshoot** to perform troubleshooting and analysis of the service for which functional audit is performed.
- Select the check box next to a service that you want to analyze and monitor for its working and efficiency. The Execute OP Scripts page is displayed.

14. Select an OP script on the **Execute OP Scripts** page.

Script Name	Description	Version	Type	Created Date	Last Updated Date	
<input checked="" type="checkbox"/>	RSVPLSPPredefinedSc...	RSVP LSP Predefined ...	1	Local	Sep 01, 2015 08:43:08 ...	Sep 01, 2015 08:43:08 ...

Enter Parameters for RSVPLSPPredefinedScript.slax			
Script Name	Name	Description	Value

NOTE: To enter the value for PARAMETERS, click on VALUE column. The value for parameters may be required.

Execute View Last Result Cancel

15. Click the **Value** column to enter any additional parameter for the selected OP script, besides the ones coded in the script.



NOTE: The selection of parameters is entirely dependent on the OP scripts. If the OP scripts support parameters, then all the parameters are listed and you need to enter the values. Parameters can be optional, on the basis of the OP scripts.

16. Click **Execute** to execute the selected OP scripts with the newly added parameters, if any.

A dialog box confirms the execution of the OP scripts along with the **Job ID**.

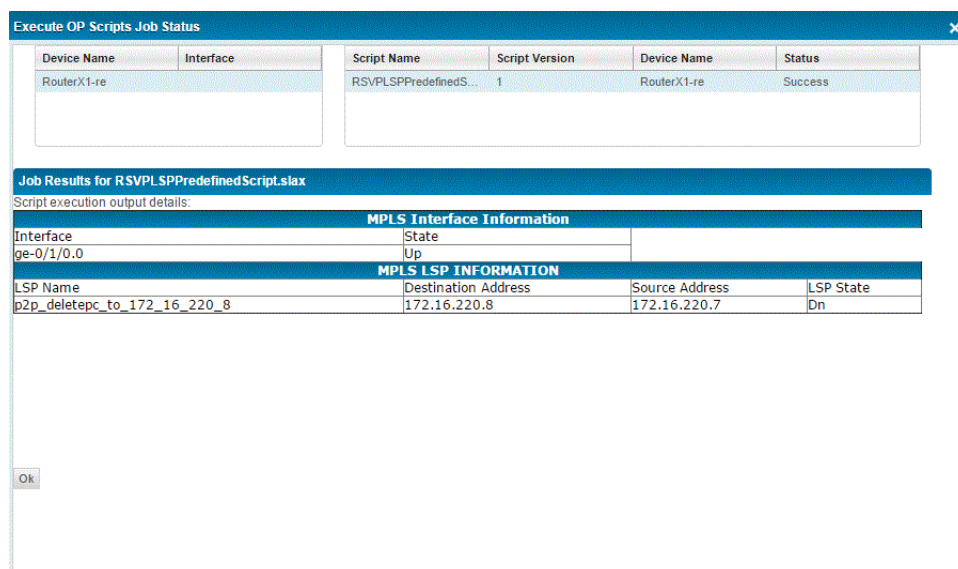
17. Click **OK**.

You are redirected to the **Execute OP Scripts** page.

18. Click **View Last Result** to view the previous OP scripts execution results.



NOTE: This is an optional step.



Related Documentation

- [Performing a Functional Audit on page 1067](#)
- [Performing a Configuration Audit on page 1077](#)
- [Troubleshooting N-PE Devices Before Provisioning a Service on page 1080](#)
- [Modifying the Application Settings of Connectivity Services Director on page 1082](#)
- [Viewing Configuration Audit Results on page 1098](#)
- [Viewing Functional Audit Results on page 1102](#)
- [Viewing Functional Audit Results for an Inverse Multiplexing for ATM Service on page 1106](#)

Clearing LSP Statistics

When you clear LSP statistics on a device using Connectivity Services Director, the operation releases the routes and states associated with MPLS label-switched paths (LSPs), and starts new LSPs. This GUI operation is equivalent to entering the **clear mpls lsp** command on a device using the Junos OS CLI interface. This command disconnects existing Resource Reservation Protocol (RSVP) sessions on the ingress routing device. If there is a time lag between the old path being torn down and the new path being set up, this command might impact traffic traveling along the LSPs.

To clear the label-switched path (LSP) statistical details for an RSVP LSP service:

1. From the View selector, select Service View. The functionalities that you can configure in this view are displayed.
2. Click the Monitor mode icon in the Service View of the Connectivity Services Director banner. The workspaces that are applicable to this mode are displayed.

3. From the Service View pane, click the plus sign (+) beside the **Network Services > Tunnel > RSVP LSPs** tree and select the service for which you want to reset the LSP statistics. The service statistical details are displayed in the middle pane.
4. From the task pane, which is displayed on the rightmost pane, select **Tasks > Clear LSP Statistics**. The Clear LSP Statistics task enables you to delete all the LSP statistics associated with the selected service. A dialog box appears, prompting you to confirm the deletion. The device name and LSPs associated with the device are displayed. In this dialog box, you can also choose to delete the LSP statistics on devices.

Figure 138: Clear LSP Statistics Dialog Box

Confirmation?

Are you sure you want to go ahead and clear all LSP statistics associated with service Fullmesh ?

Service Details	
Device Name	LSP Name
Ingress: 480R3_SV_Alok_re (2 Items)	
480R4_SV_Alok_re	Fullmesh_480R3_SV_Alok_re_to_128_102_162_222
960R1_SV_Alok_re	Fullmesh_480R3_SV_Alok_re_to_128_102_163_58
Ingress: 480R4_SV_Alok_re (2 Items)	
480R3_SV_Alok_re	Fullmesh_480R4_SV_Alok_re_to_128_102_167_35
960R1_SV_Alok_re	Fullmesh_480R4_SV_Alok_re_to_128_102_163_58
Ingress: 960R1_SV_Alok_re (2 Items)	
480R3_SV_Alok_re	Fullmesh_960R1_SV_Alok_re_to_128_102_167_35
480R4_SV_Alok_re	Fullmesh_960R1_SV_Alok_re_to_128_102_162_222

☒ Clear LSP Statistics from Devices

OK Cancel

5. Select the **Clear LSP Statistics from Devices** check box to clear the statistics from devices. This operation is equivalent to the clear mpls lsp command that you can run from the Junos OS CLI interface. If you select the **Clear LSP Statistics from Devices** check box, the statistics are cleared on the device for all the LSPs in the service, in addition to being removed from the Connectivity Services director database. Otherwise, the LSP statistics are only reset in the application database and not on the device.
6. Click OK to confirm; alternatively, click Cancel to discard this operation.

Related Documentation

- [Viewing MAC Table Details on page 1239](#)
- [Viewing Interface Statistics on page 1241](#)
- [Viewing Interface Status Details on page 1243](#)
- [MPLS Connectivity Verification and Troubleshooting Methods on page 1245](#)
- [Using MPLS Ping on page 1247](#)
- [Pinging VPNs, VPLS, and Layer 2 Circuits on page 1249](#)

- [Monitoring Network Reachability by Using the MPLS Ping Capability on page 1250](#)
- [Monitoring Network Reachability by Using the Layer 3 VPN Ping Capability on page 1253](#)
- [Routing Table Overview on page 1256](#)

Monitoring Network Reachability by Using the MPLS Traceroute Capability

You can perform a traceroute operation to examine the network reachability and identify connection failures from a source or ingress host to a remote host for an MPLS LSP signaled by RSVP. It is a debugging tool to locate MPLS label-switched path (LSP) forwarding issues in a network. (Currently supported for IPv4 packets only.)

1. From the View selector, select **Service View**.

The functionalities that you can configure in this view are displayed.

2. Click the **Monitor** mode icon in the Service View of the Connectivity Services Director banner.

The workspaces that are applicable to this mode are displayed.

3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.

4. Click the plus sign (+) beside Tunnels > RSVP LSPs, and select the RSVP service for which you want to run the traceroute utility.

5. From the task pane, select MPLS Traceroute.

The MPLS Traceroute Service Type - Service Name window appears.

Figure 139: MPLS Traceroute Service Type - Service Name Window

MPLS Traceroute-LSP(RSVP)-Fullmesh

Endpoint Device

Ingress Device: 480R4_SV_Alok_re

Egress Device: 960R1_SV_Alok_re

LSP Name: Fullmesh_480R4_SV_Alok_re_to_128_102_163_58

Advance Options

Hop Limit: (1..255)

Probe Retries: (1..9)

Class Of Service: (0..7)

Reply

Format: ASCII

Traceroute

Response Console:

Results for - MPLS Traceroute (RSVP)

Hop Depth	Current Hop	Previous Hop
1	40.2.4.1	(null)
2	40.1.2.1	40.2.4.1

close

6. In the Endpoint Device section, do the following:

- From the Ingress Device list, select the ingress device of the LSP, whose IP address to be used as the packet source address. The local router always is considered to be the ingress router, which is the beginning of the LSP. The software automatically determines the proper outgoing interface and IP address to use to reach the next router in an LSP.
- From the Egress Device list, select the egress device that is connected using the LSP from the ingress LSP, whose IP address is used of the target for the MPLS traceroute packets.

The name of the LSP is displayed in the LSP Name field.

