

Junos[®] Space

Junos Space Cross Provisioning Platform

Published
2022-06-06

Release
19.3

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 Junos Space Cross Provisioning Platform
Release 19.3
Copyright © 2022 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 | xxv

Documentation and Release Notes | xxv

Documentation Conventions | xxv

Documentation Feedback | xxviii

Requesting Technical Support | xxviii

Self-Help Online Tools and Resources | xxix

Creating a Service Request with JTAC | xxix

1

Junos Space Network Topology

Junos Space Network Topology Overview | 31

2

Cross Provisioning Platform

Cross Provisioning Platform Overview | 33

1

Prestaging Devices

Prestaging Devices Overview | 36

Prestaging Devices Overview | 36

Prestaging Devices Process Overview | 37

Prestaging Devices Configuration | 40

Prestaging Rules | 40

Prerequisites for Prestaging Devices in Network Activate | 44

Prestaging ATM and TDM Pseudowire Devices | 46

Prestaging Devices and Device Roles | 51

Adding a UNI | 51

Managing NNI Ports | 52

Assigning Device Roles | 53

Deleting UNIs | 53

Discovering Device Roles | 54

Excluding Interfaces from UNI Role Assignments	56
VLAN Pool Profiles Overview	57
Viewing Pre-Staging Statistics	58
Viewing Available UNIs on N-PE Devices	58
Viewing Services on N-PE Devices	59
Viewing Pre-Staging Rules	60
Viewing Pre-Staging Rules in a Table	60
Migrating Service Interfaces in Cross Provisioning Platform	61
Creating a User-Specific Role to Prevent or Allow Certain Actions on a Service	65
Creating a User-Specific Role	65
Applying the New Role to a User	67
N-PE Devices and Role Assignments 	68
Discovering and Assigning All N-PE Devices	68
Discovering Device Roles	68
Assigning Device Roles	70
Discovering and Assigning N-PE Devices with Exceptions	71
Discovering Device Roles	71
Excluding Devices from N-PE Role Assignment	73
Changing the Loopback Address of an N-PE Device	74
Excluding Interfaces from UNI Role Assignments	74
Committing Your Pre-Staging Choices	75
Changing the Loopback Address of an N-PE Device	77
Excluding Devices from N-PE Role Assignment	78
Unassigning N-PE Devices	78
Viewing N-PE Devices	79
Viewing N-PE Devices in a Table	79
Troubleshooting N-PE Devices Before Provisioning a Service	80
Multihomed Groups 	83
Multihomed Groups Overview	83
Prerequisites to Create Multihomed Groups	84
Required N-PE Device Configuration	85
Administrator Roles Required to Create Multihomed Groups	85

Creating Multihomed Groups Process Overview | 86

Creating a Multihomed Group | 87

Creating a Connectivity File for Multihomed Groups | 87

Uploading a Connectivity File to Create Multihomed Groups | 89

Deleting Multihomed Groups | 90

Viewing Multihomed Groups | 90

Viewing Multihomed Groups | 90

Viewing a Sample Connectivity File for Multihomed Groups | 92

Prestage Services | 94

Service Recovery Overview | 94

Performing a Service Recovery Request | 94

Viewing Service Recovery Report | 100

Managing IP addresses | 106

Creating an IP Address Pool | 106

Managing IPv4 Addresses for Layer 3 VPNs | 108

Specifying IPv4 Addressing Assignment in Layer 3 VPN Service Definitions | 110

Service Templates

Service Templates Overview | 113

Service Templates Workflow | 114

Applying a Service Template to a Service Definition | 115

Creating a Service Template | 116

Naming a Template and Selecting Configuration Options | 116

Configuration Options, Their Data Types and the Tabs Displayed | 119

Deleting a Service Template | 120

Exporting a Service Template | 121

Finding Configuration Options | 122

Importing a Service Template | 125

Modifying a Service Template | 127

Specifying Service-Specific Values | 128

User Privileges in Service Templates | 138

Provisioning Dynamic Attributes to Specify the Device XPath | 139

11

Layer 2 Services

Junos Space Layer 2 Services Overview | 142

Point-to-Point Services | 143

Port-to-Port Service | 143

Single VLAN Service Using 802.1Q Interfaces | 144

All Traffic Service Using Q-in-Q Interface | 145

Range of VLANs Service with Q-in-Q Interfaces | 145

VPLS Services | 147

Service Autodiscovery | 149

VPLS and Normalization | 150

Service Attributes Overview | 152

General Attributes | 152

Service Type | 153

Signaling | 153

Signaling | 153

Signaling | 153

Signaling | 153

Enabling Additional Features | 154

Customer | 154

Enable QoS | 154

UNI Settings | 155

Ethernet Options | 155

Interface | 156

MTU | 156

Customer Traffic Type | 156

Customer VLAN ID | 156

Service VLAN ID and VLAN ID Range | 157

Physical Encapsulation | 157

Logical Encapsulation | 158

Rate Limiting and Bandwidth | 158

UNI Settings for TDM Interfaces | 159

UNI Settings for ATM Interfaces | 159

Connectivity Settings | 160

Virtual Private LAN Service Identifier (VPLS ID) | 160

Auto Discovery | 160

Virtual Circuit Identifier (VCID) (Point-to-Point Services Only) | 160

Route Targets and Route Distinguishers | 160

Normalized VLAN (Multipoint Services Only) | 161

Multihoming | 162

MAC Learning | 162

Advanced Settings | 163

Tunnel Services | 163

Local Switching | 163

Fast Reroute Priority | 163

Label Block Size | 164

Connectivity Type | 164

Redundant Pseudowires for Layer 2 Circuits and VPLS | 165

Types of Redundant Pseudowire Configurations | 165

Pseudowire Failure Detection | 166

VPLS over GRE Overview | 166

Multichassis Link Aggregation Group Overview | 168

Multi-Chassis Automatic Protection Switching Overview | 169

Layer 3 Services

Junos Space Layer 3 Services Overview | 171

Overview | 171

Layer 3 VPN Platform Support | 172

Layer 3 VPN Attributes | 172

Device Configuration for a Layer 3 VPN | 172

Multicast L3VPN Overview | 173

Service Provisioning

Provisioning Process Overview | 176

Network Operator Tasks—Provisioning Prerequisites | 177

Service Designer Tasks | 177

Service Provisioner Tasks | 178

Service Definitions

Layer 2 Ethernet and ATM or TDM Service Definitions | 181

Choosing a Predefined Service Definition or Creating a New Service Definition | 181

Choosing a Predefined Service Definition | 182

Creating an E-Line Service Definition | 188

Specifying General Information | 188

Specifying UNI Settings | 192

Specifying Connectivity Information When Signaling Is LDP | 208

Specifying Connectivity Information When Signaling Is BGP | 211

Creating a Multipoint-to-Multipoint VPLS Service Definition | 214

Specifying General Information for Multipoint-to-Multipoint VPLS Service Definitions | 215

Specifying UNI Settings for Multipoint-to-Multipoint VPLS Service Definitions | 218

UNI Settings for Port-to-Port Interfaces in VPLS Services | 218

UNI Settings for 802.1Q Interfaces in VPLS Services | 221

UNI Settings for Q-in-Q Interfaces in VPLS Services | 225

UNI Settings for Services with Flexible VLAN Tagging (Asymmetric Interface Types) | 229

Specifying Connectivity and MAC Security Information | 232

Specifying Advanced Settings | 235

Creating a Point-to-Multipoint VPLS Service Definition | 237

Specifying General Information for Point-to-Multipoint VPLS Service Definitions | 238

Specifying UNI Settings | 242

Specifying Connectivity and MAC Security Information | 261

Specifying Advanced Settings | 265

Viewing Service Definitions | 267

Tabular View | 267

Searching for Service Definitions | 268

Viewing Service Definition Details | 268

Performing Actions on Service Definitions	269
Creating a Point-to-Point ATM or TDM Pseudowire Service Definition	270
Specifying General Information for the ATM or TDM Service	271
Specifying UNI Settings for ATM and TDM Service Definitions	274
Specifying UNI Settings for ATM Interfaces	274
Specifying UNI Settings for TDM Interfaces	274
Specifying Connectivity Information for an ATM or a TDM Service	276
Creating an E-Line Service Definition	279
Specifying General Information	279
Specifying UNI Settings	283
Specifying UNI Settings for Port-to-Port Services	284
Specifying UNI Settings for Services with 802.1Q Interface Types	287
Specifying UNI Settings for Services with Q-in-Q Interface Types	292
UNI Settings for Services with Flexible VLAN Tagging (Asymmetric Interface Types)	295
Specifying Connectivity Information When Signaling Is LDP	299
Specifying Connectivity Information When Signaling Is BGP	302
Creating a Cross Provisioning Platform Service Definition	305
Publishing a Custom Service Definition	308
Unpublishing a Custom Service Definition	309
Deleting a Customized Service Definition	309
VPLS Service Definitions 	311
Creating a VPLS Service Definition in Cross Provisioning Platform	311
Creating a Multipoint-to-Multipoint VPLS Service Definition	314
Specifying General Information for Multipoint-to-Multipoint VPLS Service Definitions	315
Specifying UNI Settings for Multipoint-to-Multipoint VPLS Service Definitions	319
UNI Settings for Port-to-Port Interfaces in VPLS Services	319
UNI Settings for 802.1Q Interfaces in VPLS Services	322
UNI Settings for Q-in-Q Interfaces in VPLS Services	326
UNI Settings for Services with Flexible VLAN Tagging (Asymmetric Interface Types)	330
Specifying Connectivity and MAC Security Information	333

Specifying Advanced Settings | 336

Creating a Point-to-Multipoint VPLS Service Definition | 338

Specifying General Information for Point-to-Multipoint VPLS Service Definitions | 340

Specifying UNI Settings | 344

Specifying UNI Settings for Port-to-Port Services | 344

Specifying UNI Settings for Services with 802.1Q Interface Types | 348

Specifying UNI Settings for Services with Q-in-Q Interface Types | 353

Specifying UNI Settings for Services with Flexible VLAN Tagging (Asymmetric Interface Types) | 358

Specifying Connectivity and MAC Security Information | 363

Specifying Advanced Settings | 367

Creating a Service Definition for VPLS Access into Layer 3 Networks | 369

Layer 3 VPN Service Definitions | 376

Creating a Full Mesh Layer 3 VPN Service Definition | 376

Specifying General Information | 376

Specifying UNI Settings | 378

Specifying Connectivity Information | 382

Creating a Hub-and-Spoke (One Interface) Layer 3 VPN Service Definition | 386

Specifying General Information | 387

Specifying UNI Settings | 388

Specifying Connectivity Settings | 392

Creating a Service Definition for Point-to-Point Pseudowire Access into a Layer 3 VPN | 395

Creating a Layer 3 VPN Service Definition in Cross Provisioning Platform for Third-Party Devices | 400

Creating a Multicast VPN Service Definition | 404

Predefined Service Definitions | 408

Predefined Service Definitions | 408

Ethernet Point-to-Point Predefined Service Definitions | 408

ELine-Dot1q-SingleVLAN | 411

ELine-Dot1q-SingleVLAN-CCC | 414

ELine-Dot1q-SingleVLAN-Ext-CCC | 417

ELine-PortBased | 420

ELine-QinQ-AllVLAN | 423

ELine-QinQ-AllVLAN-CCC	426
ELine-QinQ-AllVLAN-Ext-CCC	429
ELine-QinQ-VLANRange	432
ELine-QinQ-VLANRange-CCC	435
ELine-QinQ-VLANRange-Ext-CCC	438
Multipoint-to-Multipoint Predefined Service Definitions	440
ELAN-BGP-Dot1q-Normalized-VLAN-None	443
ELAN-BGP-Dot1Q-SingleVLAN	448
ELAN-BGP-PortBased	452
ELAN-BGP-QinQ-AllVLAN	457
ELAN-BGP-QinQ-AllVLAN-Normalized-All	461
ELAN-BGP-QinQ-AllVLAN-Normalized-None	466
ELAN-BGP-QinQ-Range-Normalized-VLAN	470
Point-to-Multipoint Service Definitions	473
ELAN-Hub-Spoke-QinQ-AllVLAN	475
ELAN-Hub-Spoke-QinQ-AllVLAN-No	476
Predefined Point-to-Point Service Definitions	477
ELine-Dot1q-SingleVLAN Service Definition	481
Configuration on Endpoint A	482
Configuration on Endpoint Z	483
ELine-Dot1q-SingleVLAN-CCC Service Definition	484
Configuration on Endpoint A	484
Configuration on Endpoint Z	486
ELine-Dot1q-SingleVLAN-Ext-CCC Service Definition	487
Configuration on Endpoint A	487
Configuration on Endpoint Z	489
ELine-PortBased Service Definition	490
Configuration on Endpoint A	490
Configuration on Endpoint Z	491
ELine-QinQ-AllVLAN Service Definition	493
Configuration on Endpoint A	493
Configuration on Endpoint Z	494

ELine-QinQ-AllVLAN-CCC Service Definition | 496

Configuration on Endpoint A | 496

Configuration on Endpoint Z | 497

ELine-QinQ-AllVLAN-Ext-CCC Service Definition | 499

Configuration on Endpoint A | 499

Configuration on Endpoint Z | 500

ELine-QinQ-VLANRange Service Definition | 502

Configuration on Endpoint A | 502

Configuration on Endpoint Z | 503

ELine-QinQ-VLANRange-CCC Service Definition | 505

Configuration on Endpoint A | 505

Configuration on Endpoint Z | 506

ELine-QinQ-VLANRange-Ext-CCC Service Definition | 508

Configuration on Endpoint A | 508

Configuration on Endpoint Z | 509

ELine-BGP-Port-Based | 511

Configuration on Endpoint A | 511

Configuration on Endpoint Z | 512

Eline-BGP-Dot1q-SingleVLAN | 514

Configuration on Endpoint A | 514

Configuration on Endpoint Z | 516

Eline-BGP-QinQ-AllVLAN | 517

Configuration on Endpoint A | 517

Configuration on Endpoint Z | 519

Predefined Multipoint-to-Multipoint Ethernet Service Definitions | 521**ELAN-BGP-Dot1q-Normalized-VLAN-None Service Definition | 524**

Configuration on Endpoint A | 524

Configuration on Endpoint B | 525

Configuration on Endpoint Z | 527

ELAN-BGP-Dot1Q-SingleVLAN Service Definition | 528

Configuration on Endpoint A | 529

Configuration on Endpoint B | 530

Configuration on Endpoint Z | 531

ELAN-BGP-PortBased Service Definition | 533**Configuration on Endpoint A | 533****Configuration on Endpoint B | 534****Configuration on Endpoint Z | 536****ELAN-BGP-QinQ-AllVLAN Service Definition | 537****Configuration on Endpoint A | 537****Configuration on Endpoint B | 539****Configuration on Endpoint Z | 540****ELAN-BGP-QinQ-AllVLAN-Normalized-All Service Definition | 542****Configuration on Endpoint A | 542****Configuration on Endpoint B | 543****Configuration on Endpoint Z | 545****ELAN-BGP-QinQ-AllVLAN-Normalized-None Service Definition | 546****Configuration on Endpoint A | 547****Configuration on Endpoint B | 548****Configuration on Endpoint Z | 549****ELAN-BGP-QinQ-Range-Normalized-VLAN Service Definition | 551****Configuration on Endpoint A | 551****Configuration on Endpoint Z | 553****Predefined Point-to-Multipoint Ethernet Service Definitions | 554****ELAN-Hub-Spoke-QinQ-AllVLAN-Normalized-All Service Definition | 556****Configuration on Endpoint A | 557****Configuration on Endpoint B | 559****Configuration on Endpoint Z | 561****ELAN-Hub-Spoke-QinQ-AllVLAN Service Definition | 563****Configuration on Endpoint A | 564****Configuration on Endpoint B | 567****Configuration on Endpoint Z | 569****Predefined Full Mesh Layer 3 VPN Service Definitions | 571****Predefined Hub-and Spoke Layer 3 VPN Service Definitions | 572**

Service Orders

Service Order Operations | 575

Service Order States and Service States Overview | 576

- Service Order States | 576

- Service States | 577

Creating a Service Order | 577

Creating a Point-to-Point ATM or TDM Pseudowire Service Order | 578

- Selecting the Service Definition | 578

- Entering General/Connectivity Settings Information | 579

- Specifying Endpoint Information | 582

- Deploying the New Service | 585

Creating a Point-to-Point Service Order | 586

- Selecting the Service Definition | 586

- Entering General Settings Information | 587

- Specifying the Connectivity | 588

- Specifying QoS Settings | 591

- Specifying OAM Settings | 592

- Specifying Endpoint Information | 592

- Specifying Connectivity and Endpoint Information for Managing VLANs | 598

- Deploying and Monitoring the Progress of the New Service | 601

Cloning Deployed Point-to-Point Services | 602

Creating a Bulk-Provisioning Service Order for Pseudowire Services | 606

Inverse Multiplexing for ATM Overview | 612

Creating an Inverse Multiplexing for ATM Service Order | 613

Creating a Cross Provisioning Platform Service Order | 616

Viewing Service Orders | 620

- Viewing Service Orders in a Table | 621

Viewing Cross Provisioning Platform Service Order Details | 622

Service Lock for Cross Provisioning Platform | 625

Modifying a Saved Service Order | 628

Deploying a Service Order | 631

Force-Deploying a Service | 632

Viewing the Configuration of a Pending Service Order | 634

Provisioning a Single-Ended Point-to-Point Service	636
Selecting Specific LSPs for Network Activate Services	638
Associating an LSP with a Point-to-Point Service	639
Viewing LSP Details in a Service Order	640
Viewing LSP Details in a Service	641
Viewing LSP Configuration Details	642
Validating a Service Order	643
Stitching Two Point-to-Point Pseudowires	645
Providing Broadband Network Gateway Service Support with Cross Provisioning Platform	648
Create Workflow for Broadband Network Gateway Services	649
Modify Workflow for Broadband Network Gateway Services	651
Viewing Broadband Network Gateway Services Details	653
Child-Endpoint Support for Broadband Network Gateway Services	654
API for Finding the Service Element ID	654
Deleting a Partial Configuration	654
Deleting a Service Order	655
Re-creating a Cross Provisioning Platform Service Order After a Failed Deployment	656
Re-creating a Cross Provisioning Platform Service Order After a Successful Deployment	657
Viewing the Script Output on the Service Orders Inventory Page	658
Layer 2 VPLS Service Orders 	660
Creating a Multipoint-to-Multipoint VPLS Service Order	660
Selecting the Service Definition	660
Entering General Settings Information	661
Specifying QoS Settings	662
Specifying OAM Settings	663
Configuring Connectivity Settings	663
Setting Attributes for All Endpoints	665
Setting Attributes for Endpoints on a Service	666
Setting Attributes for Endpoints on a Service with Flexible VLAN Tagging	669
Selecting N-PE Devices and Multihomed Groups	671
Modifying Endpoint Settings	672