7. On the Advance Options list, do the following:

- a. In the Probe Retries field, specify the number of times to resend probe. The range of values is 1 through 9. The default value is 3.
 - b. In the Hop Limit field, specify the maximum number of routers that an LSP can traverse. The configured hop limit includes the ingress and egress routers. You can specify a hop limit for an LSP and for both primary and secondary paths. By default, each LSP can traverse a maximum of 255 hops, including the ingress and egress routers. The number of hops can be from 2 through 255. (A path with two hops consists of the ingress and egress routers only.)
 - c. In the Class of Service field, specify the class-of-service (CoS) value given to all packets in the LSP. The CoS value might affect the scheduling or queuing algorithm of traffic traveling along an LSP. A higher value typically corresponds to a higher level of service. The range is from 1 through 7. If you do not specify a CoS value, the IP precedence bits from the packet's IP header are used as the packet's CoS value
8. In the Format list, select **XML** to display the result or the response of the MPLS traceroute operation in XML format. Alternatively, select **ASCII** to display the output in the format in which it is displayed on the CLI. The Junos XML API is an XML representation of Junos configuration statements and operational mode commands. Junos XML configuration tag elements are the contents to which the Junos XML protocol operations apply. Junos XML operational tag elements are equivalent in function to operational mode commands in the CLI, which administrators use to retrieve status information for a device.
9. Click **Traceroute** to start the traceroute application and to send the MPLS traceroute requests from the source to the destination device.

The results of the traceroute operation are displayed in the Response Console pane at the bottom of the MPLS Traceroute Service Type - Service Name window.

**Related
Documentation**

- [MPLS Connectivity Verification and Troubleshooting Methods on page 1245](#)
- [Using MPLS Ping on page 1247](#)
- [Pinging VPNs, VPLS, and Layer 2 Circuits on page 1249](#)
- [Monitoring Network Reachability by Using the MPLS Ping Capability on page 1250](#)
- [Monitoring Network Reachability by Using the Layer 3 VPN Ping Capability on page 1253](#)

Monitoring Network Reachability by Using the MPLS Ping Capability for RSVP LSPs

In IP networks, you can use the ping and traceroute commands to verify network connectivity and find broken links or loops. In an MPLS-enabled network, you can use the mpls ping and trace mpls commands to detect plane failures in different types of MPLS applications and network topologies.

1. From the View selector, select **Service View**. The functionalities that you can configure in this view are displayed.
2. Click the **Monitor** mode icon in the Service View of the Connectivity Services Director banner. The workspaces that are applicable to this mode are displayed.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside Tunnels > RSVP LSPs, and select the service for which you want to run the ping application.
5. From the task pane, select MPLS Ping. The MPLS Ping Service Type - Service Name window appears.



NOTE: A warning message is displayed in the window stating that the MPLS echo request to the device might be timed out if the response is delayed from the device.

6. In the Endpoint Device section, do the following:
 - a. From the Ingress Device list, select the source device, whose IP address is to be used as the packet source address.
 - b. From the Egress Device list, select the target endpoint, which IP address of the target for the MPLS ping packets or echo requests. The source device sends an MPLS echo request packet to the specified IP or IPv6 address or, alternatively, sends MPLS echo packets to the egress node in a point-to-multipoint LSP. The MPLS echo request packets and echo reply packets created by this command use the LDP IPv4 LSP sub-TLV described in RFC 4379—Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures (February 2006).
7. On the Advance Options list, do the following:

- a. In the Ping count (packets) field, enter the number of packets to send to the destination address, in the range 0–4294967295. The default value is 5 and 0 (zero) means ping forever.
 - b. In the Ping size (bytes) field, specify the number of bytes comprising the MPLS packet, including the header, in the range 0–64000. The default value is 100 bytes.
 - c. In the Forwarding Class field, specify the value of the forwarding class for the MPLS ping packets.
 - d. In the Sweep field, configure the payload size, which enables you to vary the sizes of the echo packets being sent. This capability is useful for determining the minimum sizes of the MTUs configured on the nodes along the path to the destination address. This reduces packet fragmentation, which contributes to performance problems. The default is not to sweep; all packets are of the same size.
 - e. From the Reply Mode field, select the reply mode for the echo request packet:
 - **IP-UDP**—Specifies that the echo request packet is an IPv4 UDP packet
 - **Application Level Control Channel**—Specifies that the echo request packet is replied using the application-level control channel connection.
8. From the Format list, select **XML** to display the result or the response of the MPLS ping operation in XML format. Alternatively, select **ASCII** to display the output in the format in which it is displayed on the CLI. The Junos XML API is an XML representation of Junos configuration statements and operational mode commands. Junos XML configuration tag elements are the contents to which the Junos XML protocol operations apply. Junos XML operational tag elements are equivalent in function to operational mode commands on the CLI, which administrators use to retrieve status information for a device.
 9. Click **Ping** to start the ping operation and to send the MPLS echo requests from the source to the destination device.

The results of the ping operation are displayed in the Response Console pane at the bottom of the MPLS Ping Service Type - Service Name window.

Related Documentation

- [MPLS Connectivity Verification and Troubleshooting Methods on page 1245](#)
- [Using MPLS Ping on page 1247](#)
- [Pinging VPNs, VPLS, and Layer 2 Circuits on page 1249](#)
- [Monitoring Network Reachability by Using the MPLS Ping Capability on page 1250](#)
- [Monitoring Network Reachability by Using the Layer 3 VPN Ping Capability on page 1253](#)

PART 20

Appendix: Managing Network Activate Features Using the Older Version of Services Activation Director

- [Service Design: Working with Point-to-Point, Layer 3 VPN, and VPLS Service Templates on page 1811](#)
- [Service Provisioning: Working with Threshold Alarm Profiles on page 1841](#)

CHAPTER 60

Service Design: Working with Point-to-Point, Layer 3 VPN, and VPLS Service Templates

- [Service Templates Overview on page 1812](#)
- [Service Templates Workflow on page 1813](#)
- [Applying a Service Template to a Service Definition on page 1814](#)
- [Creating a Service Template on page 1815](#)
- [Deleting a Service Template on page 1819](#)
- [Exporting a Service Template on page 1820](#)
- [Finding Configuration Options on page 1821](#)
- [Importing a Service Template on page 1824](#)
- [Modifying a Service Template on page 1825](#)
- [Specifying Service-Specific Values on page 1826](#)
- [User Privileges in Service Templates on page 1836](#)
- [Provisioning Dynamic Attributes to Specify the Device XPath on page 1837](#)
- [Viewing Service Template Inventory on page 1838](#)

Service Templates Overview

Service Templates provides a powerful mechanism to configure advanced service-related options that are not exposed via the service order creation workflow. Create and attach one or more service templates to a service definition to define any provisioning-related configuration option beyond the current coverage of Network Services. Using a single template, the same parameter values can be pushed to all service instances. Use multiple templates to push different sets of parameters to different endpoints in the same service order.

The service specific values in service templates enable configuration values to be automatically resolved at the time of deployment, without the intervention of the service provisioner. The template designer can also enable the service provisioner to edit parameters in the template.



.....

NOTE: Service templates usually contain “Service Specific Values.” These cannot and should not be edited by service provisioners. The service specific values are resolved by Network Services and the device.

.....

As an extension to Device Templates, Service Templates is designed exclusively for the purpose of service configuration. Configuration of all other options is available through Device Templates. See *Device Templates Overview*. The Service Templates workspace is located under Service Design in Network Services.

Related Documentation

- [Service Templates Workflow on page 1813](#)
- [Applying a Service Template to a Service Definition on page 1814](#)
- [Creating a Service Template on page 1815](#)
- [Deleting a Service Template on page 1819](#)
- [Exporting a Service Template on page 1820](#)
- [Finding Configuration Options on page 1821](#)
- [Importing a Service Template on page 1824](#)
- [Creating a Service Order Based on a Service Definition with a Template on page 990](#)

Service Templates Workflow

A designer, who is typically a network engineer or someone with an equivalent level of knowledge, uses Service Templates to apply service specific values (service variables) by creating service templates. The designer then attaches one or more templates to a service definition.

A service provisioner selects a definition to create a service order. Any templates attached to the definition can be applied and, if required, edited by the provisioner during endpoint configuration.

Deployment automatically resolves service specific values.

The roles of designer and provisioner require the appropriate user privileges (see [“User Privileges in Service Templates” on page 1836](#)).

- [Service Designer Tasks on page 1813](#)
- [Service Provisioner Tasks on page 1813](#)

Service Designer Tasks

The service designer's role in the service template workflow covers the following tasks:

1. [Creating a Service Template on page 1815](#)
2. [Finding Configuration Options on page 1821](#)
3. [Specifying Service-Specific Values on page 1826](#)
4. [Applying a Service Template to a Service Definition on page 1814](#)
5. [Modifying a Service Template on page 1825](#)
6. [Deleting a Service Template on page 1819](#)
7. [Exporting a Service Template on page 1820](#)
8. [Importing a Service Template on page 1824](#)
9. [Viewing Service Template Inventory on page 1838](#)

Service Provisioner Tasks

The service provisioner's tasks in the service template workflow remain creating and deploying service orders. [“Creating a Service Order Based on a Service Definition with a Template” on page 990](#) covers service template handling within a service order.

Related Documentation

- [Service Templates Overview on page 1812](#)
- [Applying a Service Template to a Service Definition on page 1814](#)
- [Creating a Service Template on page 1815](#)
- [Deleting a Service Template on page 1819](#)
- [Exporting a Service Template on page 1820](#)

- [Finding Configuration Options on page 1821](#)
- [Importing a Service Template on page 1824](#)

Applying a Service Template to a Service Definition

To deploy a service template, you must apply it to a service definition. Both templates and definitions are service type specific. If you have a point-to-point service template in the system, you can apply it to a definition of the corresponding service type: point-to-point. You cannot attach it to a multipoint-to-multipoint, or layer 3 VPN service definition. Service variables in a template must be compatible with the definition to which you attach the template. Each service type has its own set of variables, and if the template you want to attach contains any service variables not compatible with the service and definition type, the template will not appear in the definition's list of available templates.