Deploying the New Service | 677

Creating a Point-to-Multipoint VPLS Service Order | 678

Selecting the Service Definition | 679

Entering General Settings Information | 679

Configuring Connectivity Settings | 681

Specifying QoS Settings | 683

Specifying OAM Settings | 683

Setting Attributes for All Endpoints | 684

Setting Attributes for Endpoints on a Service | 684

Setting Attributes for Endpoints on a Service with Flexible VLAN Tagging | 687

Selecting N-PE Devices and Multihomed Groups | 690

Selecting Hubs and Modifying Endpoint Settings | 690

Deploying the New Service | 696

Creating a Service Order for VPLS Access into Layer 3 Networks | 698

Creating a VPLS Service Order in Cross Provisioning Platform | 705

Seamless MPLS Support in Junos Space Overview | 708

Understanding VLAN Manipulation (Normalization and VLAN Mapping) on Ethernet Services | 710

VLAN Translation (Normalization) for VPLS Services | 711

VLAN Mapping for VPLS Services | 711

Sample VLAN Configuration on MX Series and M Series PE Routers | 713

Layer 3 VPN Service Orders | 715

Stitching a Pseudowire to an L3VPN Service | 715

Creating a Full Mesh Layer 3 VPN Ethernet Service Order | 718

Selecting the Service Definition | 719

Configuring Order Information | 719

Specifying General Settings | 719

Specifying QoS Settings | 720

Specifying VPN Settings and PE-CE Settings Information | 721

Selecting N-PE Devices | 725

Setting Attributes for UNI Endpoints | 726

Adding, Deleting, and Modifying Endpoints | 731

Deploying the New Service	732
Creating a Hub-and-Spoke Layer 3 VPN Service Order	733
Selecting the Service Definition	734
Entering Order Information	734
Entering General Settings Information	734
Specifying QoS Settings	735
Entering VPN Settings and PE-CE Settings Information	736
Selecting Endpoint PE Devices	740
Configuring Endpoint Settings	740
Setting Attributes for UNI Endpoints	741
Adding, Deleting and Modifying Endpoints	746
Deploying the New Service	746
Creating a Multicast VPN Service Order	748
Selecting a Published L3VPN Service Definition for a Service Order	753
Entering Layer 3 VPN Order Information	753
Setting General Settings	753
Entering VPN Settings Information	754
Entering PE-CE Settings	755
Selecting Endpoint PE Devices	755
Creating a Service Order Based on a Service Definition with a Template	756
Deploying a Layer 3 VPN Service Order	759
Creating a Cross Provisioning Platform Layer 3 VPN Service Order	760
Creating a Layer 3 VPN Service Order in Cross Provisioning Platform for Third-Party Devices	765

Service Types

Managing Service Types in Cross Provisioning Platform	771
Creating Service Types in Cross Provisioning Platform	771
Modifying a Service Type in Cross Provisioning Platform	772
Deleting a Service Type in Cross Provisioning Platform	773

22

Scripts

Adding Scripts Created for Cross Provisioning Platform | 775

Exporting Scripts Created for Cross Provisioning Platform | 776

Importing Scripts Created for Cross Provisioning Platform | 778

Modifying Scripts Created for Cross Provisioning Platform | 779

Viewing Scripts Created for Cross Provisioning Platform | 781

Predefined Scripts for Cross Provisioning Platform | 784

Predefined Service Scripts | 785

Predefined Feature Scripts | 786

Predefined Troubleshooting Scripts | 787

Viewing Script Version Support for Cross Provisioning Platform | 787

Debugging a Cross Provisioning Platform Script | 789

Modifying a Cross Provisioning Platform Script | 790

Previewing a Cross Provisioning Platform Script | 790

Verifying a Cross Provisioning Platform Script | 791

23

Device Configlet Services

Creating and Deploying a Device Configlet Order for Cross Provisioning Platform | 793

Administering a Device Configlet Service Order for Cross Provisioning Platform | 795

Administering a Device Configlet Service for Cross Provisioning Platform | 797

Decommissioning Bulk Device Configlet Services in Cross Provisioning Platform | 799

Modifying a Device Configlet Service in Cross Provisioning Platform | 801

Deleting Bulk Device Configlet Orders in Cross Provisioning Platform | 802

24

Third-Party Devices

Adding a Third-Party Device to the Cross Provisioning Platform System | 806

Viewing Third-Party Device Details for Cross Provisioning Platform | 807

Synchronizing Third-Party Devices with the OSS for Cross Provisioning Platform | 808

Confirming Communication with the Third-Party OSS Server for Cross Provisioning Platform | 810

Preconfiguring the Third-Party OSS Device for Cross Provisioning Platform | 811

25

Bulk Services and Devices

Modifying Bulk Services and Devices in Cross Provisioning Platform | 816

Modifying Bulk Services in Cross Provisioning Platform | 816

Modifying Bulk Devices in Cross Provisioning Platform | 819

Administering Bulk Service Operations in Cross Provisioning Platform | 822

Decommissioning Bulk Services in Cross Provisioning Platform | 826

Deleting Bulk Service Orders in Cross Provisioning Platform | 828

26

Deployed Services

Viewing Services | 832

Viewing Services in a Table | 832

Editing a Service Name | 834

Decommissioning a Service | 834

Modifying a Full Mesh Layer 3 VPN Ethernet Service | 837

Adding an Endpoint | 837

Adding a UNI Interface | 841

Deleting a UNI Interface and Deleting an Endpoint | 843

Modifying a Multipoint-to-Multipoint Ethernet Service | 844

Adding an Endpoint | 845

Adding a UNI Interface | 847

Deleting a UNI Interface and Deleting an Endpoint | 849

Changing the Endpoint Bandwidth | 850

Changing the Primary Device in a Multihomed Group | 851

Changing Advanced Settings for an Endpoint | 853

Modifying a Point-to-Multipoint Ethernet Service | 855

Adding a Spoke | 856

Adding a Hub | 858

- Changing a Spoke to a Hub | 860
- Changing a Hub to a Spoke | 861
- Adding a UNI Interface | 862
- Deleting a UNI Interface or Deleting an Endpoint | 864
- Changing the Endpoint Bandwidth | 866
- Changing the Primary Device in a Multihomed Group | 867
- Changing Advanced Settings for an Endpoint | 868

Modifying a Point-to-Point Ethernet Service | 871

Modifying a Service in Cross Provisioning Platform | 873

Understanding Service Validation | 875

Service Troubleshooting Overview | 875

Troubleshooting Services in Cross Provisioning Platform | 876

- Troubleshooting Cross Provisioning Platform Services Using Operational Scripts | 878
- Troubleshooting Cross Provisioning Platform Services Using CLI Configlet Scripts | 880

NEC iPASOLINK Management

Cross Provisioning Platform for iPASOLINK Devices Overview | 883

Worldwide Junos OS Adapter Overview | 884

Installing the Worldwide Junos OS Adapter | 885

Device Discovery Profiles Overview | 887

- Connections Initiated by Junos Space or the Device | 888
- Device Information Fetched During Device Discovery | 889

Creating a Device Discovery Profile | 889

- Specifying Device Targets | 890
- Specifying Probes | 893
- Selecting the Authentication Method and Specifying Credentials | 896
- (Optional) Specifying SSH Fingerprints | 897

Scheduling Device Discovery | 898

Running Device Discovery Profiles | 900

Modifying a Device Discovery Profile | 901

Discovering and Assigning Roles in Cross Provisioning Platform for iPASOLINK Devices | 902

Discovering Device Roles | 903

Assigning Device Roles | 903

Predefined Scripts for Provisioning iPASOLINK Devices | 904

Creating a Cross Provisioning Platform Service Definition for iPASOLINK Devices | 905

Creating a Cross Provisioning Platform Service Order for iPASOLINK Devices | 909

Configuring QoS Settings for iPASOLINK Devices | 913

Canoga Perkins Network Interface Device Management

Cross Provisioning Platform for Canoga Perkins NIDs Overview | 916

Configuring OSS Parameters for Canoga Perkins NIDs | 918

Confirming Communication with Canoga Perkins OSS Server | 920

Adding a Canoga Perkins NID to Cross Provisioning Platform | 921

Synchronizing Canoga Perkins NIDs with OSS | 922

Synchronize All Canoga Perkins NIDs with OSS | 922

Synchronize Selected Canoga Perkins NIDs with OSS | 923

Resynchronize Failed Canoga Perkins NIDs based on the Port Number | 924

Schedule OSS Synchronization for Canoga Perkins NIDs | 924

Cancel OSS Synchronization for Canoga Perkins NIDs | 924

Adding Canoga Perkins Scripts | 925

Creating a Service Definition for Canoga Perkins NIDs | 926

Creating a Cross Provisioning Platform Service Order for Canoga Perkins NIDs | 929

Performing Service Activation Test | 931

29

Service-Level Alarms

Viewing Service-Level Alarms in Network Activate | 934

30

Flexible Services

Configuring Flexible Service Attributes to Modify Service Template Attributes | 938

Recovering Flex Services with Cross Provisioning Platform | 940

Before You Recover Flex Services | 941

High-Level Workflow for Recovering a Flex Service | 941

Workflow for Recovering a Complete Flex Service | 942

List of REST APIs for Recovering a Flex Service | 943

Mandatory Tags in the Payload for Recovering a Flex Service | 944

31

Device Configuration and Prestaging Examples

Example: Base Configuration for N-PE Device in a Multipoint Service | 947

Example: Base Configuration for N-PE Device in a Point-to-Point Ethernet (LDP) Service | 949

Example: Base Configuration for a P Router | 950

Example: Base Configuration for BX7000 Multi-Access Gateway Supporting ATM and TDM Pseudowires | 953

32

End-to-End Configuration Examples

Example: Configuring and Deploying a Point-to-Point Ethernet Service | 960

Preparing Devices for Discovery | 961

Discovering Devices | 961

Preparing Devices for Prestaging | 963

Discovering and Assigning N-PE Roles | 965

Choosing or Creating a Service Definition | 965

Creating a Customer | 968

Creating and Deploying a Point-to-Point Service Order | 969

Performing a Functional Audit and a Configuration Audit | 970

Example: Configuring and Deploying a Multipoint-to-Multipoint VPLS Service | 972

Preparing Devices for Discovery | 973

Discovering Devices | 974

- Preparing Devices for Prestaging | 975
- Discovering and Assigning N-PE Roles | 978
- Choosing or Creating a Service Definition | 979
- Creating a Customer | 982
- Creating and Deploying a Multipoint-to-Multipoint Service Order | 983
- Performing a Functional Audit and a Configuration Audit | 984

Example: Configuring and Deploying a Layer 3 VPN Full-Mesh Service | 986

- Preparing Devices for Discovery | 987
- Discovering Devices | 988
- Preparing Devices for Prestaging | 989
- Discovering and Assigning N-PE Roles | 990
- Choosing or Creating a Service Definition | 991
- Creating a Customer | 993
- Creating and Deploying a Layer 3 VPN Service Order | 993
- Performing a Functional Audit and a Configuration Audit | 995

Example: Creating Cross Provisioning Platform Services | 996

33

Statistics and Reports

Viewing Service Design Statistics | 1045

- Viewing Services Created from a Service Definition | 1045
- Viewing How Many Service Definitions Are in Each Service Definition State | 1046

Viewing Service Template Inventory | 1047

Search Techniques on the Cross Provisioning Platform Inventory Page | 1048

Managing Reports for Broadband Network Gateway Services in Cross Provisioning Platform | 1050

Viewing Service Provisioning Statistics | 1051

- Viewing Service Orders by Customer | 1052
- Viewing the Percentage of Service Orders in Each Service Order State | 1053

34

Customer Operations

Adding a New Customer | 1056

Deleting Customers | 1057

Editing an Existing Customer | 1058

Viewing Customers | 1059

Viewing Customers as Graphics | 1059

Viewing Customers in a Table | 1059

35

Auditing

Performing a Configuration Audit | 1062

Performing a Functional Audit | 1064

Viewing Configuration Audit Results | 1078

Viewing Functional Audit Results | 1081

Viewing Functional Audit Results for an Inverse Multiplexing for ATM Service | 1086

36

Performance Management and Statistics

Performance Management Overview | 1089

Monitoring Performance Statistics | 1089

On-Demand Mode | 1089

Proactive Mode | 1090

Performance Management of Test Traffic | 1090

Monitoring Performance Management Statistics | 1091

Monitoring Statistics for Point-to-Point Service | 1091

Monitoring Statistics for VPLS Service | 1093

Viewing Performance Management Statistics | 1094

Viewing Statistics for Point-to-Point Service | 1095

Viewing Statistics for VPLS Service | 1097

Monitoring Performance Statistics Derived from MIB Objects | 1100

Viewing Performance Statistics Collected According to SLAX Scripts | 1103

37

Collection of Log Files

Downloading the Collection of Cross Provisioning Platform Log Files | 1110

38

Application Settings

Modifying Application Settings | 1113

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | xxv
- Documentation Conventions | xxv
- Documentation Feedback | xxviii
- Requesting Technical Support | xxviii

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 xxvi 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 xxvi 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>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<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>
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.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

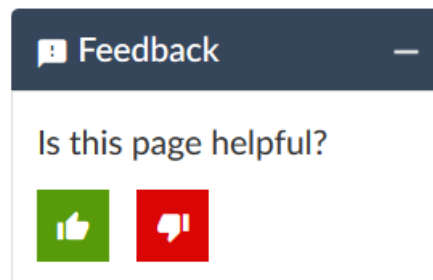
Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
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/>.

1

CHAPTER

Junos Space Network Topology

[Junos Space Network Topology Overview](#) | **31**

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 **Application Network 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 Point-to-Point ATM or TDM Pseudowire Service Order | 578](#)

[Creating a Point-to-Point Service Order | 586](#)

[Creating a Multipoint-to-Multipoint VPLS Service Order | 660](#)

[Creating a Point-to-Multipoint VPLS Service Order | 678](#)

[Creating a Full Mesh Layer 3 VPN Ethernet Service Order | 718](#)

[Creating a Hub-and-Spoke Layer 3 VPN Service Order | 733](#)

2

CHAPTER

Cross Provisioning Platform

[Cross Provisioning Platform Overview](#) | 33

Cross Provisioning Platform Overview

The Cross Provisioning Platform (CPP) software provides a real-time, operations support system (OSS) for creating and deploying multi-vendor LAN/WAN services.

Creating services for Cross Provisioning Platform deployment requires the coordination of tasks performed in several areas of expertise including script design, system administration, and service provisioning.

Junos Space Release 13.1P1 includes software modules that manage the essential interaction between the Juniper Networks devices and the devices of other vendors for which the Cross Provisioning Platform service will be deployed.

The CPP software manages a module called the Service Aware Manager (SAM). Scripts imported into the system that pertain to the outside vendor device are managed by the SAM. Another type of script renders the graphical user interface (GUI) window that enables a service provisioner to configure the devices for the service.

Before you use Junos Space to provision a service definition upon which to base the service order, you must import several required scripts to the system.

An important aspect of creating a Cross Provisioning Platform service definition is using Cross Provisioning Platform to attach the required scripts to the definition. When you create the Cross Provisioning Platform service definition, you attach scripts designed for the service of SAM. The CPP software in Junos Space manages the information that defines the service for the outside vendor device and the information that defines the service for the Juniper Networks device.

Juniper Networks script designers create the scripts that provide required information for the Juniper Networks devices. Script designers for the outside vendor must create scripts that provide required information for their devices. The scripts for Juniper Networks devices and third-party devices are all managed by the script manager in the CPP software.

To enable Cross Provisioning Platform, script designers create the following three types of scripts and upload them to the local file system.

- Junos XSLT—Provides the code that enables provisioning a particular Juniper Networks device.
- SAM XSLT—Provides the code that enables provisioning the device of another vendor.
- GUI JavaScript—Provides the code that renders the Cross Provisioning Platform GUI window through which a service provisioner enters data to configure a Juniper device.

A system administrator adds the scripts into the local file system using the Junos Space Cross Provisioning Platform application. Thereafter, the service provisioner uses Cross Provisioning Platform to attach the scripts to the service definition and service order.

The GUI scripts generate high level service data with service topology embedded. The transformation code in the CPP software compiles high-level service data into low-level configuration data, which is pushed to the network devices.

RELATED DOCUMENTATION

Adding Scripts Created for Cross Provisioning Platform 775
Importing Scripts Created for Cross Provisioning Platform 778
Modifying Scripts Created for Cross Provisioning Platform 779
<i>Deleting Scripts</i>
Viewing Scripts Created for Cross Provisioning Platform 781
Creating a Cross Provisioning Platform Service Definition 305
Creating a Cross Provisioning Platform Service Order 616

1

PART

Prestaging Devices

Prestaging Devices Overview | **36**

Prestaging Devices Configuration | **40**

Prestaging Devices and Device Roles | **51**

N-PE Devices and Role Assignments | **68**

Multihomed Groups | **83**

Prestage Services | **94**

Managing IP addresses | **106**

Prestaging Devices Overview

IN THIS CHAPTER

- [Prestaging Devices Overview | 36](#)
- [Prestaging Devices Process Overview | 37](#)

Prestaging Devices Overview

In the Junos Space product, pre-staging takes the devices already under Junos Space management and prepares them for service activation. The pre-staging 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 Network Activate application does not support provisioning for J Series devices.