You can apply multiple templates to a single definition.

To apply a service template to a service definition:

1. Create or import a service template. See [“Creating a Service Template” on page 1815](#) or [“Importing a Service Template” on page 1824](#).
2. In the Network Services > Connectivity view pane, select **Service Design > Manage Service Definitions**.
3. Click **Create P2P Service Def...**, or **Create VPLS Service Def...**, or **Create L3 VPN Service Def...**

The **General** window appears.

4. From the Service Template Definition section, click **Add** to select a template. The Choose Templates dialog box appears. Select the desired template(s) and click **OK** to attach the templates to the service definition.

Figure 140: Choose Templates dialog Box

Pool Name	Description	Type	Sub Type	Managed By	Size	Allocated
global-vcid-pool	Global pool of VC-ids	Virtual Circuit	-	-	-	19
IPv4 Resource Pool: 10.0.77.0/24	Pool of IPv4 Addresses: 10.0.77.0/24, (10.0.77.0/24)	IPv4 Address	Global	Global Pool	256	0
IPv4 Resource Pool: 10.0.88.0/24	Pool of IPv4 Addresses: 10.0.88.0/24, (10.0.88.0/24)	IPv4 Address	Global	Global Pool	256	1
IPv4 Resource Pool: 10.0.99.0/24	Pool of IPv4 Addresses: 10.0.99.0/24, (10.0.99.0/24)	IPv4 Address	Global	Global Pool	256	2
AsRTPool36000	RT Pool for AS36000	Route Target	-	-	-	0
AsRDPool36000	RD Pool for AS36000	Route Distinguisher	-	-	-	0
VLAN 917509 ge-0/0/0	VLAN Id Pool For Interface : ge-0/0/0 : ON Device Id : 917509	VLAN	-	Device (917509)	-	0
Unit 917509 ge-0/0/0	Unit Pool For Interface : ge-0/0/0 : ON Device Id : 917509	Unit	-	Device (917509)	-	0
VLAN 917509 ge-0/0/1	VLAN Id Pool For Interface : ge-0/0/1 : ON Device Id : 917509	VLAN	-	Device (917509)	-	0
Unit 917509 ge-0/0/1	Unit Pool For Interface : ge-0/0/1 : ON Device Id : 917509	Unit	-	Device (917509)	-	0
VLAN 917509 ge-0/0/2	VLAN Id Pool For Interface : ge-0/0/2 : ON Device Id : 917509	VLAN	-	Device (917509)	-	0
Unit 917509 ge-0/0/2	Unit Pool For Interface : ge-0/0/2 : ON Device Id : 917509	Unit	-	Device (917509)	-	0
VLAN 917509 ge-0/0/4	VLAN Id Pool For Interface : ge-0/0/4 : ON Device Id : 917509	VLAN	-	Device (917509)	-	0
Unit 917509 ge-0/0/4	Unit Pool For Interface : ge-0/0/4 : ON Device Id : 917509	Unit	-	Device (917509)	-	0
VLAN 917509 ge-0/0/5	VLAN Id Pool For Interface : ge-0/0/5 : ON Device Id : 917509	VLAN	-	Device (917509)	-	0
Unit 917509 ge-0/0/5	Unit Pool For Interface : ge-0/0/5 : ON Device Id : 917509	Unit	-	Device (917509)	-	0
VLAN 917509 ge-0/0/6	VLAN Id Pool For Interface : ge-0/0/6 : ON Device Id : 917509	VLAN	-	Device (917509)	-	0
Unit 917509 ge-0/0/6	Unit Pool For Interface : ge-0/0/6 : ON Device Id : 917509	Unit	-	Device (917509)	-	0
VLAN 917509 ge-0/0/8	VLAN Id Pool For Interface : ge-0/0/8 : ON Device Id : 917509	VLAN	-	Device (917509)	-	0
Unit 917509 ge-0/0/8	Unit Pool For Interface : ge-0/0/8 : ON Device Id : 917509	Unit	-	Device (917509)	-	0
VLAN 917509 ge-0/0/9	VLAN Id Pool For Interface : ge-0/0/9 : ON Device Id : 917509	VLAN	-	Device (917509)	-	0
Unit 917509 ge-0/0/9	Unit Pool For Interface : ge-0/0/9 : ON Device Id : 917509	Unit	-	Device (917509)	-	0

The list of templates available is filtered according to the type of service definition.

- For instructions on filling in the rest of the fields on this page and completing the definition, see [“Creating a Point-to-Point Ethernet Service Definition” on page 625](#), [“Creating a Multipoint-to-Multipoint VPLS Service Definition” on page 653](#), [“Creating a Point-to-Multipoint VPLS Service Definition” on page 678](#), or [“Creating a Full-Mesh Layer 3 VPN Service Definition” on page 709](#).

Related Documentation

- [Service Templates Overview on page 1812](#)
- [Service Templates Workflow on page 1813](#)
- [Creating a Service Template on page 1815](#)
- [Deleting a Service Template on page 1819](#)
- [Exporting a Service Template on page 1820](#)
- [Finding Configuration Options on page 1821](#)
- [Importing a Service Template on page 1824](#)

Creating a Service Template

There are two stages in creating a template. This topic deals with the first stage, while the second stage is covered by [“Specifying Service-Specific Values” on page 1826](#).

Service templates are specific to service definitions. Both are specific to service types, so that if you are dealing with an L3VPN service type, for example, both your service definition and service template must be of that type. A service template's type is determined by the service variables (service specific values) it uses. Some service variables

are specific to one service type only. A table in [“Specifying Service-Specific Values” on page 1826](#) lists the available variables and their types.



NOTE: You can create a service template only using the older version of the Services Activation Director GUI and not using the Connectivity Services Director GUI.

1. [Naming a Template and Selecting Configuration Options on page 1816](#)
2. [Configuration Options, Their Data Types and the Tabs Displayed on page 1818](#)

Naming a Template and Selecting Configuration Options

You create configuration pages as part of the process of selecting configuration options, to organize and group those options.

To name the template :

1. In the Network Activate task pane, select **Service Design > Manage Service Templates > Create Service Template**.

The **Create Service Template** page appears, showing the supported device families above the **Available Configuration** panel and the **Selected Configuration Layout** panel.

2. In the **Name** field, enter a unique name for the template (limit of 63 alphanumeric characters without spaces).
3. (Optional) Enter a description of the template in the **Description** field (limit of 255 characters).

The description is displayed when you double-click the template on the **Service Template** inventory page.

The list in the **Available Configuration** panel displays the Junos OS configuration options available. In the **Selected Configuration Layout** panel, construct logical groupings by putting the options you select into pages.

To select configuration options and create a configuration page:

5. In the **Create Service Template** page, in the **Available Configuration** panel, expand the list of options by opening the list or searching, as described in [“Finding Configuration Options” on page 1821](#).
6. Select an option in the **Available Configurations** panel and move it to a page in the **Selected Configuration Layout** panel.

The first page, “Config Page 1,” is available by default.

There are two ways to move an option from the **Available Configurations** panel to a page in the **Selected Configuration Layout** panel:

- a) Select an option, and drag it and drop it onto the name of the page or any options already on a page.
- b) Select the name of a page by clicking on it, then click the desired option, and finally click the arrow between the panels to transfer the option to the page.

Any sequence is permissible, and there is no limit on the number of options a page can hold.



NOTE: You cannot put children of the same parent into different pages.



NOTE: Options that are either subsidiary or integral to others bring their respective parents and children with them when you move them onto a page. If you drill down and select a parameter deep in the hierarchy, such as L3 interface, dragging that parameter causes all the other parameters that require configuration to come with it. In this example, you get not only L3 interface, but also Name, both of which are under Vlan. This ensures that all the parameters required for a particular configuration option are present in your configuration group.

Conversely, you cannot add an option of the 'choice' data type directly to a page. Instead, add a child of the choice to add the choice itself.

7. Select your configuration grouping by double-clicking the placeholder name, Config page x.
On the right, the **General** tab appears.
8. (Optional) In the **Label** field on the **General** tab, replace the placeholder name (Config Page x) with a more informative name.
9. (Optional) Enter a description of the page in the **Description** field.
10. Save your selections by electing another tab or another configuration option or configuration page.
Clicking **Next** also saves your settings.
To save and finish the template later, click **Finish**. To restart work on the template, you must modify it.

Add or remove pages as desired.

To add a page:

- Click the plus icon [+] at the top left of the **Selected Configuration Layout** panel.
- A new page appears: "Config Page x."

To remove a page or a configuration option from a page:

- Select the page or configuration option and click the X at the top left of the **Selected Configuration Layout** panel.

The page disappears.

Configuration Options, Their Data Types and the Tabs Displayed

Table 257 on page 1818 lists the possible data types of the configuration options, and the tabs associated with each type.

Table 257: Data Types and Tabs

Data Types	Tabs			
	General	Description	Validation	Advanced
Container	*	*		
Table	*	*	*	*
String - Key column in a table	*	*	*	*
String	*	*	*	*
Integer [Number]	*	*	*	*
Boolean	*	*		*
Enumeration	*	*		*
Choice	*	*		*

- All table configuration options have a key column by default.
- You can use any sequence to move options onto your pages.

The subsequent task is "Specifying Service-Specific Values" on page 1826.

- See Also**
- [Service Templates Overview on page 1812](#)
 - [Service Templates Workflow on page 1813](#)
 - [Applying a Service Template to a Service Definition on page 1814](#)
 - [Deleting a Service Template on page 1819](#)

- [Exporting a Service Template on page 1820](#)
- [Finding Configuration Options on page 1821](#)
- [Importing a Service Template on page 1824](#)
- [Creating a Service Order Based on a Service Definition with a Template on page 990](#)

Deleting a Service Template

If a service definition is using a template, you cannot delete that template.

To delete a service template:

1. In the Network Activate task pane, select **Service Design > Manage Service Templates**.
The **Service Template** inventory page appears.

2. Select the template you want to delete.

3. Either right-click the selected template or open the **Actions** menu and select **Delete Service Template**.

The **Delete Template** window appears, displaying the following information about it:

- The name of the template,
- The username of the person who last modified it,
- The date when it was last updated,
- Its state.

4. To delete the template, click **Delete**.

The **Manage Service Templates** page appears, displaying any remaining templates.

5. To abort deletion, click **Cancel**.

The **Manage Service Templates** page appears, displaying all the templates.

Related Documentation

- [Service Templates Overview on page 1812](#)
- [Service Templates Workflow on page 1813](#)
- [Applying a Service Template to a Service Definition on page 1814](#)
- [Creating a Service Template on page 1815](#)
- [Exporting a Service Template on page 1820](#)
- [Finding Configuration Options on page 1821](#)

- [Importing a Service Template on page 1824](#)

Exporting a Service Template

Exporting a template enables you to transfer it to another Junos Space fabric.

Before you begin, you must have a template already created.

To export a template:

1. In the **Network Activate** task pane, select **Service Design > Manage Service Templates**. Select the definition to export.

2. Open the **Actions** menu and select **Export** or right-click the template and select **Export**. The **Export Template** dialog appears.

3. Click **Download file for selected templates (tgz format)**.

The **Opening xxx.tgz** window appears. (XXX is a placeholder for the name of the template.)

4. Select **Save File** and click **OK**.

You may have to toggle between the radio buttons to activate the **OK** button.

The **Enter name of file to save to ...** dialog appears.

5. Rename the file if desired and save it to the appropriate location.

The **Export Template** dialog reappears.

6. Click **Close**.

Although the exported template file is an .xml file, it is saved as a .tgz file, which is the format the system uses to import xml files.

You can now import the template into another Junos Space fabric.

Related Documentation

- [Service Templates Overview on page 1812](#)
- [Service Templates Workflow on page 1813](#)
- [Applying a Service Template to a Service Definition on page 1814](#)
- [Creating a Service Template on page 1815](#)
- [Deleting a Service Template on page 1819](#)
- [Finding Configuration Options on page 1821](#)
- [Importing a Service Template on page 1824](#)

- [Creating a Service Order Based on a Service Definition with a Template on page 990](#)

Finding Configuration Options

There are three ways to locate particular configuration options: you can use the search function, or display the whole list, or use the available service perspectives (P2P, VPLS, L3VPN).

Searching

To search for a specific configuration option:

1. Click the magnifying glass icon.

The search term bar appears.

2. Enter your search term.

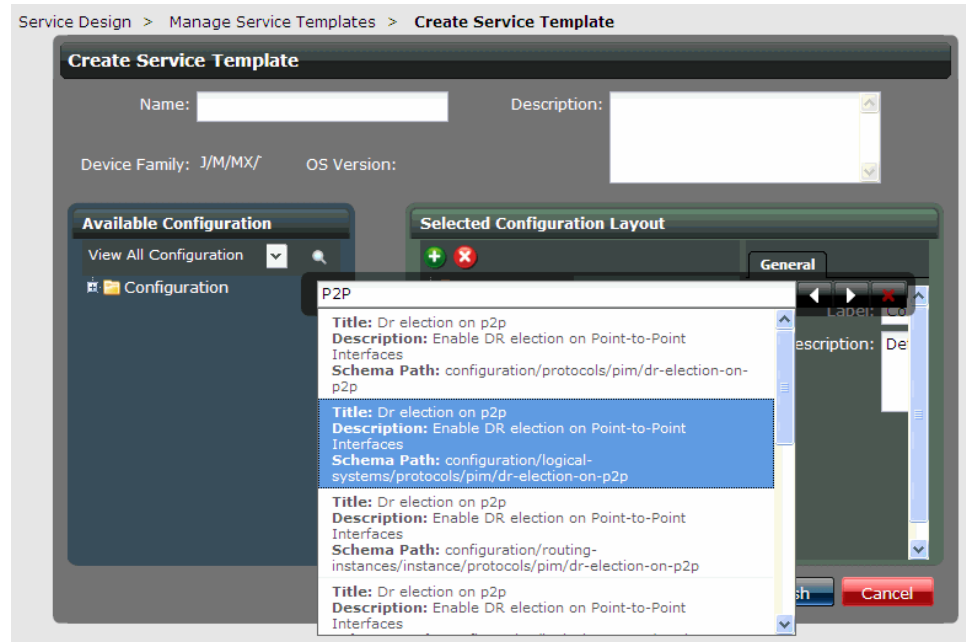
As soon as you enter the first two letters, the bar opens downwards, displaying the search results.

Search displays only the first ten matches for your term .



TIP: Search results appear while you are typing. You can continue typing or even delete text. Note that the cursor might not be visible in the search field if the focus is somewhere within the list of search results.

The order of the search results is not dependent on the order of those items in the **Available Configuration** panel. It is based on the similarity of your search term to indexed fields.



3. While the result list is still visible, select a result by:

- Using the mouse to click on it.
- Pressing the Enter key to select the first result in the list.
- Using the up and down arrow keys on the keyboard to move through the list, pressing the Enter key to select a result.

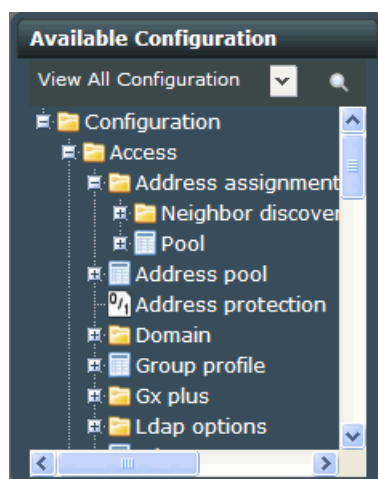
The tree in the **Available Configuration** panel jumps to the location of the match for the result you selected and highlights the option. The list of results disappears.

4. (Optional) To review the results that you did *not* select, either:

- Click the white arrows next to the Search field.
Click the arrow to the left to move to the result listed previous to the selected result.
Click the arrow to the right to move to the result after the selected result.
- Use the left and right arrow keys on the keyboard.
Press the arrow to the left to move to the result listed previous to the selected result.
Press the arrow to the right to move to the result after the selected result.

5. To close the search bar, click the X in the top right corner of the bar.

Displaying all configuration options: To display the top level configuration options, click the plus sign [+] or expansion icon at the top of the tree in the **Available Configuration** panel. Many of the options contain further parameters. To display these, click on the plus sign [+] or expansion icon left of the option.



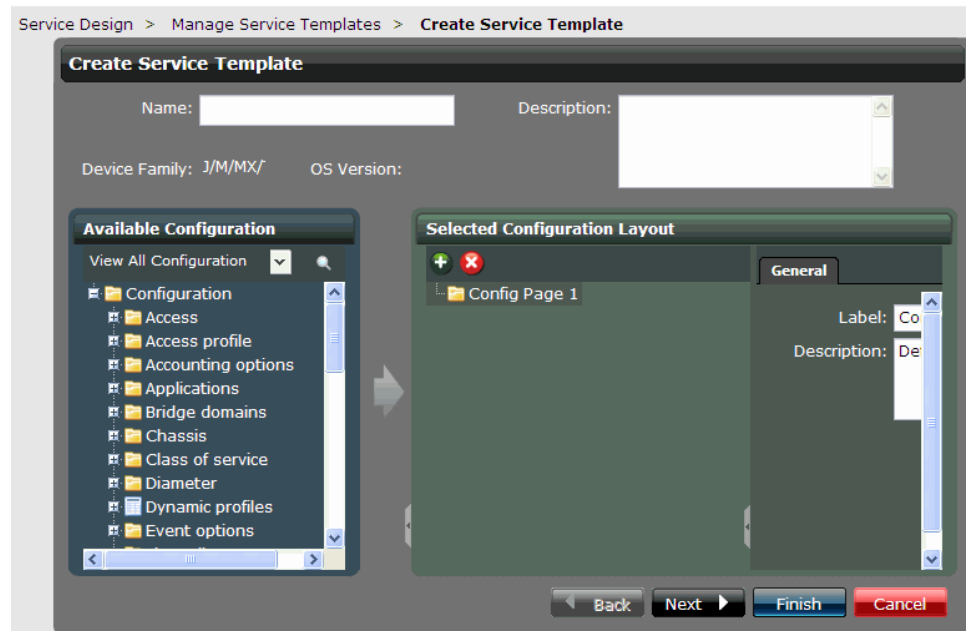
Service Perspective: The configuration parameters are grouped service wise. In the Connectivity Services Director application you can choose either of the following service perspectives:

- P2P
- VPLS
- L3VPN

The **Available Configuration** panel displays the configuration parameters that are specific to the selected service.

For example, if you select L3VPN in the **Available Configuration** the following configuration parameters are displayed:

- Interface
- Policy statement
- Instance



Related Documentation

- [Service Templates Overview on page 1812](#)
- [Service Templates Workflow on page 1813](#)
- [Applying a Service Template to a Service Definition on page 1814](#)
- [Creating a Service Template on page 1815](#)
- [Deleting a Service Template on page 1819](#)
- [Exporting a Service Template on page 1820](#)
- [Importing a Service Template on page 1824](#)

Importing a Service Template

Importing a service template enables you to transfer it from another Junos Space fabric.