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

Pre-staging uses the Network Activate software 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 Network Activate software 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.

To pre-stage devices while accepting all recommendations made by the Network Activate software, see [“Discovering and Assigning All N-PE Devices” on page 68](#). To make exceptions to the Network Activate recommendations, see [“Discovering and Assigning N-PE Devices with Exceptions” on page 71](#).

RELATED DOCUMENTATION

Discovering and Assigning All N-PE Devices	68
Discovering and Assigning N-PE Devices with Exceptions	71
Prerequisites for Prestaging Devices in Network Activate	44
Prestaging Devices Process Overview	37
Prestaging Rules	40
Viewing Pre-Staging Rules	60
VLAN Pool Profiles Overview	57

Prestaging Devices Process Overview

After Junos Space has discovered the devices, you must perform a two- or three-stage process to pre-stage devices:

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 you confirm device assignments, 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, you need to run the role discovery operation 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 Assign Roles screen shows a device inventory of N-PE routers that Network Activate has discovered in its database that have not yet been assigned. You can perform the following operations from the Assign Roles 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 68](#) 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 loopback address or the UNI assignments on that device. For step-by-step instructions on selecting a different loopback address, see [“Changing the Loopback Address of an N-PE Device” on page 74](#).

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 71](#) for step-by-step instructions.
- The Manage Device UNIs screen is an inventory of UNI-qualified interfaces for a specific discovered device. You can view a separate Manage Device UNIs 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 56](#).

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. Select **Network Activate > Prestage Devices > Manage Device Roles**.
2. Select **Discover Roles** to view the relevant window.
3. Click **Continue** to view the **Role Discovery Status** window.

The **Role Discovery Status** window displays a graph which shows the number of unassigned devices that could be assigned the role of **N-PE** or **PE**.

To re-sync the role of the network elements configured:

1. Select **Network Activate > Prestage Devices > Manage Device Roles**.
2. To re-sync the role capability of a network element, right-click the network element's name.

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.

RELATED DOCUMENTATION

[Viewing N-PE Devices | 79](#)

[Discovering and Assigning All N-PE Devices | 68](#)

[Discovering and Assigning N-PE Devices with Exceptions | 71](#)

Prestaging Devices Configuration

IN THIS CHAPTER

- [Prestaging Rules | 40](#)
- [Prerequisites for Prestaging Devices in Network Activate | 44](#)
- [Prestaging ATM and TDM Pseudowire Devices | 46](#)

Prestaging Rules

Pre-staging 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.

AS Number Check

The Junos Space software checks for the Autonomous System (AS) number of a device. If the AS number is not configured for a device, the **Service Capability** is assigned as *Layer 2*.

RELATED DOCUMENTATION

| [Viewing Pre-Staging Rules](#) | 60

Prerequisites for Prestaging Devices in Network Activate

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 Network Activate prestaging workspace works on devices that have already been discovered and imported into the Junos Space database, but have not yet been pre-staged.

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. Select **Network Activate > Prestage Devices > Manage Device Roles**.
2. Select **Discover Roles** to view the relevant window.
3. Click **Continue** to view the **Role Discovery Status** window.

The **Role Discovery Status** window displays a graph which shows the number of unassigned devices that could be assigned the role of **N-PE** or **PE**.

To re-sync the role of the network elements configured:

1. Select **Network Activate > Prestage Devices > Manage Device Roles**.

2. To re-sync the role capability of a network element, right-click the network element's name.
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.

For details about bringing devices under Junos Space management, see *Discovering Devices* in the *Junos Space Network Application Platform User Guide*.

RELATED DOCUMENTATION

| [Discovering Devices in the Junos Space Network Application Platform User Guide](#)

Prestaging ATM and TDM Pseudowire Devices

Junos Space supports ATM and TDM pseudowires in IP/MPLS networks on BX7000 Multi-Access Gateways and 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 *Layer 2 VPN Configuration Example* and *Configuring Layer 2 Circuit and Layer 2 VPN Pseudowires* [Junos OS VPNs Configuration Guide](#).

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 *Discovering Devices* 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-hcl-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-...	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 Network Activate Prestaging feature to bring the PE and CSR devices into Network Activate together with their UNI interfaces. In the **Network Activate** task pane, select **Prestage Devices > Manage Device Roles**.

Prestage Devices > Manage Device Roles

0 Items Selected Actions

Name	Management Address	Loopback Address
<input type="checkbox"/> vjx-junos-mx80-2-space	10.213.52.119	40.1.255.9
<input type="checkbox"/> vjx-junos-mx80-1-space	10.213.53.57	40.1.255.1
<input type="checkbox"/> vjx-junos-mx480-space	10.213.50.234	40.1.255.3
<input type="checkbox"/> vjx-junos-mx240-space	10.213.51.206	40.1.255.8
<input type="checkbox"/> vjx-junos-m10-2-space	10.213.51.130	40.1.255.4
<input type="checkbox"/> vjx-junos-m10-1-space	10.213.53.151	40.1.255.10
<input type="checkbox"/> vjx-embassy-mx80-space	10.213.51.177	40.1.255.7
<input type="checkbox"/> vjx-acx4-space	10.213.52.148	40.1.255.2
<input type="checkbox"/> vjx-acx3-space	10.213.53.203	40.1.255.11
<input type="checkbox"/> vjx-acx2-space	10.213.53.68	40.1.255.6
<input type="checkbox"/> vjx-acx1-space	10.213.50.227	40.1.255.5
<input type="checkbox"/> junos-space5	10.216.114.123	30.1.2.11
<input type="checkbox"/> junos-space3	10.216.114.121	30.1.2.9
<input type="checkbox"/> junos-space2	10.216.114.120	30.1.2.8
<input type="checkbox"/> junos-space1	10.216.114.119	30.1.2.7
<input type="checkbox"/> junos-mx80-2-space	10.216.114.105	30.1.2.3
<input type="checkbox"/> junos-mx80-1-space	10.216.114.104	30.1.2.5
<input type="checkbox"/> junos-mx480-space	10.216.114.100	30.1.2.6
<input type="checkbox"/> 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.

NPE



Name: junos-space5

MPLS role: N_PE

Serial number: yyyyyyyyyyyy

OS version: 12.2R1.8

Platform: ACX2000

Loopback address: 30.1.2.11

Connection status: up

Service capability: L2, L3

Additional device CSR
role:

UNI Interfaces


Name	VLAN Profile
em0	default [1-4094]
ge-0/1/3	default [1-4094]
ge-0/1/4	default [1-4094]
ge-0/1/6	default [1-4094]
ge-0/1/7	default [1-4094]
t1-0/0/3	N/A
xe-0/3/0	default [1-4094]
xe-0/3/1	default [1-4094]

Page 1 of 1 | Displaying 1 - 8 of 8

OK

Double-click another listed device. In this example, the details window shows the channelized ATM and T1 interfaces.

NPE



Name: junos-space2

MPLS role: N_PE

Serial number: yyyyyyyyyyyy

OS version: 12.2R1.3

Platform: ACX2000

Loopback address: 30.1.2.8

Connection status: up

Service capability: L2, L3

Additional device CSR role:

UNI Interfaces

Name	VLAN Profile
at-0/0/0	N/A
ge-0/1/1	default [1-4094]
ge-0/1/3	default [1-4094]
ge-0/1/4	default [1-4094]
ge-0/1/5	default [1-4094]
ge-0/1/7	default [1-4094]
t1-0/0/1	N/A
t1-0/0/2	N/A
xe-0/3/0	default [1-4094]
xe-0/3/1	default [1-4094]

Page 1 of 2 | Displaying 1 - 10 of 11

OK

RELATED DOCUMENTATION

Creating an RSVP LSP Order	
Creating an RSVP LSP Definition	
Creating a Single-Hop Static LSP Order	
Creating a Single-Hop Static LSP Definition	
Discovering and Assigning All N-PE Devices	68
Discovering Device Roles	54
Creating a Point-to-Point ATM or TDM Pseudowire Service Definition	270
Creating a Point-to-Point ATM or TDM Pseudowire Service Order	578

Prestaging Devices and Device Roles

IN THIS CHAPTER

- Adding a UNI | 51
- Managing NNI Ports | 52
- Assigning Device Roles | 53
- Deleting UNIs | 53
- Discovering Device Roles | 54
- Excluding Interfaces from UNI Role Assignments | 56
- VLAN Pool Profiles Overview | 57
- Viewing Pre-Staging Statistics | 58
- Viewing Pre-Staging Rules | 60
- Migrating Service Interfaces in Cross Provisioning Platform | 61
- Creating a User-Specific Role to Prevent or Allow Certain Actions on a Service | 65

Adding a UNI

To add a UNI to the list of UNIs that can be assigned to a service on a specific device:

1. In the **Network Activate** task pane, select the **Prestage Devices > Manage Device Roles**.
2. In the **Manage Device Roles** window, select the device on which you want to add an interface to the list of potential UNIs.
3. Open the **Actions** menu and select **Add Device UNIs**.
4. The **Assign Device UNIs** window appears, displaying all interfaces on the device that have not been assigned.
5. Select the interface you want to make available for assignment as a UNI. To select multiple interfaces, use the multiple selection feature.

6. Open the **Actions** menu and select **Assign UNI**.
7. In the **Assign UNI role** window, click **Confirm** to assign the UNI.

RELATED DOCUMENTATION

[Viewing N-PE Devices | 79](#)

[Deleting UNIs | 53](#)

Managing NNI Ports

Along with user-to-network interface (UNI) ports, the Cross Provisioning Platform application enables you to configure network-to-network interface (NNI) ports on a device. You can configure the NNI ports on Juniper Networks and Nokia devices.

To manage or add a network-to-network interface (NNI) for a specific device:

1. In the Cross Provisioning Platform task pane, select the **Prestage Devices > Manage Device Roles**.

The Manage Device Roles window appears.

2. In the Manage Device Roles window, select the device to which you want to add an NNI port.

3. Open the **Actions** menu and select **Manage Device NNIs**.

The Manage Device NNIs page appears.

4. Click the **+** option to add an NNI.

The Add Device NNIs window appears, displaying all NNI ports on the device that have not been managed.

5. Select the interface you want to make available for assignment as an NNI. To select multiple interfaces, use the multiple selection feature.

6. Open the **Actions** menu and select **Assign NNI**.

7. In the Assign NNI role window, click **Confirm** to assign the NNI.

A new column `isNNIPort` is added on the View Third Party Devices page. If a device has an NNI port, the `isNNIPort` value is `true`.

To delete an NNI, select the NNI interface from the Manage Device NNIs page and select **Delete NNI**.

RELATED DOCUMENTATION

| [Assigning Device Roles](#) | 53

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 71](#).

To assign all discovered roles and interfaces:

1. In the **Network Activate** task pane, select **Prestage Devices > Manage Device Roles > Assign Roles**.
2. In the **Assign Roles** page, click **Multiple** in the quick view pane and select all devices.
3. Open the **Actions** menu and select **Assign NPE Role**.
4. In the confirmation window, click **Assign**.
5. To view the assignment status, in the **Job Management** window, click the job ID of the assignment job.

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.

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. In the **Network Activate** task pane, select the **Prestage Devices > Manage Device Roles**.
2. In the **Manage Device Roles** page, select the device you want to work on.
3. Open the **Actions** menu and select **Manage Device UNIs**.
The **Manage Device UNIs** window appears, showing all interfaces assigned the UNI role.
4. Select the interface you no longer want to have the UNI role. To unassign multiple interfaces, use the multiple selection feature.
5. Open the **Actions** menu and select **Delete UNI**.
6. In the **Exclude from UNI Role** confirmation window, click **Exclude**.

RELATED DOCUMENTATION

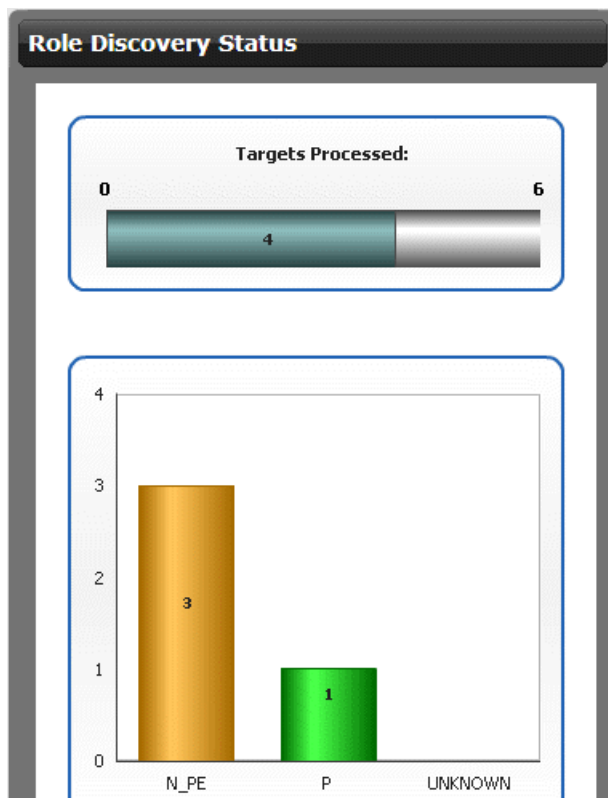
[Viewing N-PE Devices | 79](#)

[Adding a UNI | 51](#)

Discovering Device Roles

To discover the roles of devices found during element discovery:

1. In the **Network Activate** task pane, select **Prestage Devices > Manage Device Roles > Discover Roles**.
The **Role Discovery Status** window shows the discovery of unassigned devices found in the database.:



The graph portion of this example shows how many of the unassigned devices the pre-staging rules determined could be assigned the N-PE role and how many could be assigned the P role. The UNKNOWN bar indicates devices that had no MPLS role assigned but for which the Network Activate software was unable to recommend a role.

NOTE: You cannot discover a device as a PE device if no user-to-network interfaces (UNIs) are available in the device.