Before you begin, make sure you have access to a template file. Although it is an xml file, the system expects to find it packed into a .tgz file, which is the way the system exports .xml files.

To import a template :

1. In the **Network Activate** task pane, select **Service Design > Manage Service Templates > Import Service Template**.

The **Import Service Template** dialog appears.

2. Click **Browse**.

The **File Upload** window opens.

3. Navigate to the appropriate file, select it, and click **Open**.

The **Import Service Template** dialog reappears, displaying the name of the selected file in the **Template File** field.



NOTE: Under some circumstances, when the **Import Definition** dialog reappears, it displays a message beginning **Confirm name mapping of**. This message serves as a warning that the system has changed the name of the definition itself. This happens when you import a template with the same name as an existing template.

4. Click **Import**.

The **Manage Template Definitions** page reappears, displaying the newly imported template definition.

Related Documentation

- [Service Templates Overview on page 1812](#)
- [Service Templates Workflow on page 1813](#)
- [Applying a Service Template to a Service Definition on page 1814](#)
- [Creating a Service Template on page 1815](#)
- [Deleting a Service Template on page 1819](#)
- [Exporting a Service Template on page 1820](#)
- [Finding Configuration Options on page 1821](#)
- [Creating a Service Order Based on a Service Definition with a Template on page 990](#)

Modifying a Service Template

If a service is using a definition, you cannot modify any template associated with that definition. To modify a template attached to a service definition that is not in use:

1. In the **Network Activate** task pane, select **Service Design > Manage Service Templates**.

The **Manage Service Templates** inventory page appears.

2. Select the template you want to modify.

It is not possible to select multiple templates for simultaneous modification.

3. Right-click the selected template or open the **Actions** menu and select **Modify Service Template**.

The **Modify Service Template** page appears. The options selected in the template to be modified are not visible initially.

4. To see the options currently selected in the template, click the plus [+] icon(s) next to the configuration pages in the **Selected Configuration Layout** panel.

When all the plus [+] icon(s) are open, all the currently selected configuration options are visible.

5. Add and/or remove configuration pages and options as required. For instructions on this, see [“Creating a Service Template” on page 1815](#).
6. Specify service-specific data with service variables as required. For instructions on this, see [“Specifying Service-Specific Values” on page 1826](#).
7. To finish modifying the template, click **Finish**.

Related Documentation

- [Creating a Service Template on page 1815](#)
- [Deleting a Service Template on page 1819](#)
- [Exporting a Service Template on page 1820](#)
- [Finding Configuration Options on page 1821](#)
- [Importing a Service Template on page 1824](#)
- [Specifying Service-Specific Values on page 1826](#)
- [Creating a Service Order Based on a Service Definition with a Template on page 990](#)

Specifying Service-Specific Values

Using service-specific variables, you can specify values that Network Services can resolve when the service order is deployed. .

Service definitions filter the service templates available for attachment according to the set of service variables associated with each service definition type. If a template contains any variables that are not in the filter set for that service definition type, the template does not appear in the selection list, so you cannot attach it to the definition.

You can set multiple variables for a single value.

The following table shows the correlation between service definition types and service variables:

Table 258: Service Definition Types and Associated Service Variables

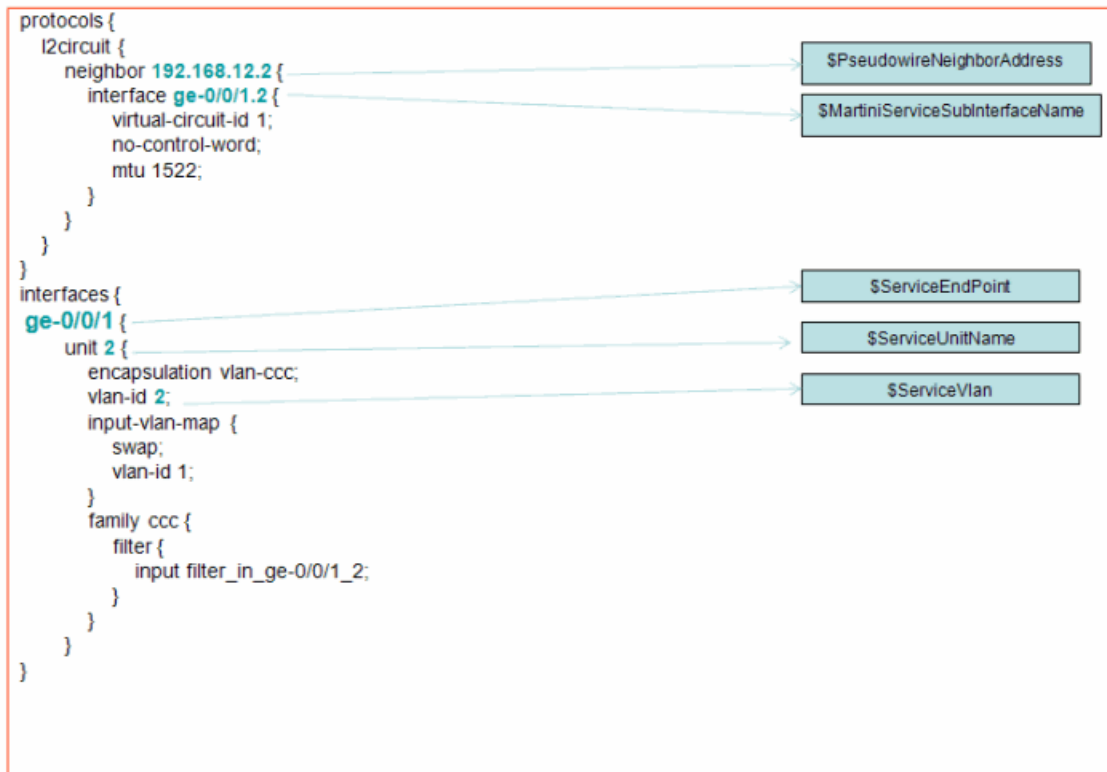
Point-to-Point	VPLS	L3VPN
\$CustomerName	\$CustomerName	\$CustomerName
-	-	\$PEIPAddress

Table 258: Service Definition Types and Associated Service Variables (continued)

Point-to-Point	VPLS	L3VPN
\$PseudowireNeighborAddress	-	-
-	\$RoutingInstanceName	\$RoutingInstanceName
-	-	\$ServiceBGPGroupName
-	-	\$ServiceBGPNeighbor
\$ServiceDefinition	\$ServiceDefinition	\$ServiceDefinition
\$ServiceEndPoint	\$ServiceEndPoint	\$ServiceEndPoint
-	-	\$ServiceOSPFArea
-	-	\$ServiceOSPFIntfName
\$ServiceSubInterfaceName	\$ServiceSubInterfaceName	\$ServiceSubInterfaceName
\$ServiceUnitName	\$ServiceUnitName	\$ServiceUnitName
\$ServiceVlan	\$ServiceVlan	\$ServiceVlan
\$ServiceVlanIdRange	\$ServiceVlanIdRange	-
-	\$SiteName	-
\$KompellaServiceSubInterfaceName	-	-
\$MartiniServiceSubInterfaceName	-	-
-	\$VPLSServiceSubInterfaceName	-
\$MartiniServiceLocalSwitchInterfaceName	-	-
-	-	\$VRFExportPolicy
-	-	\$VRFImportPolicy

The following examples show how the service variables map to the device configuration attributes:

Figure 141: Point-to-Point Example: Device Configuration Deployed Through Network Services



```

protocols {
  l2circuit {
    local-switching {
      interface ge-0/1/0.2 {
        end-interface {
          interface ge-0/2/3.4;
        }
      }
    }
  }
}

```

Variable `$MartiniServiceLocalSwitchInterfaceName` maps to the interface `ge-0/2/3.4`.

Figure 142: VPLS Example: Device Configuration Deployed Through Network Services

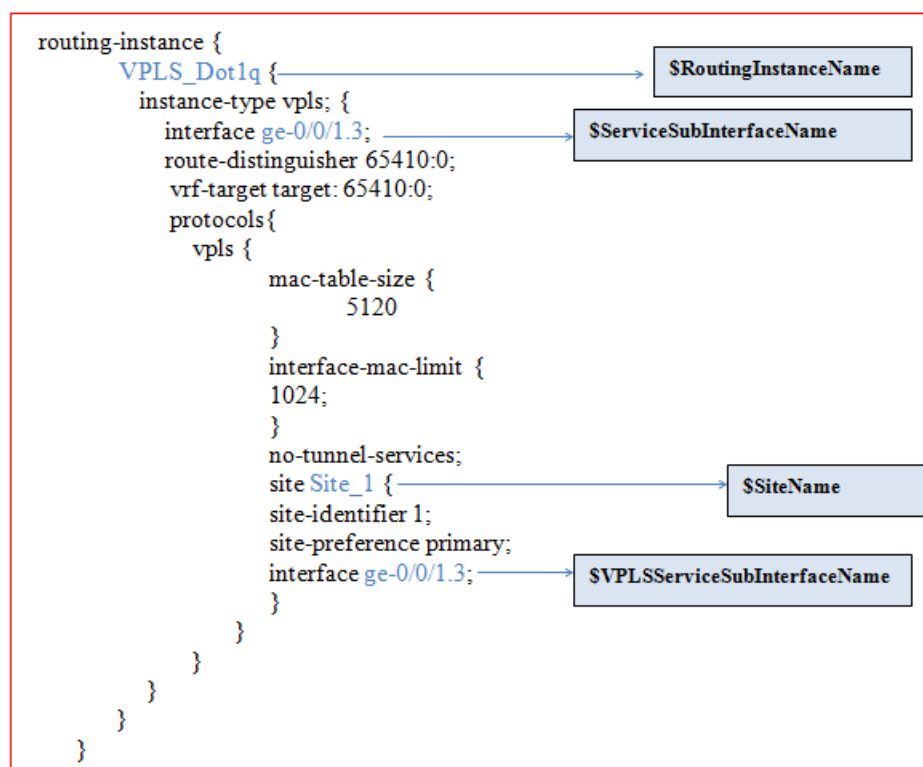


Figure 143: L3VPN Example: When OSPF Is a CE-PE Protocol

```

routing-instances {
  l3vp_ospf {
    instance-type vrf;
    interface ge-0/0/1.3;
    route-distinguisher 65410:3;
    vrf-import l3vp_ospf_fm_import_pol;
    vrf-export l3vp_ospf_fm_export_pol;
    vrf-table-label;
    routing-options {
      auto-export;
    }
    protocols {
      ospf {
        export l3vp_ospf_bgp2ospf_pol;
        area 0.0.0.0 {
          interface ge-0/0/1.3;
        }
      }
    }
  }
}

```

Diagram illustrating the configuration for an L3VPN when OSPF is a CE-PE Protocol. The configuration is shown within the `routing-instances` block, specifically for the `l3vp_ospf` instance. The instance is of type `vrf` and has an interface `ge-0/0/1.3`. The configuration includes a route-distinguisher, VRF import/export policies, a VRF table label, and routing options (auto-export). The OSPF protocol is configured with an export policy and an area `0.0.0.0`, which includes the interface `ge-0/0/1.3`.