The Network Activate 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
```

2. To view the devices for which the Network Activate software recommends the PE role, click on the N_PE bar.

The **Assign Roles** window appears.

The question mark on each icon indicates that the device role has not yet been assigned.

Device role discovery is now complete. To assign device and interface roles, follow the steps in the next section, [“Assigning Device Roles” on page 53](#).

Excluding Interfaces from UNI Role Assignments

To exclude interfaces from the list of interfaces that the pre-staging rules determined were suitable for use as UNIs:

1. In the **Network Activate** task pane, select **Prestage Devices > Manage Device Roles > Assign Roles**.

The results of the most recent role discovery operation appear, including any changes you have subsequently made to your pre-staging data.

Repeat Step 2 through Step 7 for each device for which you want to exclude some recommended UNI selections:

2. In the **Assign Roles** page, select the device for which you want to manage UNIs.

3. Open the **Actions** menu and select **Manage Device UNIs**.

The **Manage Device UNIs** window shows all the device interfaces for the selected device and indicates those that the Network Activate software recommends for use as UNIs.

4. In the **Manage Device UNIs** window, select the UNI you want to exclude.

To exclude more than one UNI, use the multiple selection capability.

5. Open the **Actions** menu and select **Exclude from UNI Role**.

6. Open the **Actions** menu and select **Return to Assign Roles** to return to the **Assign Roles** page.

RELATED DOCUMENTATION

| [Excluding Devices from N-PE Role Assignment](#) | 73

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 Network Activate 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, Network Activate 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 Network Activate software assigns the appropriate VLAN range.

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

RELATED DOCUMENTATION

[Prestaging Devices Process Overview | 37](#)

[Prerequisites for Prestaging Devices in Network Activate | 44](#)

[Viewing Pre-Staging Rules | 60](#)

[Discovering and Assigning All N-PE Devices | 68](#)

[Discovering and Assigning N-PE Devices with Exceptions | 71](#)

Viewing Pre-Staging 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:

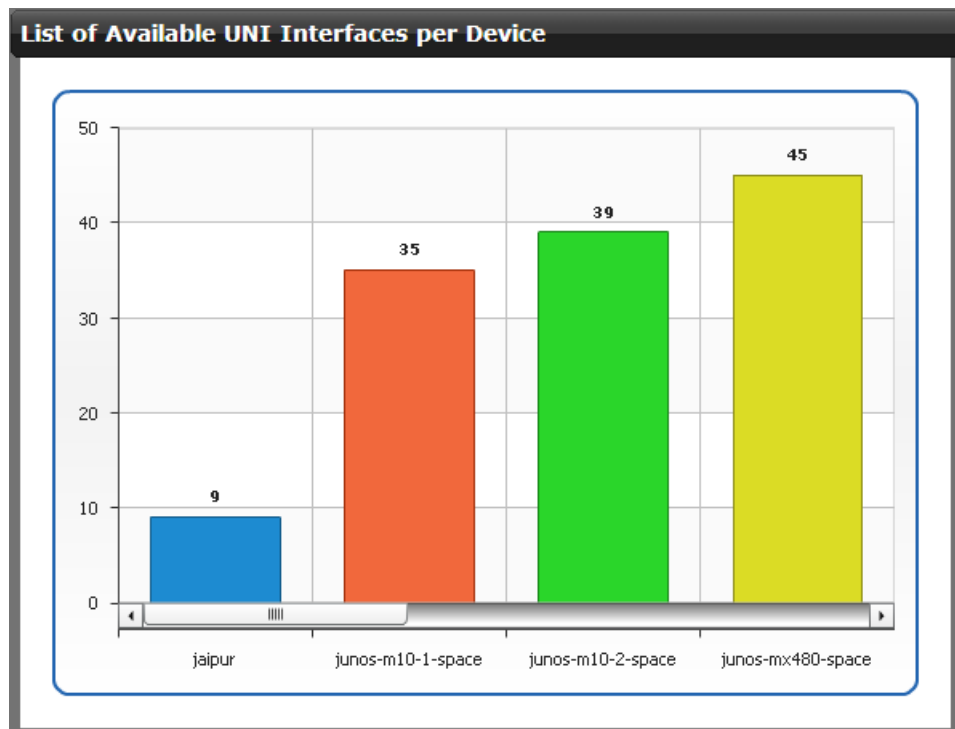
- [Viewing Available UNIs on N-PE Devices | 58](#)
- [Viewing Services on N-PE Devices | 59](#)

Viewing Available UNIs on N-PE Devices

To view the number of available UNIs on each device allocated an N-PE role:

1. In the **Network Activate** task pane, select **Prestage Devices**.

The Junos Space software displays the chart named List of Available UNI Interfaces per Device.



Each vertical bar represents an N-PE device. The number of UNIs is shown on the Y axis. If more than four devices on your network have been assigned the N-PE role, drag the slider across the bottom of the graph to view all devices.

2. To list the UNIs configured on a specific N-PE device:
 - a. Click on the bar that represents the device.
 - b. In the **Manage Device Roles** page, double-click the device.

The **Manage Device Roles** page shows only the data for the selected device.

SEE ALSO

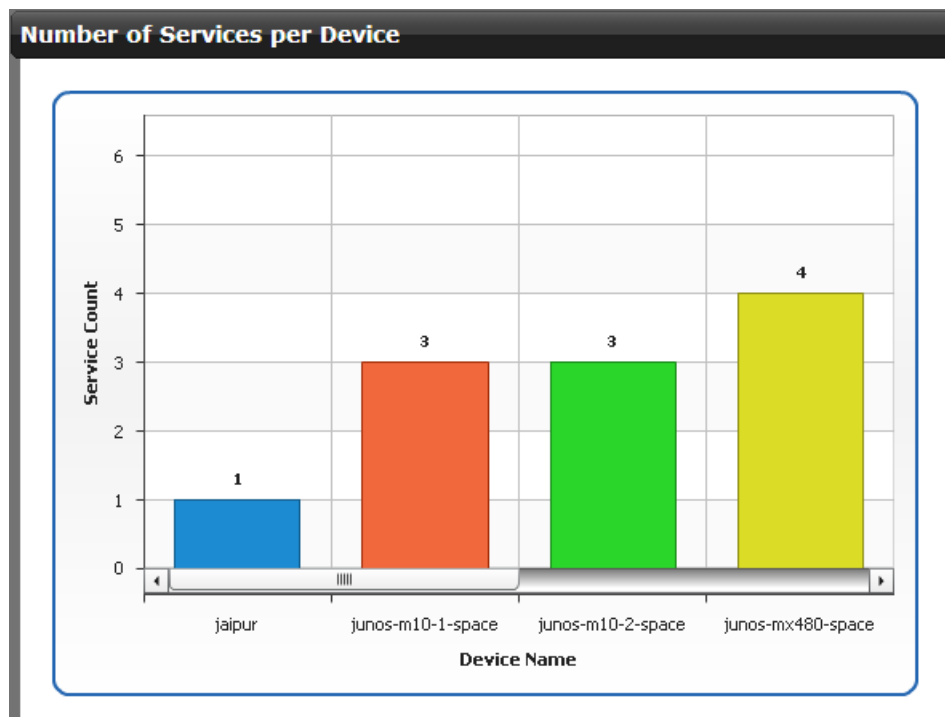
[Viewing Services on N-PE Devices](#) | 59

Viewing Services on N-PE Devices

To view the number of services provisioned on each N-PE device in your network:

1. In the **Network Activate** task pane, select **Prestage Devices**.

The Junos Space software displays the chart named Number of Services per Device.



2. Each vertical bar represents an N-PE device. The number of services provisioned on each device is shown on the Y axis. If more than four devices on your network have been assigned the N-PE role, drag the slider across the bottom of the graph to view all devices.

- 3. To find out more information about the services provisioned on a specific device, click on the bar that represents the device.

The **Manage Services** page displays only those services provisioned on that device.

SEE ALSO

| [Viewing Pre-Staging Rules](#) | 60

RELATED DOCUMENTATION

Prestaging Devices Overview 36
Viewing Services 832
<i>Viewing Managed Devices</i>

Viewing Pre-Staging Rules

Pre-staging 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 pre-staging 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 pre-staging rules. You can view a summary of all pre-staging rules, see a summary, or view details of a specific pre-staging rule.

- [Viewing Pre-Staging Rules in a Table](#) | 60

Viewing Pre-Staging Rules in a Table

To view pre-staging rules in a tabular format:

1. In the **Network Activate** task pane, select **Prestage Devices > Manage Device Roles > Rules**.

The **Rules** window appears.

The **Rules** window lists all the pre-staging rules by type, along with the name and a brief description of each rule.

2. To view rule details, including a sample configuration, double-click the table row.

SEE ALSO

[Viewing Pre-Staging Statistics | 58](#)

RELATED DOCUMENTATION

[Prestaging Devices Overview | 36](#)

[Viewing N-PE Devices | 79](#)

[Discovering and Assigning All N-PE Devices | 68](#)

[Discovering and Assigning N-PE Devices with Exceptions | 71](#)

Migrating Service Interfaces in Cross Provisioning Platform

When an interface becomes faulty or needs to be migrated to a higher-capacity port, you must migrate all services deployed on a specific interface to the destination interface on the same device. In all the devices of Juniper Networks, the Cross Provisioning Platform application actually modifies the device configuration to migrate all the services. The Cross Provisioning Platform application deletes the source interface and adds the destination interface to the service. A migration XSLT script is required to generate the configuration changes to delete or add an interface from or to a service. The script is independent of the service type and attached to the device configlet definition.

Before you can migrate the service interfaces in Cross Provisioning Platform, make sure that the configuration script and the GUI script are present in the local machine.

To migrate interfaces on third-party devices, a third-party network management product is required to modify the device configuration.

To perform service interface migration on Juniper Networks devices:

1. From the **Cross Provisioning Platform** task pane, select **CPP > Scripts**.

The **Scripts** page that appears displays a list of existing scripts in the Cross Provisioning Platform application.

2. Click **Add Script** above the tool grid.

The **Add Script(s)** page appears.

3. In the **Name** field, type 3 through 128 alphanumeric characters to identify the name of the script.
4. In the **Description** field, type 3 through 128 alphanumeric characters to further identify the script you named.
5. From the **Vendor Type** drop-down list, select **Junos Space**.
6. Click **Browse** and select the configuration script and the GUI script from the local machine to add them to the Cross Provisioning Platform application.
7. Click **Create** to add the scripts that you uploaded.

A confirmation dialog box appears with the **Scripts added successfully** message.

8. Click **OK**.
9. From the **Cross Provisioning Platform** task pane, select **CPP > Service Definition**.

The **Service Definition** page that appears displays a list of the existing service definitions in the Cross Provisioning Platform application.

10. Click the **Create CPP Service Definition** icon above the tool grid.

The **Create Service Definition** dialog box appears with the **General**, the **SAM Service Scripts**, and the **JUNOS Space Service Scripts** sections.

11. On the **Create Service Definition** page, perform the following steps:

- In the **General** section:
 - a. In the **Name** field, type 3 through 128 alphanumeric characters to identify the name of the service definition.
 - b. In the **Description** field, type 3 through 128 alphanumeric characters to further identify the service definition you named.
 - c. From the **Type** drop-down list, select **Device**.
- In the **SAM Service Scripts** section:
 - a. From the **Creation** drop-down list, select the appropriate SAM service script.
 - b. From the **Modification** drop-down list, select the appropriate SAM service script.
- In the **JUNOS Space Service Scripts** section:
 - a. From the **Creation** drop-down list, select the appropriate Junos Space service script.

- b. From the **Modification** drop-down list, select the appropriate Junos Space service script.

12. Click **Create**.

The **Service Definition** page appears with the existing service definitions along with the service definition that you created.

13. From the **Cross Provisioning Platform** task pane, select **CPP > Bulk Service Operations**.

The page that appears has three option buttons: **Service Deletion**, **Interface Migration** and **Resync Services**.

14. Select the **Interface Migration** option button.

The page that appears has three grids: **Step 1: Select From Device**, **Step 1: Select From Interface**, and **View Service(s)**.

15. On the **Step 1: Select From Device**, select **Vendor** as **Juniper** and select the Juniper Networks device from the list.

The corresponding interfaces are listed on the **Step 2: Select From Interface** grid.

16. On the **Step 2: Select From Interface** grid, select an interface.

The corresponding services are listed on the **View Service(s)** grid.

17. Click **Next**.

The **Interface Migration** window appears.

18. Perform the following steps on the **Interface Migration** page:

- a. From the **Service Definition** drop-down list, select the service definition that you created.
- b. In the **Description** field, type 3 through 128 alphanumeric characters to identify the service interface migration.
- c. From the **To Interface** drop-down list, select an interface to which you want to migrate the services.

19. Click **Migrate** to initiate the service interface migration.

A job is triggered to show the migration status.

NOTE: When you migrate one service interface, the configuration of all the services present in that interface from the device **CLI**, irrespective of the services present on the Junos Space server, are also migrated. You can do the service interface migration only for one device at a time.

Perform the following steps to migrate services to third-party devices:

1. From the **Cross Provisioning Platform** task pane, select **CPP > Bulk Service Operations**.

The page that appears has three option buttons: **Service Deletion**, **Interface Migration** and **Resync Services**.

2. Select the **Interface Migration** option button.

The page that appears has three grids: **Step 1: Select From Device**, **Step 1: Select From Interface**, and **View Service(s)**.

3. On the **Step 1: Select From Device**, select **Vendor** as **Alcatel** and select the Nokia device from the list.

The corresponding interfaces are listed on the **Step 2: Select From Interface** grid.

4. On the **Step 2: Select From Interface** grid, select an interface.

The corresponding services are listed on the **View Service(s)** grid.

5. Click **Next**.

The **Interface Migration** window appears.

6. Perform the following steps:

- In the **To Interface** field, click the drop-down to select an interface to which you want to migrate the services.
- In the **Service Definition** field, click the drop-down field to select the service definition associated with this migration.
- In the **Description** field, type 3 through 128 alphanumeric characters to describe this service interface migration.

7. Click **Migrate** to initiate the service interface migration.

A job is triggered to show the migration status.

NOTE: If you have created multi-vendor services, i.e. JNPR-ALU and need to migrate the end point of both Juniper Networks and the third-party devices, then you need to perform the migration on the third-party devices using a third-party network management product first and then perform the migration on Juniper Networks devices and third party devices in Cross Provisioning Platform in the same manner as above. This records all the changes related to this migration in the Cross Provisioning Platform database.

RELATED DOCUMENTATION

| [Adding Scripts Created for Cross Provisioning Platform | 775](#)

Creating a User-Specific Role to Prevent or Allow Certain Actions on a Service

IN THIS SECTION

- [Creating a User-Specific Role | 65](#)
- [Applying the New Role to a User | 67](#)

With Cross Provisioning Platform Release 15.1R1, you can create a user-specific role that prevents or allows the following actions on the Service page by the user to whom the role is assigned:

- Decommissioning a service
- Modifying a service
- Bulk-decommissioning services on Service and Bulk Service Operations pages
- Re-creating a service order after a failed deployment
- Bulk-modifying services

Complete the following tasks to create a role and assign the role to a specific user account:

Creating a User-Specific Role

NOTE: Only an administrator can create a role.

To create a user-specific role:

1. On the Junos Space 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.

3. In the **Title** text box, type a role name.

The role name cannot exceed 32 characters. The name can contain letters, numbers, and the following special characters: hyphen (-), underscore (_), and period (.).

4. In the **Description** text box, type a role description.

The role description cannot exceed 256 characters. The description can contain letters, numbers, and the following special characters: hyphen (-), underscore (_), period (.), and comma (,).

5. Select the **CPP** workspace from the application selection ribbon.

Mouse over an application workspace icon to view the application workspace name. An expandable and collapsible tree of associated tasks appear below the selection ribbon for you to modify specific tasks that you want included on the Task Summary pane.

6. On the **CPP** task pane, select or clear the following check boxes:

- **Modify PW-LDP**—If you want to create a user-specific role to allow the user to modify an LDP-based point-to-point CPP service, select the **Modify PW-LDP** check box.
- **Modify PW-BGP**—If you want to create a user-specific role to allow the user to modify a BGP-based point-to-point CPP service, select the **Modify PW-BGP** check box.
- **Modify L3VPN**—If you want to create a user-specific role to allow the user to modify a Layer 3 VPN CPP service, select the **Modify L3VPN** check box.
- **Modify VPLS**—If you want to create a user-specific role to allow the user to modify a VPLS CPP service, select the **Modify VPLS** check box.
- **Decommission PW-LDP**—If you want to create a user-specific role to allow the user to decommission an LDP-based point-to-point CPP service, select the **Decommission PW-LDP** check box.
- **Decommission PW-BGP**—If you want to create a user-specific role to allow the user to decommission a BGP-based point-to-point CPP service, select the **Decommission PW-BGP** check box.
- **Decommission L3VPN**—If you want to create a user-specific role to allow the user to decommission a Layer 3 VPN CPP service, select the **Decommission L3VPN** check box.
- **Decommission VPLS**—If you want to create a user-specific role to allow the user to decommission a VPLS CPP service, select the **Decommission VPLS** check box.
- **Bulk Service Operations**—If you want to create a user-specific role to allow the user to perform bulk service operations, select the **Bulk Service Operations** check box.

For example, if you move the newly created role with the **Modify L3VPN** check box selected, the user can modify the Layer 3 VPN service on the **CPP > Services** inventory page.

If you move the newly created role with the **Modify L3VPN** check box cleared, the user cannot modify the Layer 3 VPN service on the **CPP > Services** inventory page.

7. Click **Create**.

The new user role is created. Apply the new role to a user account.

Applying the New Role to a User

NOTE: Only an administrator can assign a role to a user account.

To apply the new role to a user account:

1. On the Junos Space Platform user interface, select **Role Based Access Control > User Accounts**.

The User Accounts inventory page appears.

2. From the inventory page, right-click the user account that you want to modify and select **Modify User**.

The Modify User page appears. The Modify User page contains three areas—General, Role Assignment, and Domain Assignment

3. To add or remove role assignments, click **Role Assignment** on the upper right of the Modify User page.

4. Move the newly created role to the **Selected** list and click **Finish**.

The new role is now applied to the selected user account.

RELATED DOCUMENTATION

[Modifying a Service in Cross Provisioning Platform | 873](#)

[Decommissioning a Service | 834](#)

N-PE Devices and Role Assignments

IN THIS CHAPTER

- [Discovering and Assigning All N-PE Devices | 68](#)
- [Discovering and Assigning N-PE Devices with Exceptions | 71](#)
- [Changing the Loopback Address of an N-PE Device | 77](#)
- [Excluding Devices from N-PE Role Assignment | 78](#)
- [Unassigning N-PE Devices | 78](#)
- [Viewing N-PE Devices | 79](#)
- [Troubleshooting N-PE Devices Before Provisioning a Service | 80](#)

Discovering and Assigning All N-PE Devices

Pre-staging all Network Activate assignment recommendations is a powerful yet simple way to prepare your devices for provisioning. This procedure provides the pre-staging steps that accept all system recommendations. To pre-stage devices and make exceptions to the system recommendations, see [“Discovering and Assigning N-PE Devices with Exceptions” on page 71](#).

Before discovering and assigning N-PE devices, you must have already run device discovery. See *Discovering Devices* in the *Junos Space Network Application Platform User Guide*.

Pre-staging has two parts:

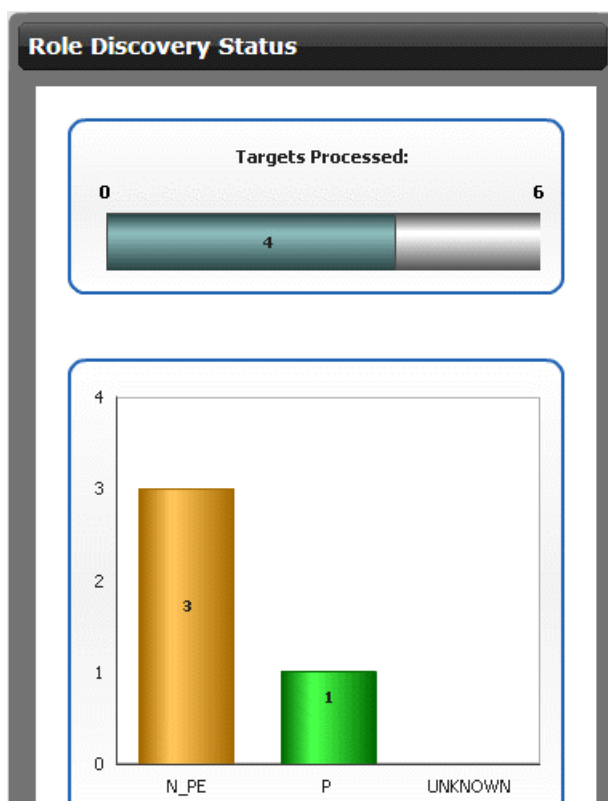
1. [Discovering Device Roles | 68](#)
2. [Assigning Device Roles | 70](#)

Discovering Device Roles

To discover the roles of devices found during element discovery:

1. In the **Network Activate** task pane, select **Prestage Devices > Manage Device Roles > Discover Roles**.

The **Role Discovery Status** window shows the discovery of unassigned devices found in the database.:



The graph portion of this example shows how many of the unassigned devices the pre-staging rules determined could be assigned the N-PE role and how many could be assigned the P role. The UNKNOWN bar indicates devices that had no MPLS role assigned but for which the Network Activate software was unable to recommend a role.

NOTE: You cannot discover a device as a PE device if no user-to-network interfaces (UNIs) are available in the device.

The Network Activate 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
```

2. To view the devices for which the Network Activate software recommends the PE role, click on the N_PE bar.

The **Assign Roles** window appears.

The question mark on each icon indicates that the device role has not yet been assigned.

Device role discovery is now complete. To assign device and interface roles, follow the steps in the next section, [“Assigning Device Roles” on page 53](#).

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 71](#).

To assign all discovered roles and interfaces:

1. In the **Network Activate** task pane, select **Prestage Devices > Manage Device Roles > Assign Roles**.
2. In the **Assign Roles** page, click **Multiple** in the quick view pane and select all devices.
3. Open the **Actions** menu and select **Assign NPE Role**.
4. In the confirmation window, click **Assign**.
5. To view the assignment status, in the **Job Management** window, click the job ID of the assignment job.

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 Overview | 36](#)

[Discovering and Assigning N-PE Devices with Exceptions | 71](#)

[Unassigning N-PE Devices | 78](#)

[Deleting UNIs | 53](#)

[Viewing Jobs in the Junos Space Network Application Platform User Guide](#)

[Viewing Pre-Staging Rules | 60](#)

[Discovering Devices in the Junos Space Network Application Platform User Guide](#)

Discovering and Assigning N-PE Devices with Exceptions

Preparing network devices for service activation is usually a simple process which directs the Network Activate software to prepare your devices automatically. When you pre-stage devices, the Network Activate software 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 Network Activate software 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 Network Activate software makes, see [“Discovering and Assigning All N-PE Devices” on page 68](#). These topics describe how to pre-stage devices with exceptions:

- [Discovering Device Roles | 71](#)
- [Excluding Devices from N-PE Role Assignment | 73](#)
- [Changing the Loopback Address of an N-PE Device | 74](#)
- [Excluding Interfaces from UNI Role Assignments | 74](#)
- [Committing Your Pre-Staging Choices | 75](#)

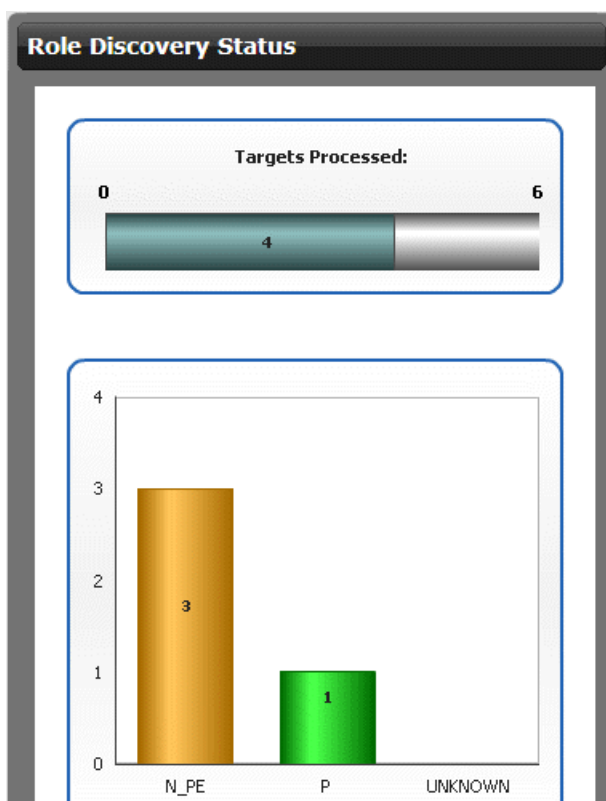
Discovering Device Roles

Before discovering device roles, you must run device discovery. See *Discovering Devices* in the *Junos Space Network Application Platform User Guide*.

To discover unassigned PE devices:

1. In the **Network Activate** task pane, select **Prestage Devices > Manage Device Roles > Discover Roles**.

The **Role Discovery Status** window shows the discovery of unassigned devices found in the database.



NOTE: If this is not the first time you have run the discover roles operation, this action overwrites any recommendations remaining from the previous discover roles operation. Devices with confirmed roles are not affected.

The Targets Processed box contains a progress bar, which when finished, shows how many unassigned devices the Network Activate software found in its database.

The graph portion of this example shows how many of the unassigned devices the pre-staging rules determined could be assigned the N-PE role and how many could be assigned the P role. The UNKNOWN bar indicates devices that had no MPLS role assigned but for which the Network Activate software was unable to recommend a role.

2. To view the devices for which the Network Activate software recommends the PE role, click on the N_PE bar.

The **Assign Roles** page appears.

The question mark on each icon indicates that the device role has not yet been assigned.

NOTE: You cannot discover a device as a PE device if no user-to-network interfaces (UNIs) are available in the device.

The Network Activate 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
```

Excluding Devices from N-PE Role Assignment

The rules-driven process that the Network Activate software uses to discover device roles recommends the correct roles in most cases. To exclude a device from N-PE role assignment:

1. In the **Network Activate** task pane, select **Prestage Devices > Manage Device Roles > Assign Roles**.

The results of the most recent role discovery operation appear.

2. In the **Assign Roles** page, select the N-PE device that you want to exclude from role assignment. To exclude several N-PE devices, use the multiple selection capability.

3. Open the **Actions** menu and select **Exclude from NPE Role**.

The **Assign Roles** page refreshes. The excluded devices are no longer visible.

SEE ALSO

[Changing the Loopback Address of an N-PE Device](#) | 74

Changing the Loopback Address of an N-PE Device

The Network Activate software allows you to change the loopback address of an N-PE device to that of a different loopback unit.

NOTE: Although Junos software 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 loopback address of an N-PE device:

1. In the **Network Activate** task pane, select **Prestage Devices > Manage Device Roles > Assign Roles**.

The results of the most recent role discovery operation appear, including any changes you have subsequently made to your pre-staging data.

Repeat Step 2 through Step 5 for each device for which you want to change the loopback address.

2. In the **Assign Roles** page, select the device for which you want to change the loopback address.
3. Open the **Actions** menu and select **Modify Loopback Address**.
4. In the **Modify Loopback Address** window, select the loopback address you want to use.
5. Click **Modify**.

The new loopback address appears.

SEE ALSO

| [Excluding Devices from N-PE Role Assignment](#) | 73

Excluding Interfaces from UNI Role Assignments

To exclude interfaces from the list of interfaces that the pre-staging rules determined were suitable for use as UNIs:

1. In the **Network Activate** task pane, select **Prestage Devices > Manage Device Roles > Assign Roles**.

The results of the most recent role discovery operation appear, including any changes you have subsequently made to your pre-staging data.

Repeat Step 2 through Step 7 for each device for which you want to exclude some recommended UNI selections:

2. In the **Assign Roles** page, select the device for which you want to manage UNIs.

3. Open the **Actions** menu and select **Manage Device UNIs**.

The **Manage Device UNIs** window shows all the device interfaces for the selected device and indicates those that the Network Activate software recommends for use as UNIs.

4. In the **Manage Device UNIs** window, select the UNI you want to exclude.

To exclude more than one UNI, use the multiple selection capability.

5. Open the **Actions** menu and select **Exclude from UNI Role**.

6. Open the **Actions** menu and select **Return to Assign Roles** to return to the **Assign Roles** page.

SEE ALSO

| [Excluding Devices from N-PE Role Assignment](#) | 73

Committing Your Pre-Staging Choices

This procedure provides instructions for assigning the N-PE role to selected devices and committing all device pre-staging 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 pre-staging choices to the database:

1. In the **Network Activate** task pane, select **Prestage Devices > Manage Device Roles > Assign Roles**.
2. Examine the list of devices to be sure these are the devices you want to assign the N-PE role.
3. Select all devices.
4. Open the **Actions** menu and click **Assign NPE Role**.
5. In the confirmation screen, click **Assign**.
6. 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. 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.

NOTE: After you pre-stage a device, you can check to see if a particular device is capable of supporting Layer 2 or Layer 3 services.

In the Network Activate task pane, select **Prestage Devices > Manage Device Roles**. Double-click the device for which you want to check its service capability. The **NPE Details** window appears.

Check the **Service capability** field to ensure that the values L2, L3 appear, which indicate that the device can support Layer 2 and Layer 3 services.

NOTE: If you modify the configuration of a device after the device is pre-staged, remove the device from pre-staged status and then Discover Roles and pre-stage the device again.

RELATED DOCUMENTATION

[Prestaging Devices Overview | 36](#)

[Discovering and Assigning All N-PE Devices | 68](#)

[Unassigning N-PE Devices | 78](#)

[Adding a UNI | 51](#)

[Deleting UNIs | 53](#)

[Viewing Jobs in the Junos Space Network Application Platform User Guide](#)

[Viewing Pre-Staging Rules | 60](#)

[Viewing N-PE Devices | 79](#)

[Discovering Devices in the Junos Space Network Application Platform User Guide](#)

Changing the Loopback Address of an N-PE Device

The Network Activate software allows you to change the loopback address of an N-PE device to that of a different loopback unit.

NOTE: Although Junos software 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 loopback address of an N-PE device:

1. In the **Network Activate** task pane, select **Prestage Devices > Manage Device Roles > Assign Roles**.

The results of the most recent role discovery operation appear, including any changes you have subsequently made to your pre-staging data.

Repeat Step 2 through Step 5 for each device for which you want to change the loopback address.

2. In the **Assign Roles** page, select the device for which you want to change the loopback address.
3. Open the **Actions** menu and select **Modify Loopback Address**.
4. In the **Modify Loopback Address** window, select the loopback address you want to use.
5. Click **Modify**.

The new loopback address appears.

RELATED DOCUMENTATION

Excluding Devices from N-PE Role Assignment

The rules-driven process that the Network Activate software uses to discover device roles recommends the correct roles in most cases. To exclude a device from N-PE role assignment:

1. In the **Network Activate** task pane, select **Prestage Devices** > **Manage Device Roles** > **Assign Roles**.

The results of the most recent role discovery operation appear.

2. In the **Assign Roles** page, select the N-PE device that you want to exclude from role assignment. To exclude several N-PE devices, use the multiple selection capability.

3. Open the **Actions** menu and select **Exclude from NPE Role**.

The **Assign Roles** page refreshes. The excluded devices are no longer visible.

RELATED DOCUMENTATION

| [Changing the Loopback Address of an N-PE Device](#) | 74

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. In the **Network Activate** task pane, select **Prestage Devices** > **Manage Device Roles**.
2. In the **Manage Device Roles** page, select the N-PE device you want to unassign.
3. Open the **Actions** menu and select **Unassign NPE Role**.

NOTE: If services are deployed on this device, the Unassign NPE Role action will be dimmed and not selectable.

4. The **Manage Device Roles** page refreshes and shows that the selected device has been removed.

RELATED DOCUMENTATION

[Viewing N-PE Devices | 79](#)

[Discovering and Assigning All N-PE Devices | 68](#)

[Discovering and Assigning N-PE Devices with Exceptions | 71](#)

Viewing N-PE Devices

You can view network devices that have been assigned the N-PE role.

The following topic provides a procedure for viewing N-PE devices:

- [Viewing N-PE Devices in a Table | 79](#)

Viewing N-PE Devices in a Table

To view N-PE devices in a table:

1. In the Network Activate task pane, select **Prestage Devices > Manage Device Roles**.

The **Manage Device Roles** page displays the following information about all N-PE devices on your network:

- Name—The assigned device name.
- 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.

2. To view more device details and UNI information, double-click the table row for the device. 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:

- Name—The name assigned to the device
- MPLS role—The assigned MPLS role for the N-PE 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.
- Connection status—up or down.
- Service capability—N-PE device role: L2 or L3.
- UNI Interfaces—All assigned UNIs on the device with the applied VLAN pool profile.

SEE ALSO

[Viewing Available UNIs on N-PE Devices | 58](#)

[Viewing Services on N-PE Devices | 59](#)

RELATED DOCUMENTATION

[Prestaging Devices Overview | 36](#)

[Viewing Pre-Staging Statistics | 58](#)

[Viewing Pre-Staging Rules | 60](#)

[Adding a UNI | 51](#)

[Unassigning N-PE Devices | 78](#)

[Deleting UNIs | 53](#)

Discovering Devices in the Junos Space Network Application Platform User Guide

Troubleshooting N-PE Devices Before Provisioning a Service

You can use the **Troubleshoot** option in Network Activate 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 Activate** 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 3: 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
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.

Table 3: Commands Available in the Troubleshoot Device Window (*continued*)

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 Configuration Audit | 1062](#)

[Viewing Configuration Audit Results | 1078](#)

[Performing a Functional Audit | 1064](#)

[Viewing Functional Audit Results | 1081](#)

[Canceling a Job](#)

Multihomed Groups

IN THIS CHAPTER

- [Multihomed Groups Overview | 83](#)
- [Creating a Multihomed Group | 87](#)
- [Deleting Multihomed Groups | 90](#)
- [Viewing Multihomed Groups | 90](#)
- [Viewing a Sample Connectivity File for Multihomed Groups | 92](#)

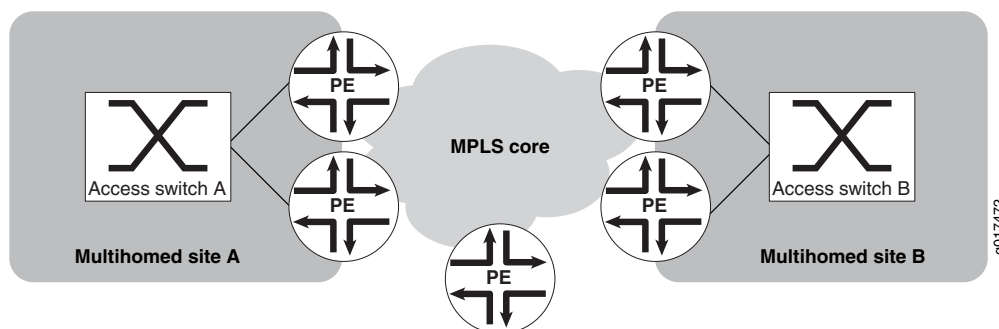
Multihomed Groups Overview

IN THIS SECTION

- [Prerequisites to Create Multihomed Groups | 84](#)
- [Required N-PE Device Configuration | 85](#)
- [Administrator Roles Required to Create Multihomed Groups | 85](#)
- [Creating Multihomed Groups Process Overview | 86](#)

In the Junos Space product, you can create a multihomed group to connect a customer site to multiple PE routers to provide redundant connectivity across a VPLS site, while preventing the formation of Layer 2 loops in the service provider's network. A VPLS site multihomed to two or more N-PE routers provides redundant connectivity in the event of a PE-router-to-CE-device link failure or the failure of an N-PE router. [Figure 1 on page 84](#) shows two multihomed sites in which each access switch is connected to a primary and a backup PE router. If the PE router functioning as the primary device fails or the link connection between the access switch and PE router fails, the backup PE router automatically takes over the role of primary device.

Figure 1: Multihomed Sites Connected to Primary and Backup PR Routers



This multihomed groups overview includes the following topics:

Prerequisites to Create Multihomed Groups

The following requirements must be met before you create a multihomed group:

- Ensure that the N-PE devices included in the multihomed group meet the following requirements:
 - The same site ID is assigned to the N-PE devices that are connected to the same CE devices.
 - The same route distinguisher is assigned to the N-PE devices that are connected to the same CE devices.
 - The N-PE device is either designated as a primary interface or allows the router to select the interface to be used as the primary interface.

If the router selects the interface, the interface that is used to connect the N-PE device to the site depends on the order in which the interfaces are listed in the N-PE device's configuration. The first operational interface in the set of configured interfaces is selected as the designated interface. If this interface fails, the next interface in the list is selected to send and receive traffic for the site.

- Perform device discovery to import the N-PE devices that you want to include in the multihomed group.
- Pre-stage the N-PE devices that you want to include in multihomed groups.

Required N-PE Device Configuration

The configuration for each N-PE device that you include in a multihomed group must include the following statements:

```
[edit routing-instances routing-instance-name]
instance-type vpls;
interface interface-name;
interface interface-name;
protocols vpls {
  site site-name {
    active-interface {
      any;
      primary interface-name;
    }
    interface interface-name;
    interface interface-name;
    multihoming;
    site-identifier number;
  }
}
route-distinguisher (as-number:id |ip-address:id)
```

Administrator Roles Required to Create Multihomed Groups

The steps required to create a multihomed group are 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 the PE devices that you want to include in the multihomed group.
- The Service Manager role allows an administrator to perform device pre-staging actions including discovering and assigning device roles and importing the connectivity file for the multihomed group.
- 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.

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

Creating Multihomed Groups Process Overview

To create a multihomed group to connect a customer site to multiple PE routers:

1. Create an XML connectivity file to name the multihomed group and configure endpoint connections between the CE device (access switch) and N-PE devices—Each multihomed group connects individual customer sites to up to three PE routers to provide redundant connectivity across a VPLS site. For step-by-step instructions on creating an XML connectivity file for multihomed groups, see [“Creating a Connectivity File for Multihomed Groups” on page 87](#).
2. Upload the XML connectivity file in Junos Space—After you create the XML connectivity file, you upload it to Junos Space. For step-by-step instructions on uploading an XML connectivity file for multihomed groups, see [“Uploading a Connectivity File to Create Multihomed Groups” on page 89](#).
3. Create a VPLS service definition with multihoming enabled.
4. Publish the VPLS service definition.
5. Create a customer for the service.
6. Create a VPLS service order based on a VPLS service definition with multihoming enabled.

When you create the service order, you select one or more multihomed groups you want to include in the service from the Select Endpoint PE devices screen.

7. Deploy the service order.
8. Perform a functional audit to determine whether the service is up or down.

If the functional audit reports that the service is up, the customer(s) can begin using the service.

NOTE: You are required to create a multihomed group only if you intend to create redundant VPLS services. For point-to-point LDP services and Layer 2 VPN services, you can enable the redundant feature when you create the service order.

RELATED DOCUMENTATION

[Creating a Multihomed Group | 87](#)

[Deleting Multihomed Groups | 90](#)

Creating a Multihomed Group

In Junos Space, you can create a multihomed group to connect a customer site to multiple PE routers to provide redundant connectivity across a VPLS site. A VPLS site multihomed to two or more N-PE routers provides redundant connectivity in the event of a PE-router-to-CE-device link failure or the failure of an N-PE router.

To create one or more multihomed groups, complete the following tasks:

1. [Creating a Connectivity File for Multihomed Groups | 87](#)
2. [Uploading a Connectivity File to Create Multihomed Groups | 89](#)

Creating a Connectivity File for Multihomed Groups

The connectivity file can include one or more multihomed groups. Each multihomed group defines an access switch that is connected to one primary PE device and one or more backup PE devices.

The following requirements must be met before you create a connectivity file for a multihomed group:

- Perform device discovery to import the N-PE devices that you want to include in the multihomed group.
- Pre-stage the N-PE devices that you want to include in the multihomed group.

You must create an XML file to define connectivity for the PE devices in a multihomed group. You can specify any name for the connectivity file, but it must be a valid XML file that includes the following attributes:

- **Name**—Multihomed group name.
- **Description**—Multihomed group description.
- **AccessSwitchIP**—IP address for the CE device.
- **PEHostName**—Hostname for the N-PE device. Include two or more hostnames to identify the primary and secondary PE devices in the multihomed group.

NOTE: By default, the first PEHostname specifies the primary device.

- **PEInterface**—UNI on the N-PE device that connects to the CE device. Each multihomed group must specify the interface for the primary and secondary PE devices.
- **AccessSwitchInterface**—UNI on the CE device that connects to the primary or secondary PE device.

The following sample XML file shows the format you use to configure multihomed groups:

```
<!-- List of unmanaged connections for an Access Switch not currently modeled in
Junos Space
<MultihomedGroups>
  <MultihomedGroup Name="group1" Description="multihomed group1"
AccessSwitchIP="10.157.59.63">
    <MultihomedEndPoint PEHostName="PEHostName1" PEInterface="ge-2/0/1"
AccessSwitchInterface="ge-1/0/4"/>
    <MultihomedEndPoint PEHostName="PEHostName2" PEInterface="ge-2/0/2"
AccessSwitchInterface="ge-1/0/5"/>
  </MultihomedGroup>
  <MultihomedGroup Name="group2" Description="multihomed group2"
AccessSwitchIP="10.155.50.60">
    <MultihomedEndPoint PEHostName="PEHostName3" PEInterface="ge-2/0/1"
AccessSwitchInterface="ge-1/0/4"/>
    <MultihomedEndPoint PEHostName="PEHostName4" PEInterface="ge-2/0/2"
AccessSwitchInterface="ge-1/0/5"/>
    <MultihomedEndPoint PEHostName="PEHostName5" PEInterface="ge-3/0/2"
AccessSwitchInterface="ge-1/0/6"/>
  </MultihomedGroup>
</MultihomedGroups>
```

In the preceding sample connectivity file, the first multihomed group, *multihomed group1*, defines two PE devices in which *PEHostName1* is the primary PE device and *PEHostName2* is the backup PE device. The second multihomed group, *multihomed group2*, defines two PE devices in which *PEHostName3* is the primary PE device and *PEHostName4* and *PEHostName5* are backup PE devices.

To view a sample connectivity file for multihomed groups, see [“Viewing a Sample Connectivity File for Multihomed Groups” on page 92](#).

SEE ALSO

[Uploading a Connectivity File to Create Multihomed Groups](#) | 89

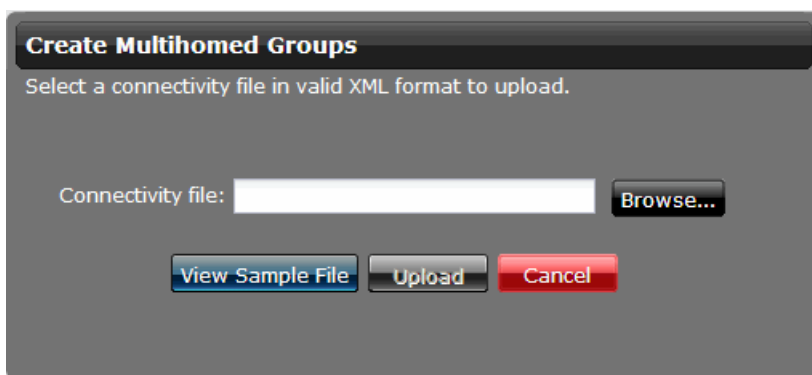
Uploading a Connectivity File to Create Multihomed Groups

To create multihomed groups, you upload the connectivity file in the Junos Space software. You create and upload a single connectivity file for all the multihomed groups you want to configure in Junos Space. To add additional multihomed groups at a later date, you can update the connectivity file and then upload the connectivity file in Junos Space again.

To upload a connectivity file and create a multihomed group:

1. In the Network Activate task pane, click **Prestage Devices > Manage Multihomed... > Create Multihomed...**

The Create Multihomed Groups screen appears.



2. To upload a Connectivity file for multihomed groups:
 - a. In the Connectivity File field, click **Browse**.
 - b. Navigate to the XML connectivity file that you want to use to create the multihomed group.
 - c. Click **Upload**.
 - d. (Optional) To view job status information, click the Job ID.
 - e. Click **OK** to upload the connectivity file in Junos Space.

SEE ALSO

| [Deleting Multihomed Groups](#) | 90

RELATED DOCUMENTATION

[Viewing Multihomed Groups | 90](#)

[Deleting Multihomed Groups | 90](#)

[Multihomed Groups Overview | 83](#)

Deleting Multihomed Groups

You can delete a multihomed group if it is not being used in a service.

To delete a multihomed group from the database:

1. In the **Network Activate** task pane, select **Prestage Devices > Manage Multihomed Groups**.
2. In the **Manage Multihomed Groups** inventory page, select the multihomed group(s) you want to delete.
3. Open the **Actions** menu and select **Delete Multihomed Group**.
A pop-up window appears requesting confirmation.
4. Click **Delete**.

The **Manage Multihomed Groups** page reappears, which confirms that the multihomed groups were deleted.

RELATED DOCUMENTATION

[Viewing Multihomed Groups | 90](#)

[Multihomed Groups Overview | 83](#)

Viewing Multihomed Groups

You can view multihomed groups and the PE devices included in each multihomed group.

1. [Viewing Multihomed Groups | 90](#)

Viewing Multihomed Groups

To view multihomed groups:

1. In the **Network Activate** task pane, select **Prestage Devices > Manage Multihomed Groups**.

The Manage Multihomed Groups page appears.

Name	Devices	Description
Test5	junos-mx80-1-space junos-mx80-2-space junos-m10-1-space	finance-west

Page 1 of 1 | Displaying 1 - 1 of 1 | Show 30 items

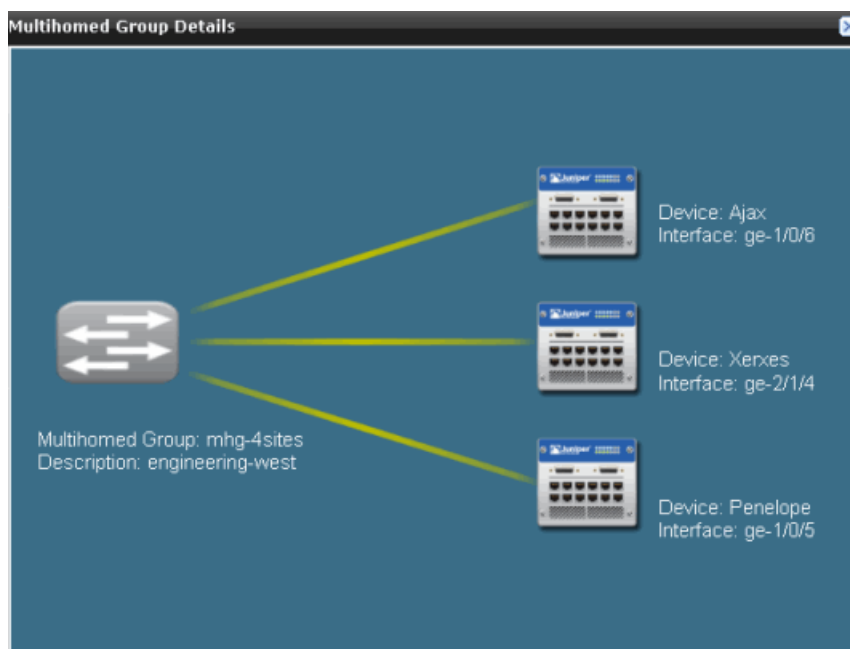
2. The following multihomed group information appears in the main display area:

- Name—The name assigned to the multihomed group
- Device—The name of the PE device in multihomed group

3. Double-click a multihomed group to view additional details.

The detailed view provides the following information:

- Multihomed Group—The name assigned to the multihomed group
- Description—A description for the multihomed group
- Device—The name of the PE device in multihomed group
- Interface—The UNI on the PE device in multihomed group



RELATED DOCUMENTATION

[Creating a Multihomed Group | 87](#)

[Deleting Multihomed Groups | 90](#)

[Multihomed Groups Overview | 83](#)

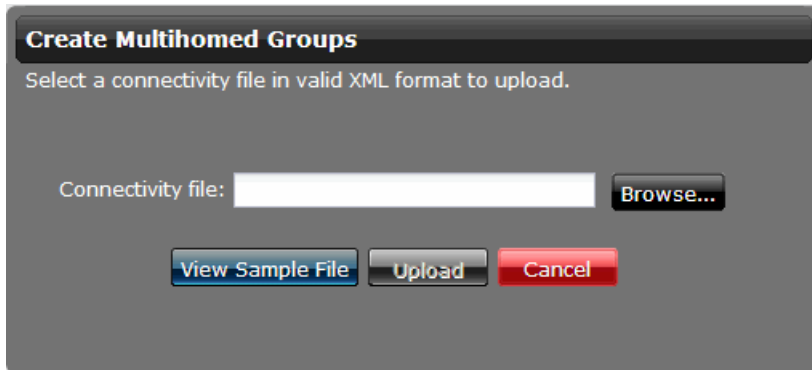
Viewing a Sample Connectivity File for Multihomed Groups

You create and upload a single connectivity file for all the multihomed groups you want to configure in Junos Space. You can view a sample connectivity file that shows the file format and required elements for creating one or more multihomed groups.

To view a sample connectivity file for multihomed groups:

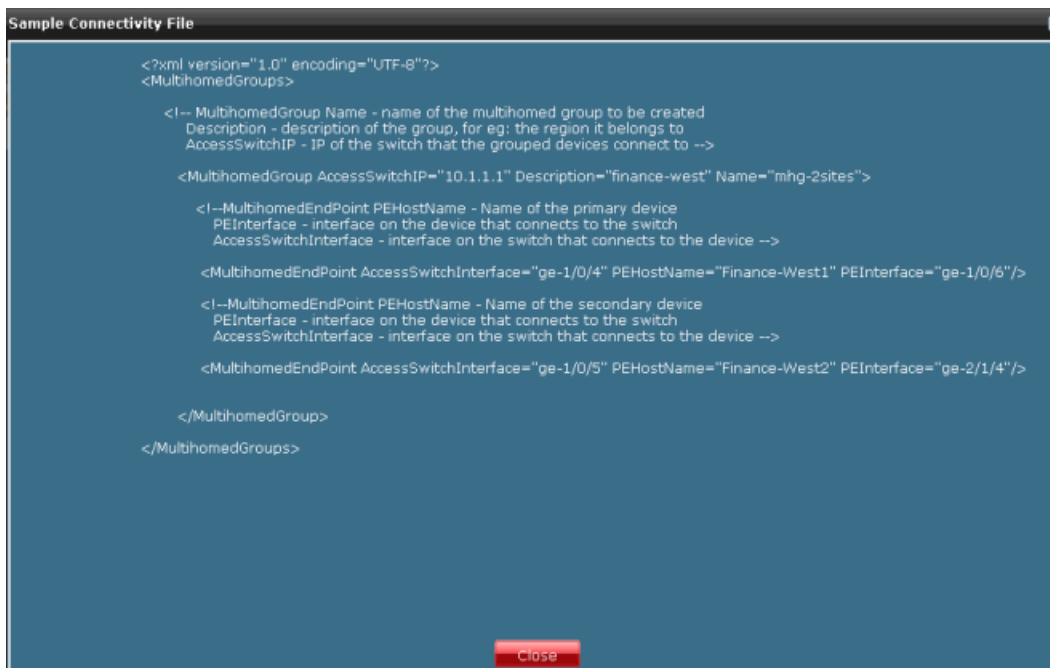
1. In the **Network Activate** task pane, select **Prestage Devices > Manage Multihomed Groups > Create Multihomed Groups**.

The **Create Multihomed Groups** window appears.



2. Click **View Sample File**.

A sample connectivity file appears.



3. Click **Close** to close the sample file and return to the **Create Multihomed Groups** window.

RELATED DOCUMENTATION

[Creating a Multihomed Group | 87](#)

[Viewing Multihomed Groups | 90](#)

[Deleting Multihomed Groups | 90](#)

[Multihomed Groups Overview | 83](#)

Prestage Services

IN THIS CHAPTER

- [Service Recovery Overview | 94](#)
- [Performing a Service Recovery Request | 94](#)
- [Viewing Service Recovery Report | 100](#)

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 Network Activate application supports Service Recovery for point-to-point services, VPLS services, and Layer 3 VPN services.

RELATED DOCUMENTATION

| [Performing a Service Recovery Request | 94](#)

Performing a Service Recovery Request

The Service Recovery feature functions within the pre-staging operation of the Network Activate application. Service Recovery has two parts.

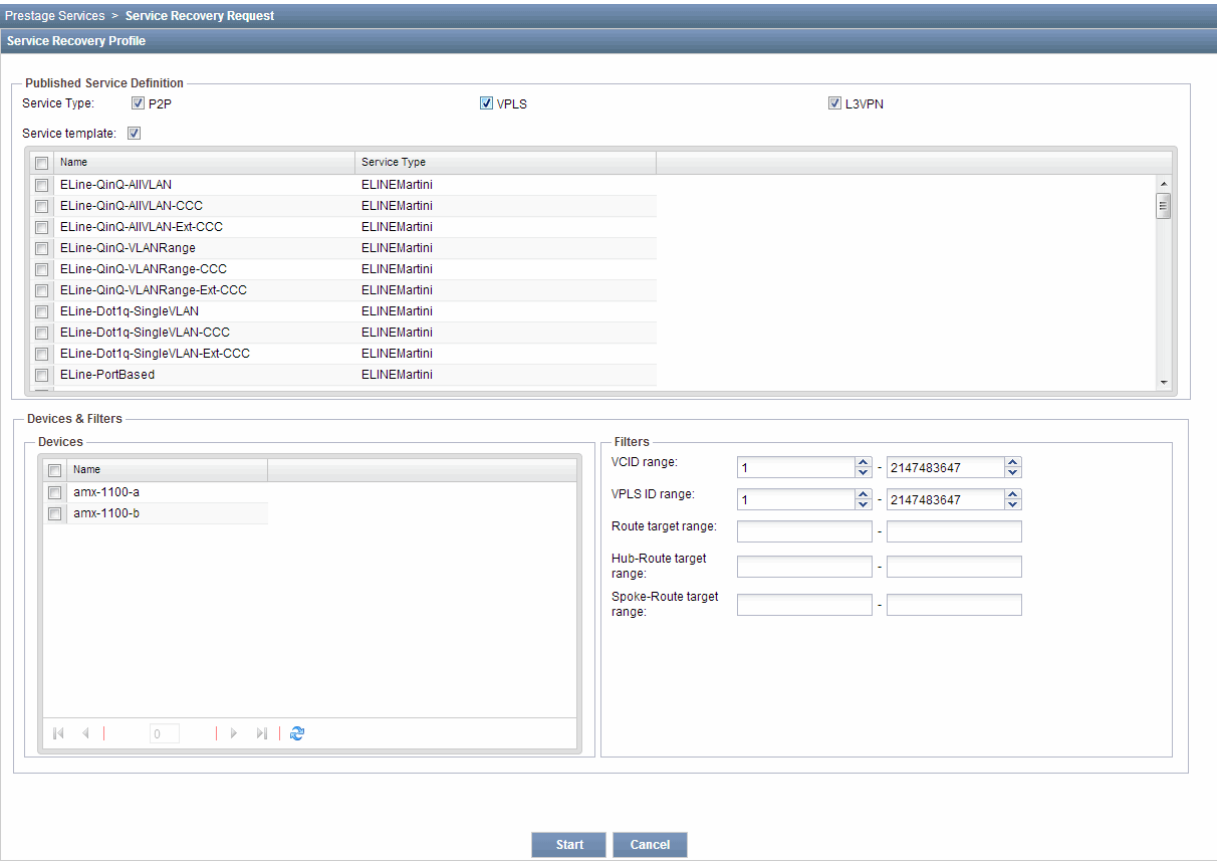
First, Service Recovery parses each device's configuration searching for service configurations and existing Network Activate service elements (P2P services, Layer 2 circuits, routing instances, firewalls, policy options, routing options, and OAM interface branches of Junos Space configurations that 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.

To perform Service Recovery, in the Network Activate task pane, select **Prestage Services > Service Recovery Request**. Initially, Service Recovery generates the following Alert message, which describes the process you are about to start and recommends saving previously recovered services.



The **Service Recovery Profile** window displays two panels, **Published Service Definition** and **Devices & Filters**.



In the **Published Service Definition** panel, you can select one or more service types: P2P, VPLS, and L3VPN.

The **Published Service Definition** panel also presents a table that lists the names of all services of the selected **Service Type**.

The **Devices & Filters** panel lists devices in the **Name** column. You can specify a **VCID Range** and **Route target range** to complete the definition of the service recovery profile search.

To recover services:

1. Fill in the fields as described in the following table.

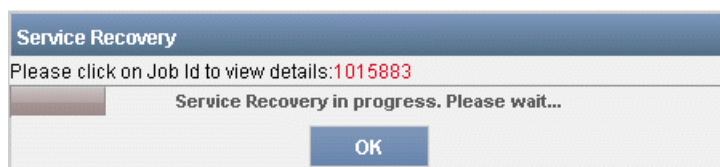
Field	Action
Published Service Definition	
Service Type	<p>Select the service type check boxes based on the service to recover:</p> <ul style="list-style-type: none"> • P2P • VPLS • L3VPN
Service template	<p>Select this check box to retrieve service templates attributes attached to the service. Junos Space supports the templates of the following MPLS VPN-related applications:</p> <ul style="list-style-type: none"> • CoS • IPsec • Stateful firewall
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>
Devices & Filters	
Devices	Select the devices whose services you want to recover
VCID Range	<p>This field is displayed if you have selected the P2P check box.</p> <p>Specify the VCID range within which services are to be recovered.</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	<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: <l2vpn-id:as-number:2-byte-number>. For example, 100:200. The AS number can be in the range from 1 through 65,535. • IPv4 format—<l2vpn-id:ip-address:2-byte-number>. For example, l2vpn-id:10.1.1.1:2. 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>

Field	Action
VPLS ID range	<p>This field is displayed if you have selected the VPLS check box.</p> <p>Specify the VPLS ID range.</p> <p>Range: 1 through 2147483647</p>
Hub-Route target range	<p>This field is displayed if you have selected the VPLS or L3VPN check boxes.</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: <l2vpn-id:as-number:2-byte-number>. For example, 100:200. The AS number can be in the range from 1 through 65,535. IPv4 format—<l2vpn-id:ip-address:2-byte-number>. For example, l2vpn-id:10.1.1.1:2. 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 the VPLS or L3VPN check boxes.</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: <l2vpn-id:as-number:2-byte-number>. For example, 100:200. The AS number can be in the range from 1 through 65,535. IPv4 format—<l2vpn-id:ip-address:2-byte-number>. For example, l2vpn-id:10.1.1.1:2. 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, click **Start**.

The Network Activate application fetches the latest device configuration. It then processes the device configuration to derive the configuration of selected service types.

The **Service Recovery in progress...** window appears, which indicates the progress of the search.



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.
- In case of a multihoming group for BGP-based VPLS service, the service recovery request recovers a multihoming BGP-based VPLS service regardless of the availability of a multihoming group. You must create a multihoming group before service recovery is performed.

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

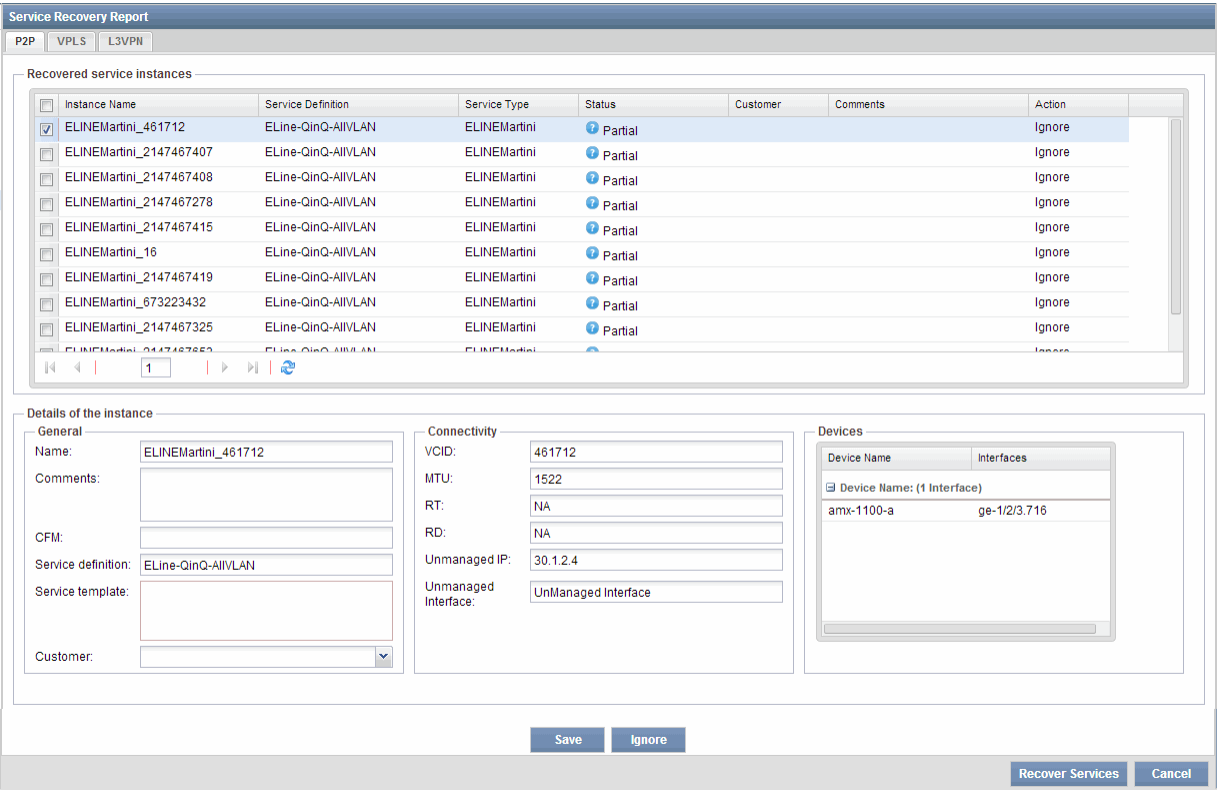
[Service Recovery Overview](#) | 94

[Viewing Service Recovery Report](#) | 100

Viewing Service Recovery Report

When the service recovery operation completes, the **Service Recovery Report** window appears.

The **Service Recovery Report** window displays the recovered services according to service type. The service recovery report for each service is displayed in different tabs.



The **Service Recovery Report** window includes several panels that provide details about the recovered services: **Recovered service instances**, **Details of the instance (General, Connectivity, Devices)**.

The **Details of the Instance** panel displays information about a service selected in the **Recovered service instances** panel. You can modify the information, and click **Save** to save the modification.

The **Devices** panel lists the endpoints associated with the service instance.

Column	Description
Recovered service instances —Lists the recovered service instances based on the tab you have selected.	
Instance Name	Name of the recovered service instance.
Service Definition	Name of the service definition attached to a service.

Column	Description
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.
Action	<ul style="list-style-type: none"> • Ignore • Recover

Details of the instance—The fields in this section differ for each service.

General

Name	Name of the selected service instance
Comments	Comments to describe the service.
CFM	Connectivity Fault Management This field is displayed in the P2P tab and the VPLS tab.
Service definition	Name of the service definition with which the instance is associated
Service template	Name of the service template with which the instance is associated
Customer	Customer for which the service is created

Connectivity

VCID	Virtual channel identifier number This field is displayed in the P2P tab only.
MTU	Maximum transmission unit number This field is displayed in the P2P tab and the VPLS tab.
RT	Route target

Column	Description
RD	Route distinguisher
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 in the P2P tab 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 in the P2P tab only.</p>
VPLS ID	<p>VPLS ID of the recovered service</p> <p>This field is displayed in the VPLS tab only.</p>
L2VPN ID	<p>Layer 2 VPN ID of the recovered service</p> <p>This field is displayed in the VPLS tab only.</p>
Hub RT	<p>Route target of the hub.</p> <p>This field is displayed only in the VPLS tab and the L3VPN tab.</p>
Spoke RT	<p>Route target of the spoke.</p> <p>This field is displayed only in the VPLS tab and the L3VPN tab.</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 in the L3VPN tab only.</p>
Routing Protocol	<p>Provider edge (PE) and customer edge (CE) routing protocol configured for the service.</p> <p>This field is displayed in the L3VPN tab only.</p>

Column	Description
Select Hub	Hub device for the hub-and-spoke Layer 3 VPN service. This field is displayed in the L3VPN tab only. This is applicable for hub-and-spoke Layer 3 VPN service only.
Devices	
Device Name	Name of the device on which the service instance was recovered.
Interfaces	The interfaces on the device on which the service instance was recovered.

To view or modify a recovered service:

1. In the **Recovered service instances** panel, select a service.

The **Details of the Instance** panel displays information about a service selected in the **Recovered service instances** panel.

2. View the information of a recovered service in the **Details of the Instance** panel. Click **Ignore** to close the Service Recovery Report window.
3. If required, modify the fields in the **Details of the Instance** panel.
4. Click **Save** to save the modification.

The **Recovered Services Status** 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 **Recovered Services Status** 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.

If you click **Cancel**, the Network Activate application displays the **Manage Service Orders** window.

NOTE: You can access the **Recovered Service Status** window whenever you want to attempt to recover additional services.

RELATED DOCUMENTATION

[Service Recovery Overview](#) | 94

[Performing a Service Recovery Request](#) | 94

Managing IP addresses

IN THIS CHAPTER

- [Creating an IP Address Pool | 106](#)
- [Managing IPv4 Addresses for Layer 3 VPNs | 108](#)
- [Specifying IPv4 Addressing Assignment in Layer 3 VPN Service Definitions | 110](#)

Creating an IP Address Pool

You, the Service Designer, can create consistent IP address pools for Layer 3 VPNs from **Prestage Devices > Manage IP Addresses > Create IP Address Pools**. 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 > Manage IP Addresses** inventory page. See [“Managing IPv4 Addresses for Layer 3 VPNs” on page 108](#)

NOTE: Preferably, create all IPv4 address pools at the beginning of the pre-staging process (see [“Prestaging Devices Overview” on page 36](#)), before you run Role Discovery (see [“Discovering and Assigning All N-PE Devices” on page 68](#)), 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 Activate** task pane, select **Navigate to Prestage Devices > Manage IP Addresses > Create IP Address Pools**.

The **Create IP Address Pool** window appears.

2. In the **IP pool type** drop-down list box, select 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.

3. In the **Pool name** field, enter a unique name.

An IP address **Pool name** can be no more than 50 characters.

4. In the **Pool description** field, enter a helpful description.

The **Pool Description** can be no longer than 200 characters.

5. 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.

6. 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 1056](#).

7. Click **Create**.

Junos Space saves the IP address pool information in the database. The IP address pool appears in the **Manage IP Address** 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 Network Activate software for Layer 3 VPN services.

RELATED DOCUMENTATION

| [Managing IPv4 Addresses for Layer 3 VPNs | 108](#)

Managing IPv4 Addresses for Layer 3 VPNs

You, the Service Designer, can specify the IPv4 IP addressing to include in Layer 3 VPN service definitions. Use the Prestage Devices > Managing IP Addresses inventory page to view existing IP Address pools that you created globally or for specific existing customers. For more information about creating an IPv4 IP address pool, see [“Creating an IP Address Pool” on page 106](#).

Viewing IP Address Pools

The **Manage IP Addresses** inventory page lists pool information in a table by name, pool type, and IP address pool.

Viewing Detail IP Address Pool Information

To view IP address details double-click an IP address pool row.

[Table 4 on page 108](#) defines the IP address pool detailed information.

Table 4: IP Address Pool Details

Detail	Description
Pool Name	<p>The mnemonic name of the IP Address pool you create using Prestage Devices > Create IP Addresses.</p> <p>An IP address Pool Name can be no more than 50 characters.</p>
Pool Description	<p>An optional description of the IP address pool name.</p> <p>The Pool Description can be no longer than 200 characters.</p>

Table 4: IP Address Pool Details (*continued*)

Detail	Description
Pool Type	<p>Either:</p> <ul style="list-style-type: none"> • 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. Addresses from global pools can be allocated across multiple L3VPNs, across multiple customers. • Customer: Pools of IPv4 addresses pertaining to a particular customer. These pools will be 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 L3VPNs, for a particular customer.
IP Address Pool	A block of IPv4 addresses in CIDR notation (for example, 10.0.77.0/24 which identifies a pool of 256 IPv4 addresses, 192.168.0.0/16, and so forth).
Customer	The existing customer name for which you created the IP address pool.

Performing Actions

You can perform the following actions on IP address pools.

- **Delete Address Pool**—Removes the selected IP address pool from the Junos Space database. Junos Space will not allow you to delete an IP address pool if it contains any addresses that are still in use.
- **Tag It**—See *Viewing Tags for a Managed Object*.
- **View Tags**—*Viewing Tags for a Managed Object*
- **Untag It**—*Untagging Objects*

RELATED DOCUMENTATION

[Creating an IP Address Pool](#) | 106

[Creating a Tag](#)

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 Network Activate 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** drop-down list box, 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 **Size of address block** 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 a Full Mesh Layer 3 VPN Service Definition](#) | 376

10

CHAPTER

Service Templates

[Service Templates Overview | 113](#)

[Service Templates Workflow | 114](#)

[Applying a Service Template to a Service Definition | 115](#)

[Creating a Service Template | 116](#)

[Deleting a Service Template | 120](#)

[Exporting a Service Template | 121](#)

[Finding Configuration Options | 122](#)

[Importing a Service Template | 125](#)

[Modifying a Service Template | 127](#)

[Specifying Service-Specific Values | 128](#)

[User Privileges in Service Templates | 138](#)

[Provisioning Dynamic Attributes to Specify the Device XPath | 139](#)

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 Activate. 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 Activate 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 Activate.

RELATED DOCUMENTATION

[Service Templates Workflow | 114](#)

[Creating a Service Template | 116](#)

[Specifying Service-Specific Values | 128](#)

[Modifying a Service Template | 127](#)

[Deleting a Service Template | 120](#)

[Importing a Service Template | 125](#)

[Exporting a Service Template | 121](#)

[Creating a Service Order Based on a Service Definition with a Template | 756](#)

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 138](#)).

The service designer's role in the service template workflow covers the following tasks:

1. [Creating a Service Template on page 116](#)
2. [Finding Configuration Options on page 122](#)
3. [Specifying Service-Specific Values on page 128](#)
4. [Applying a Service Template to a Service Definition on page 115](#)
5. [Modifying a Service Template on page 127](#)
6. [Deleting a Service Template on page 120](#)
7. [Exporting a Service Template on page 121](#)
8. [Importing a Service Template on page 125](#)
9. [Viewing Service Template Inventory on page 1047](#)

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 756](#) covers service template handling within a service order.

RELATED DOCUMENTATION

| [Service Templates Overview](#) | 113

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.

The screenshot shows the 'Create P2P Service Definition' window. The breadcrumb path is 'Service Design > Manage Service Definitions > Create P2P Service Definition'. The 'General' tab is active. The 'Name' field is empty. The 'Service type' is 'Point-to-Point Pseudowire'. The 'Signaling' dropdown is set to 'LDP'. The 'Comments' field is empty. The 'Interface type' is 'Ethernet' (selected with a radio button). Other interface options are 'TDM' and 'ATM'. There are checkboxes for 'Enable QoS' (checked), 'Static pseudowire' (unchecked), 'Enable PW access to L3 VPN network' (unchecked), and 'Enable PW Resiliency' (unchecked). The 'Service Template' dropdown is set to 'Please select ...'. At the bottom, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

To apply a service template to a service definition:

1. Create or import a service template. See [“Creating a Service Template” on page 116](#) or [“Importing a Service Template” on page 125](#).
2. In the Network Activate task 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 dropdown list for Service Template Definition, select the desired template(s).

The list of templates available is filtered according to the type of service definition.

5. For instructions on filling in the rest of the fields on this page and completing the definition, see [“Creating an E-Line Service Definition” on page 188](#), [“Creating a Multipoint-to-Multipoint VPLS Service Definition” on page 214](#), [“Creating a Point-to-Multipoint VPLS Service Definition” on page 237](#), or [“Creating a Full Mesh Layer 3 VPN Service Definition” on page 376](#).

RELATED DOCUMENTATION

[Service Templates Overview | 113](#)

[Service Templates Workflow | 114](#)

[Viewing Service Template Inventory | 1047](#)

[Service Troubleshooting Overview | 875](#)

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 128](#).

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 128](#) lists the available variables and their types.

1. [Naming a Template and Selecting Configuration Options | 116](#)
2. [Configuration Options, Their Data Types and the Tabs Displayed | 119](#)

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 122](#).
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 5 on page 119](#) lists the possible data types of the configuration options, and the tabs associated with each type.

Table 5: 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 128](#).

SEE ALSO

[Service Templates Overview | 113](#)[Service Templates Workflow | 114](#)[Specifying Service-Specific Values | 128](#)[Modifying a Service Template | 127](#)[Deleting a Service Template | 120](#)[Importing a Service Template | 125](#)[Exporting a Service Template | 121](#)[Creating a Service Order Based on a Service Definition with a Template | 756](#)

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 terminate deletion, click **Cancel**.

The **Manage Service Templates** page appears, displaying all the templates.

RELATED DOCUMENTATION

[Modifying a Service Template | 127](#)

[Importing a Service Template | 125](#)

[Exporting a Service Template | 121](#)

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

[Importing a Service Template | 125](#)

[Service Templates Overview | 113](#)

[Service Templates Workflow | 114](#)

[Creating a Service Template | 116](#)

[Specifying Service-Specific Values | 128](#)

[Modifying a Service Template | 127](#)

[Deleting a Service Template | 120](#)

[Creating a Service Order Based on a Service Definition with a Template | 756](#)

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.

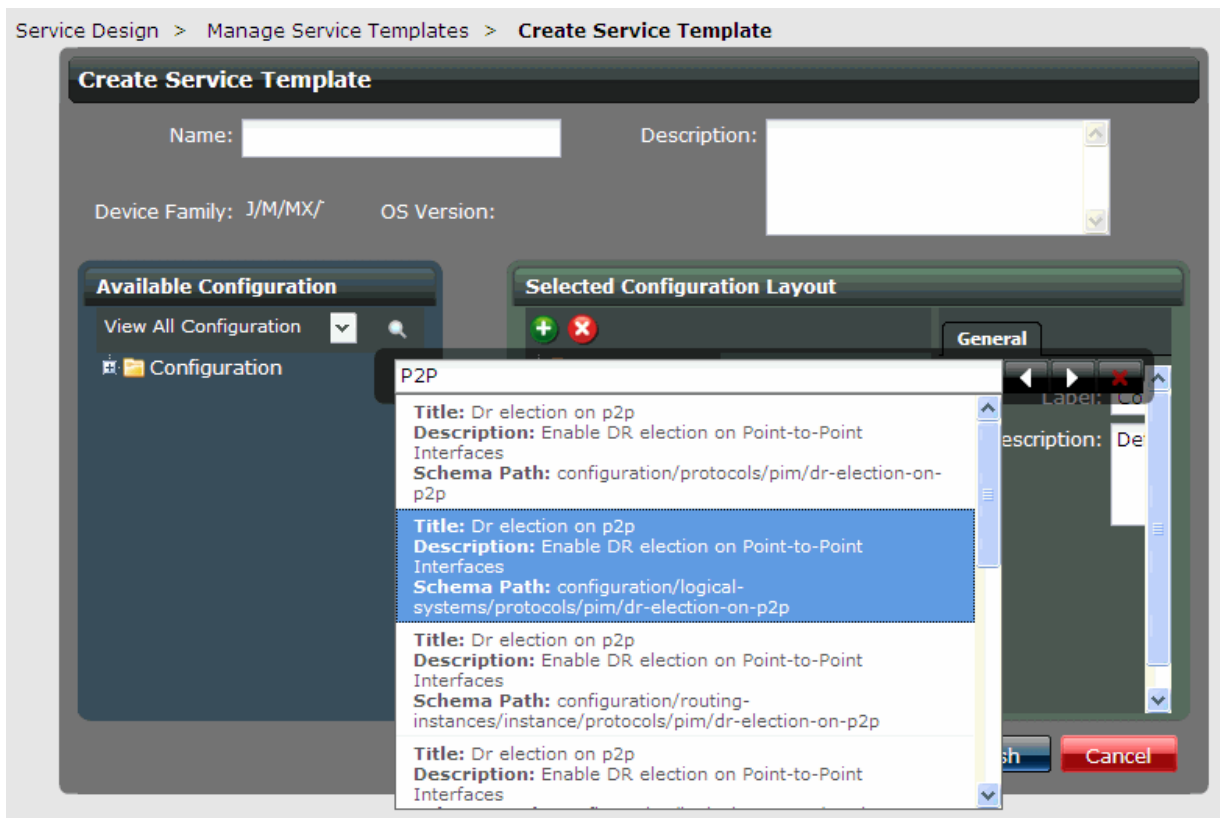
2. Enter your search term.

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.

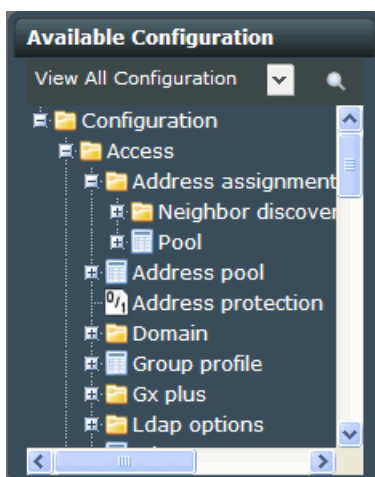
4. (Optional) To review the results that you did not select, either:

- 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 resulted 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.



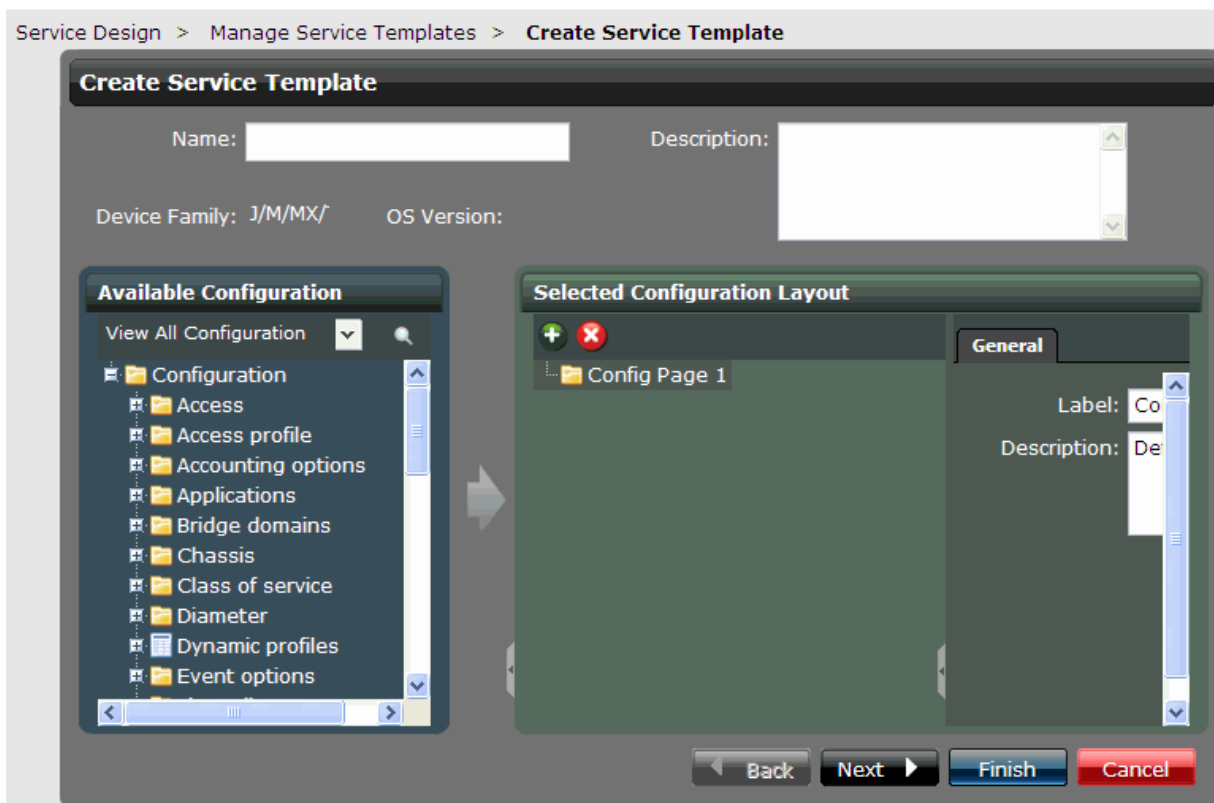
Service Perspective: The configuration parameters are grouped service wise. In the Network Activate application you can choose either of the following service perspectives:

- 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

[Creating a Service Template](#) | 116

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	 113
Service Templates Workflow	 114
Creating a Service Template	 116
Specifying Service-Specific Values	 128
Modifying a Service Template	 127
Deleting a Service Template	 120
Exporting a Service Template	 121
Creating a Service Order Based on a Service Definition with a Template	 756

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 116](#).
6. Specify service-specific data with service variables as required. For instructions on this, see [“Specifying Service-Specific Values” on page 128](#).
7. To finish modifying the template, click **Finish**.

RELATED DOCUMENTATION

Deleting a Service Template 120
Importing a Service Template 125
Exporting a Service Template 121
Service Templates Overview 113
Service Templates Workflow 114
Creating a Service Template 116

Specifying Service-Specific Values

Using service-specific variables, you can specify values that Network Activate 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 6: Service Definition Types and Associated Service Variables

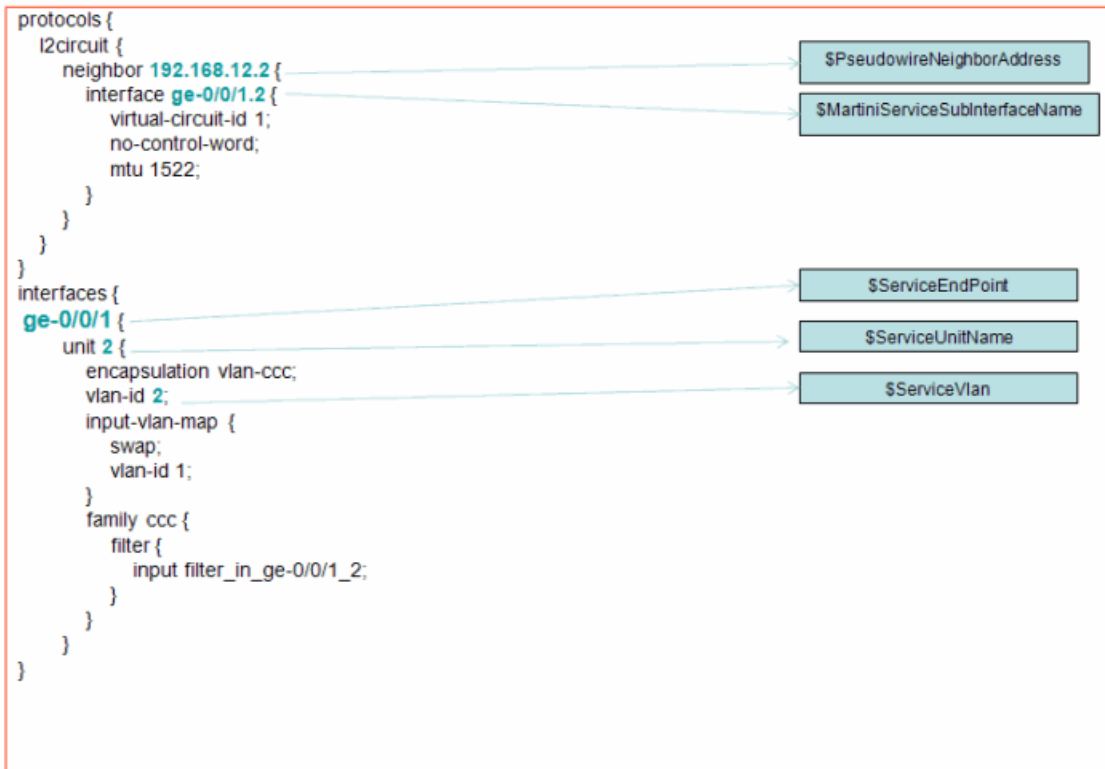
Point-to-Point	VPLS	L3VPN
\$CustomerName	\$CustomerName	\$CustomerName
-	-	\$PEIPAddress
\$PseudowireNeighborAddress	-	-
-	\$RoutingInstanceName	\$RoutingInstanceName
-	-	\$ServiceBGPGroupName
-	-	\$ServiceBGPNeighbor
\$ServiceDefinition	\$ServiceDefinition	\$ServiceDefinition
\$ServiceEndPoint	\$ServiceEndPoint	\$ServiceEndPoint
-	-	\$ServiceOSPFArea
-	-	\$ServiceOSPFIntfName
\$ServiceSubInterfaceName	\$ServiceSubInterfaceName	\$ServiceSubInterfaceName

Table 6: Service Definition Types and Associated Service Variables (*continued*)

Point-to-Point	VPLS	L3VPN
\$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 2: Point-to-Point Example: Device Configuration Deployed Through Network Activate