Variables mapped to the configuration:

- `$RoutingInstanceName` maps to `l3vp_ospf`.
- `$ServiceSubInterfaceName` maps to `ge-0/0/1.3`.
- `$ServiceOSPFArea` maps to `0.0.0.0`.
- `$ServiceOSPFIntfName` maps to `ge-0/0/1.3`.

```

interfaces {
  ge-0/0/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation flexible-ethernet-services;
    unit 1 {
      vlan-id 1;
      family inet {
        address 1.1.1.1/32;
      }
    }
  }
}

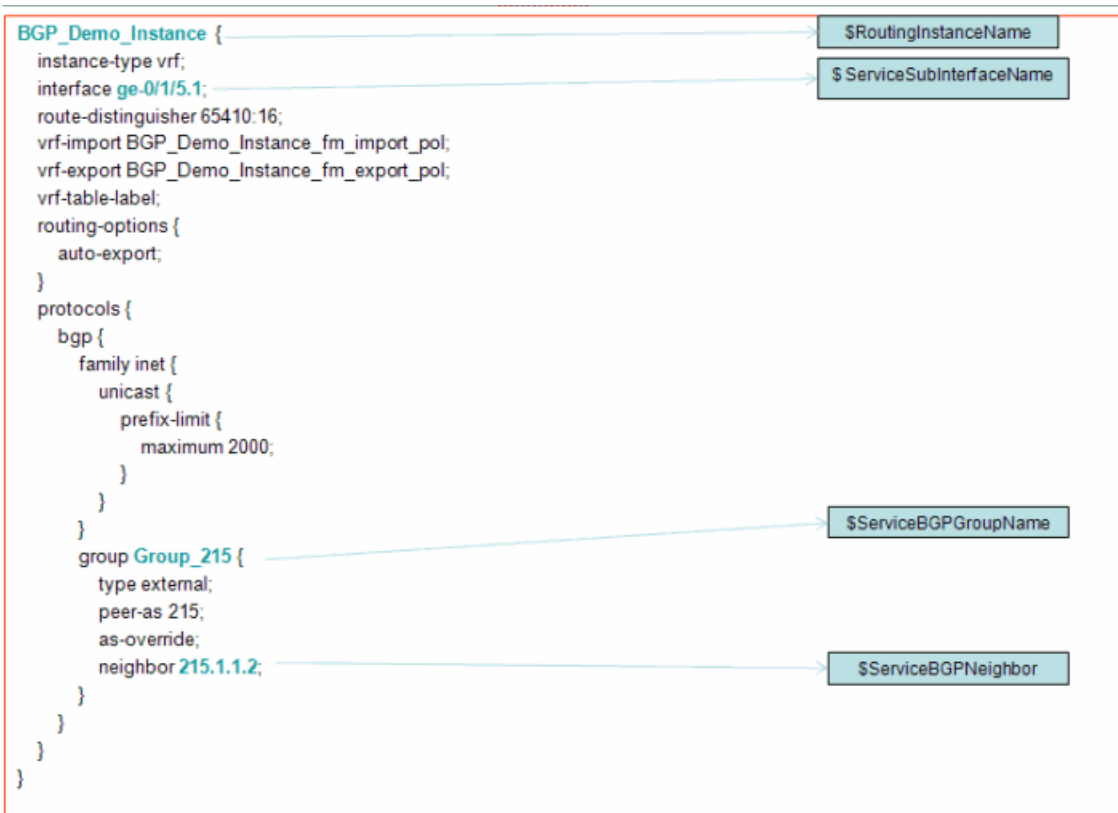
```

Diagram illustrating the configuration for the interface `ge-0/0/1`. The configuration includes flexible-vlan-tagging, mtu 1522, encapsulation flexible-ethernet-services, and a unit `1` with a VLAN ID of `1`. The unit is configured with an IPv4 address `1.1.1.1/32`.

Variables mapped to the configuration:

- `$ServiceEndPoint` maps to `ge-0/0/1`.
- `$ServiceUnitName` maps to `unit 1`.
- `$ServiceVlan` maps to `1`.
- `$PEIPAddress` maps to `1.1.1.1/32`.

Figure 144: L3VPN Example: When BGP Is a CE-PE Protocol



The last two service variables, \$ServiceDefinition and \$CustomerName, appear in the Service Provisioning workspace, in Service Order details.

Service Provisioning > Manage Service Orders > **Manage Service Orders**

Service Order Details

General Information

Name: l3vpn_test-SO_audit_2012-10-	Service definition: l3vpn_test
Customer: Tata	Service type: l3vpn
Order type: ConfigurationAudit	Order state: Completed
Created date: 2012-10-16 20:42:27.0	VRF table label: Enabled
Created by: super	Route target: 69:67174415
Comments: Audit l3vpn_test-SO2012-10-16	Route distinguisher: 69:160563224

Device

UNI Interface

Device: junos-m10-1-space (1 Item)

Device: junos-m10-2-space (1 Item)

junos-m10-1-space	ge-0/0/1
junos-m10-2-space	ge-0/0/3

Device: junos-m10-1-space

Ethernet option: VLAN

UNI interface: ge-0/0/1

Interface IP address: 10.0.77.49

VLAN ID: 200

Routing Protocol Settings

Routing protocol: OSPF

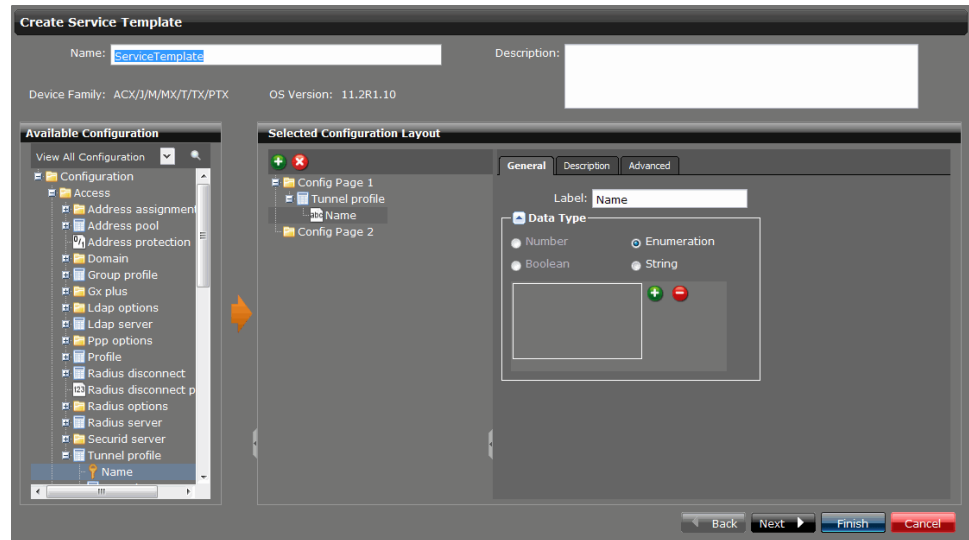
OSPF area ID: 0.0.0.0

OK

To specify service specific values in a template:

1. in the Network Services > Connectivity view pane, select **Network Services > Service Design > Manage Service Templates > Create Service Template**.

The **Create Service Template** window appears.



2. Add the configuration option for which you want to supply a service specific value (for instructions on adding an option, see [“Creating a Service Template” on page 1815](#)).
3. Fill in information in the General tab.

- a. (Optional) To rename the selected option, in the **Label** box, type a name for that configuration option.

When you save by moving on to the next page, Specifying default values for service parameters, the new name appears under Config Page 1 in the **Selected Configuration Layout**.



TIP: The default labels are ambiguous without the context of the tree. For example, there are many options called pool.

The **Data Type** box displays the selected component's data type, which determines not only which tabs are displayed, but also the method of validation. For tables showing the various data types and their tabs, see [“Creating a Service Template” on page 1815](#).

- b. (Optional) If the data type of the selected option is String, you can change it to Enumeration by clicking the String option button while the option is selected.
A box to contain the choices appears, and next to it, plus [+] and minus [-] icons.

- c. To specify the enumeration choices, for each one, click the plus [+] icon and type text in the field that appears (limit 255 alphanumeric characters).



TIP: Keep your choices short, otherwise they are hard to read when you specify the default values. You can create up to 23 choices.

Click OK to save each entry, or to delete it, click Close.

To close the window, click Close or the X.

- d. To save your entries on the General tab, select another tab or another option, or click **Next** or **Finish**.
4. Fill in information in the Description tab.
 - a. In the **Description** field, type [additional] descriptive text for the selected configuration option, or leave the default text, if desired.
 - b. To save your the description, move to another tab or another option, or click **Next**.
 5. Fill in information in the Validation tab.
 - a. Specify the parameters for the option in the appropriate fields.

If the fields already display default values and you change them, ensure that your values do not exceed the default values.
 - b. To save your entries, select another tab or another option, or click **Next** or **Finish**.
 6. Fill in information in the Advanced tab.
 - (Optional) If you intend to use a service variable, select the **Service Specific Value** check box.

Operator visibility changes to hidden. The variable is resolved by Network Services at the time the service is deployed. If the operator does change this variable, deployment fails.
 - If you are not using a service variable for this option, leave the **Service Specific Value** check box unchecked, and make a selection from the Operator Visibility choices.

Select the Editable option button if you want the service provisioner to be able to change the value.
 7. Click **Next**.

The **Specify default values for configuration parameters** page appears.
 8. You must set all the default values on this page; otherwise, service order deployment fails.
 9. Click **Click to configure** as often as necessary to reach the point where you can select a service-specific value, which appears as a drop down list containing system variables.
 10. Click the down arrow at the right of the list to display the available variables.

11. Select the appropriate variable.

If necessary, consult the previous examples to determine which variables to use.



NOTE: If you use the wrong service-specific variable, service deployment fails. The value is not resolved, and service deployment is blocked.

If you select the wrong variable by mistake, delete it by clicking the X to the right of the variable.



NOTE: To create customized service-specific variables:

1. Type the customized name followed by an underscore and dollar symbol.
2. From the list, select the service-specific variable that you want to associate.
3. To save the customized service-specific variable, click the **Save** link.

12. If you move away from the page to set other parameters by clicking the breadcrumbs above the panel, a message prompts you to save your work.

- To save your selection, click **Save**.
- To cancel your selection, click **Undo**.
- To finish the template, click **Finish**.
- To abandon the template, click **Cancel**.

The next task is “[Applying a Service Template to a Service Definition](#)” on page 1814.

Related Documentation

- [Creating a Service Template on page 1815](#)
- [Deleting a Service Template on page 1819](#)
- [Exporting a Service Template on page 1820](#)
- [Finding Configuration Options on page 1821](#)
- [Importing a Service Template on page 1824](#)
- [Modifying a Service Template on page 1825](#)
- [Creating a Service Order Based on a Service Definition with a Template on page 990](#)

User Privileges in Service Templates

In Junos Space Users, the two roles for Service Templates users are predefined: Service Designer for the template designer and Service Manager for the provisioner. For ease of use, in this documentation we refer to the Service Designer as the designer, and to the Service Manager as the provisioner.

You must have Service Designer privileges to create, delete, modify, and manage service templates and service definitions.

You must have Service Manager privileges to create and deploy service orders. However, if you wish to edit service templates or add or delete them, you must have Service Designer privileges.

Related Documentation

- [Creating a Service Template on page 1815](#)
- [Deleting a Service Template on page 1819](#)
- [Exporting a Service Template on page 1820](#)
- [Finding Configuration Options on page 1821](#)
- [Importing a Service Template on page 1824](#)
- [Modifying a Service Template on page 1825](#)
- [Specifying Service-Specific Values on page 1826](#)
- [*Role-Based Access Control Overview*](#)

Provisioning Dynamic Attributes to Specify the Device XPath

You have the flexibility to create and provision a dynamic attribute. You can mark an attribute of a service template as dynamic, and you can obtain the values for these dynamic attributes from a specific device. To create a dynamic attribute, you must first mark an attribute of a service template as dynamic and then specify the device XPath for the dynamic attribute.

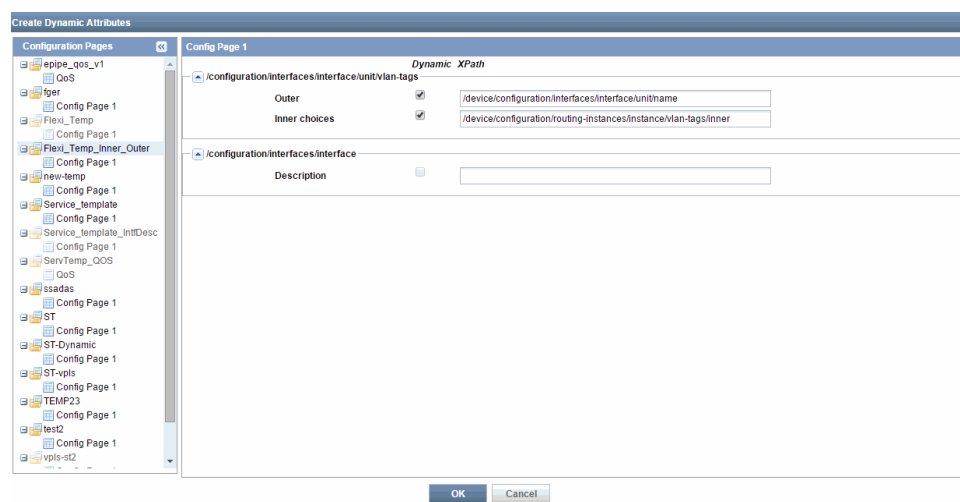
To mark an attribute as dynamic in the service template that you are creating or modifying, set the **Data Type** as *Enumeration*. If a service template attribute is dynamic while you create a service order, all possible values from the device configuration are listed in the Flexible Service Attributes link.

If you set the **Data Type** as *Enumeration*, you need to specify a default value. This default value is listed if the device configuration contain no values.

To specify the device XPath for dynamic attributes:

1. From the Network Activate task pane, select **Service Design > Manage Service Templates > Create Dynamic Attributes**.

The Create Dynamic Attributes window appears.



The Configuration Pages pane lists all the service templates.



NOTE: The service template in the Configuration Pages pane appears dimmed if a service template is attached to a service and you cannot set the dynamic attributes.

2. Select a service template.

The right pane lists all the attributes of the selected service template. If you mouse over an attribute, the XPath of the attribute is displayed.

3. Select the **Dynamic** check box to enable the **XPath** field.



NOTE: You can enable the **Dynamic** check box only for the attribute with **Data Type** as *Enumeration*.

4. Specify the device XPath in the **XPath** field.



NOTE: The device XPath must start with */device*.

From the specified device XPath, all the values from the device configuration are obtained.

5. Click **Ok**.

Related Documentation

- [Creating a Service Template on page 1815](#)
- [Deleting a Service Template on page 1819](#)
- [Exporting a Service Template on page 1820](#)
- [Finding Configuration Options on page 1821](#)
- [Importing a Service Template on page 1824](#)
- [Modifying a Service Template on page 1825](#)
- [Specifying Service-Specific Values on page 1826](#)

Viewing Service Template Inventory

The **Manage Service Templates** inventory page enables you to view and manipulate templates individually or collectively. You can browse, zoom, filter, tag, and sort templates. You can select one, several, or all templates and perform actions on them using the actions in the **Actions** menu or by right-clicking a template.

To view the **Manage Service Templates** page, in the **Network Services > Connectivity** task pane, select **Service Design > Manage Service Templates**. The **Manage Service Templates** inventory page appears.

You can do the following:

- Use the Search function to find a particular template.
- Select all templates on a page, or you can deselect them.

- You can refresh the page by clicking on the Refresh icon in the status bar.
- You can use the **Actions** menu to modify, delete, export, and tag templates.

**Related
Documentation**

- [Service Templates Overview on page 1812](#)
- [Service Templates Workflow on page 1813](#)
- [Applying a Service Template to a Service Definition on page 1814](#)
- [Creating a Service Template on page 1815](#)
- [Deleting a Service Template on page 1819](#)
- [Exporting a Service Template on page 1820](#)

CHAPTER 61

Service Provisioning: Working with Threshold Alarm Profiles

- [Creating a Threshold Alarm Profile on page 1842](#)
- [Viewing Threshold Alarm Profile Performance Parameters on page 1844](#)
- [Attaching a Threshold Alarm Profile to a Service Definition on page 1845](#)
- [Viewing Threshold Alarm Profile Performance Status on page 1846](#)
- [Editing a Threshold Alarm Profile on page 1847](#)

Creating a Threshold Alarm Profile

To create a Threshold Alarm Profile, in the Network Activate task pane, select **Service Design > Manage Threshold Alarm Profile > New**.

The **Create Threshold Alarm Profile** window appears.

Create Threshold Alarm Profile

General Settings

Name:Thresh-test

Service type:VPLS

Comments:

Performance parameters:

Available

Best-One-Way-Delay

Worst-One-Way-Delay

Average-Two-Way-Delay

Best-Two-Way-Delay

Worst-Two-Way-Delay

Average-One-Way-Delay-Variation

Selected

Average-One-Way-Delay

Performance Parameter Details

Performance Parameter	Data Type	Observation Interval (s)	Condition	Threshold	Severity	Message
Performance Parameter:						
Average-One-Way-Delay	Absolute	0	Less than	0	Critical	

CreateCancel

1. Enter information in the relevant fields of the **Create Threshold Alarm Profile** window:

Field	Action
Name	Type a name for the Threshold Alarm Profile.
Service type	Select the service type: <ul style="list-style-type: none">• P2P• VPLS

Field	Action
Performance Parameters	<p>Select the performance parameters that you want to include in the profile.</p> <p>The available parameters depend on the Service type selected.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> • Average one-way delay—Average one-way frame delay for the statistics displayed. • Average one-way delay variation—Average one-way “frame jitter” for the statistics displayed. • Best-case one-way delay—Lowest one-way frame delay for the statistics displayed. • Worst-case one-way delay—Highest one-way frame delay for the statistics displayed. • Average two-way delay—Average two-way frame delay for the statistics displayed. • Average two-way delay variation—Average two-way “frame jitter” for the statistics displayed. • Best-case two-way delay—Lowest two-way frame delay for the statistics displayed. • Worst-case two-way delay—Highest two-way frame delay for the statistics displayed. • Near-end frame loss—Count of frame loss associated with ingress data frames. • Far-end frame loss—Count of frame loss associated with egress data frames. • Near-end loss ratio—Ratio, expressed as a percentage, of the number of service frames not delivered divided by the total number of service frames during time interval T at the ingress interface. • Far-end loss ratio—Ratio, expressed as a percentage, of the number of service frames not delivered divided by the total number of service frames during time interval T at the egress interface. • Average near-end frame loss—Average frame loss measured in this session associated with ingress data frames. • Average near-end loss ratio—Average frame loss ratio measured in this session associated with ingress data frames. • Average far-end frame loss—Average frame loss measured in this session associated with egress data frames. • Average far-end loss ratio—Average frame loss ratio measured in this session associated with egress data frames. • Near-end best case loss—Lowest frame loss measured in this session associated with ingress data frames. • Near-end best case loss ratio—Lowest frame loss ratio measured in this session associated with ingress data frames. • Near-end worst case loss—Highest frame loss measured in this session associated with ingress data frames. • Near-end worst case loss ratio—Highest frame loss ratio measured in this session associated with ingress data frames. • Far-end best case frame loss—Lowest frame loss measured in this session associated with egress data frames. • Far-end best case loss ratio—Lowest frame loss ratio measured in this session associated with egress data frames. • Far-end worst case loss—Highest frame loss measured in this session associated with egress data frames. • Far-end worst case loss ratio—Highest frame loss ratio measured in this session associated with egress data frames. <p>Click Update after you select a parameter from the drop-down list to add the parameter to the threshold alarm profile.</p>
Comments	Type comments to describe the Threshold Alarm Profile.
Perf Parameter Name	This column displays the names of the parameters selected in the Performance Parameters field.

Field	Action
Data Type	<p>This parameter is configured automatically, depending on the performance parameters selected. You cannot edit this field. The possible values are:</p> <ul style="list-style-type: none"> • Absolute • Relative
Observation Interval(s)	Specify the maximum duration during which threshold crossing is allowed.
Threshold	Specify a threshold value. If the performance data exceeds the value specified in the Threshold field, the Junos Space application or OpenNMS software generates a threshold alarm for the selected service.
Condition	Specify the conditional status by which you want the performance data to be evaluated relative to the specified threshold.
Severity	<p>Specify the relative severity of the performance test results, which determines when an alarm is raised:</p> <ul style="list-style-type: none"> • Critical <p>NOTE: Currently, you can specify Critical only.</p>
Message	This column displays a message generated by the application according to the test being performed. This message is updated in the threshold alarm.

2. When you complete entering information in the **Threshold Alarm Profile** window, click **Create**.

Related Documentation

- [Viewing Threshold Alarm Profile Performance Parameters on page 1844](#)
- [Attaching a Threshold Alarm Profile to a Service Definition on page 1845](#)
- [Viewing Threshold Alarm Profile Performance Status on page 1846](#)
- [Editing a Threshold Alarm Profile on page 1847](#)

Viewing Threshold Alarm Profile Performance Parameters

To view a list of existing Threshold Alarm Profiles, in the Network Activate task pane, select **Service Design > Manage Threshold Alarm Profile**. The **Manage Threshold Alarm Profile** window appears. To view the performance parameters that are set for a particular Threshold Alarm Profile:

1. Double-click the selected profile.

The **View Threshold Alarm Profile Details** window displays the profile parameter settings.

View Threshold Alarm Profile Details

General Settings

Name: test-Thresh
Service type: VPLS
Comments:

Performance Parameter Details

Performance Parameter	Data Type	Observation Interval (s)	Condition	Threshold	Severity	Message
Performance Parameter: Average-One-Way-Delay						
Average-One-Way-Delay	Absolute	0	Less than	0	Critical	

Close

- When you finish viewing Threshold Alarm Profile performance parameters, click **Close**.

Related Documentation

- [Creating a Threshold Alarm Profile on page 1842](#)
- [Attaching a Threshold Alarm Profile to a Service Definition on page 1845](#)
- [Viewing Threshold Alarm Profile Performance Status on page 1846](#)
- [Editing a Threshold Alarm Profile on page 1847](#)

Attaching a Threshold Alarm Profile to a Service Definition

To attach a Threshold Alarm Profile to a service definition, in the Network Services > Connectivity view pane, select the path appropriate for the type of service definition that you want to create, as follows:

- **Service Design > Manage Service Definitions > Create P2P Service Definition**
- **Service Design > Manage Service Definitions > Create VPLS Service Definition**

- In the **General** window, as you enter information for the service definition, in the **Threshold Alarm Profile** field, select the Threshold Alarm Profile that you want to attach to this service definition.
- When you complete entering information for the service definition, click **Create**.

Related Documentation

- [Creating a Threshold Alarm Profile on page 1842](#)
- [Viewing Threshold Alarm Profile Performance Parameters on page 1844](#)
- [Viewing Threshold Alarm Profile Performance Status on page 1846](#)
- [Editing a Threshold Alarm Profile on page 1847](#)

Viewing Threshold Alarm Profile Performance Status

When you successfully attach a Threshold Alarm Profile to a service definition and create an associated and functioning service order, you can check the performance status of the service. To run performance management for a service:



NOTE: You can perform this procedure from the Connectivity Services Director GUI.

1. Select **Service View** from the View Selector. The workspaces that are applicable to routing and tunnel services are displayed.
2. From the Junos Space user interface, click the **Deploy** icon on the Connectivity Services Director banner. The functionalities that you can configure in this mode are displayed in the task pane.
3. From the Service View pane, which is the left pane in the window, click the plus sign (+) next to Network Services to expand the tree and display the different service types that you can configure.
4. Click the plus sign (+) beside P2P Services to view the P2P service orders. Select the P2P service order for which you want to monitor performance statistics.

Alternatively, click the plus sign (+) beside VPLS Services to view the VPLS service orders. Select the VPLS service order for which you want to monitor performance statistics.
5. From the Network Services > Connectivity task pane, select **Service Provisioning > Manage Services**.
6. Select the service you want to check and select **Audit > Run Functional Audit** at the top of the table.
7. When the functional audit is running, to run performance management in Monitor mode of Service View, from the tasks pane, select **PM Statistics > Start**. The Monitor Performance Statistics window is displayed.

The system begins to collect performance data pertaining to the parameters you specified in the Threshold Alarm profile: for example, Average-Two-Way-Delay, Best-Two-Way-Delay, or Average-One-Way-Delay.

If data exceeds the threshold value specified in the Threshold Alarm Profile, the system generates a threshold alarm. The value in the **SLA Status** column in the **Manage Services** window changes to **SLA Violated**. If the data does not cross the threshold value specified in the Threshold Alarm Profile, the value in the **SLA Status** column changes to **SLA Violation Cleared**.



NOTE: To view PM statistics, the functional audit status (FA Status) must be Up.

Service Provisioning > Manage Services									
Actions									
Name	Customized	State	FA Status	Fault Status	SLA Status	PM Status	Initiation	Activation Data	
p2p-tdp-two-way-delay-demo	TCA	Deployed	Up	None	Violated	Two Way Delay started	p2p-tdp-two-way-delay-demo	Jun 24, 2013 5:59:18 PM IST	
p2p-tdp	TCA	Deployed	Down	None	None	None	ELine-Dottiq-Singtel-LAN	Jun 24, 2013 5:45:57 PM IST	
p2p-bgp-two-way-delay-variation	TCA	Deployed	Up	None	Cleared	Two Way Delay and Loss started	p2p-bgp-two-way-delay-variation	Jun 24, 2013 5:34:41 PM IST	
p2p-bgp-two-way-Demo_1	TCA	Deployed	Up	None	Violated	Two Way Delay started	p2p-bgp-two-way-Demo	Jun 24, 2013 5:24:03 PM IST	
p2p-bgp	TCA	Deployed	Up	None	None	Two Way Delay started	ELine-BGP-Dottiq-Singtel-LAN	Jun 24, 2013 4:47:52 PM IST	

Related Documentation

- [Creating a Threshold Alarm Profile on page 1842](#)
- [Viewing Threshold Alarm Profile Performance Parameters on page 1844](#)
- [Attaching a Threshold Alarm Profile to a Service Definition on page 1845](#)
- [Editing a Threshold Alarm Profile on page 1847](#)

Editing a Threshold Alarm Profile

To edit an existing Threshold Alarm Profiles, in the Network Activate task pane, select **Service Design > Manage Threshold Alarm Profile**. The **Manage Threshold Alarm Profile** window appears. To edit a particular Threshold Alarm Profile:

1. Right-click the selected profile.
The **Edit Threshold Alarm Profile** window is displayed.
2. Modify the parameters. You will be able to modify the following fields only:
 - **Comments**
 - **Performance parameters**
 - **Performance Parameters Details**

3. When you finish editing Threshold Alarm Profile, click **Update**.

The Threshold Alarm Profile is modified.



NOTE: You cannot modify the threshold alarm profile if it is associated with a service.

**Related
Documentation**

- [Viewing Threshold Alarm Profile Performance Status on page 1846](#)