```

protocols {
  l2circuit {
    local-switching {
      interface ge-0/1/0.2 {
        end-interface {
          interface ge-0/2/3.4;
        }
      }
    }
  }
}

```

Diagram illustrating the configuration for a point-to-point example, showing the mapping of configuration elements to variables:

- `interface ge-0/2/3.4` maps to `$MartiniServiceLocalSwitchInterfaceName`.

Figure 3: VPLS Example: Device Configuration Deployed Through Network Activate

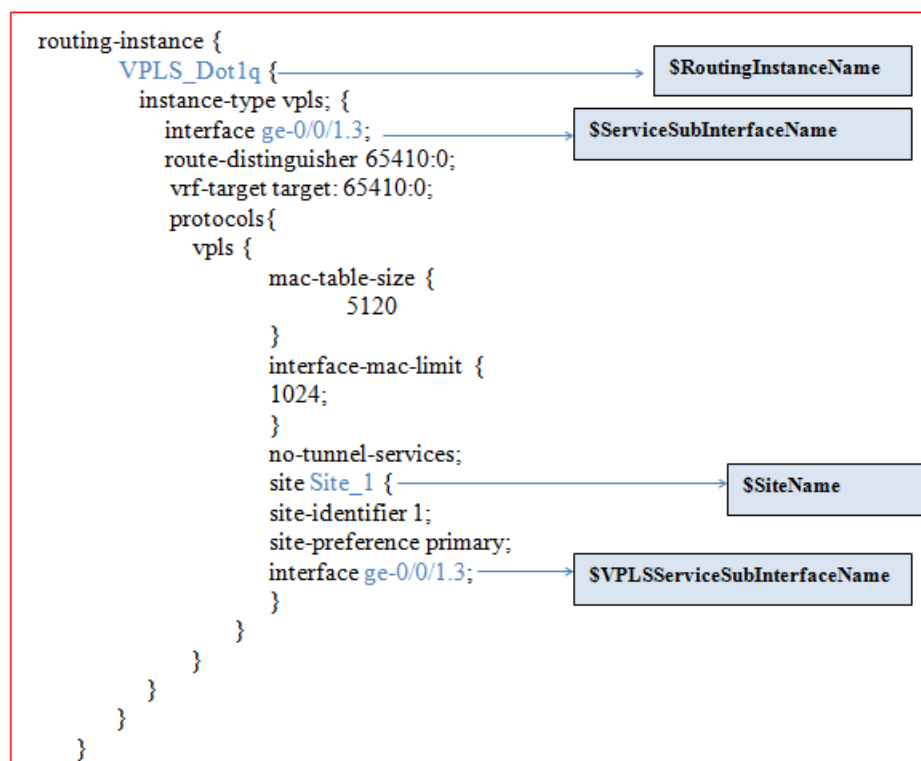


Figure 4: L3VPN Example: When OSPF Is a CE-PE Protocol

```

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 the `l3vp_ospf` routing instance, showing variable substitutions:

- `$RoutingInstanceName` points to `l3vp_ospf`.
- `$ServiceSubInterfaceName` points to `ge-0/0/1.3`.
- `$ServiceOSPFArea` points to `0.0.0.0`.
- `$ServiceOSPFIntfName` points to `ge-0/0/1.3`.

```

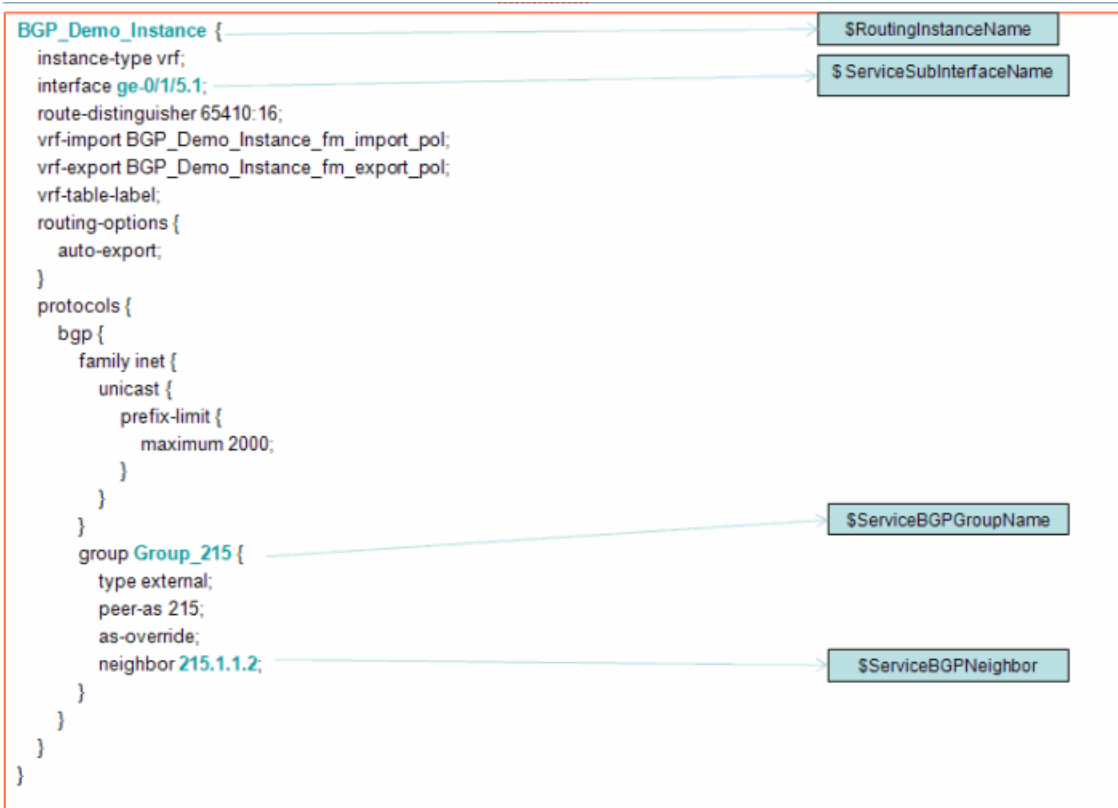
interfaces {
  ge-0/0/1 {
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation flexible-ethernet-services;
    unit 1 {
      vlan-id 1;
      family inet {
        address 1.1.1.1/32;
      }
    }
  }
}

```

Diagram illustrating the configuration for the `ge-0/0/1` interface, showing variable substitutions:

- `$ServiceEndPoint` points to `ge-0/0/1`.
- `$ServiceUnitName` points to `unit 1`.
- `$ServiceVlan` points to `1`.
- `$PEIPAddress` points to `1.1.1.1/32`.

Figure 5: 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)	
junos-m10-1-space	ge-0/0/1
Device: junos-m10-2-space (1 Item)	
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

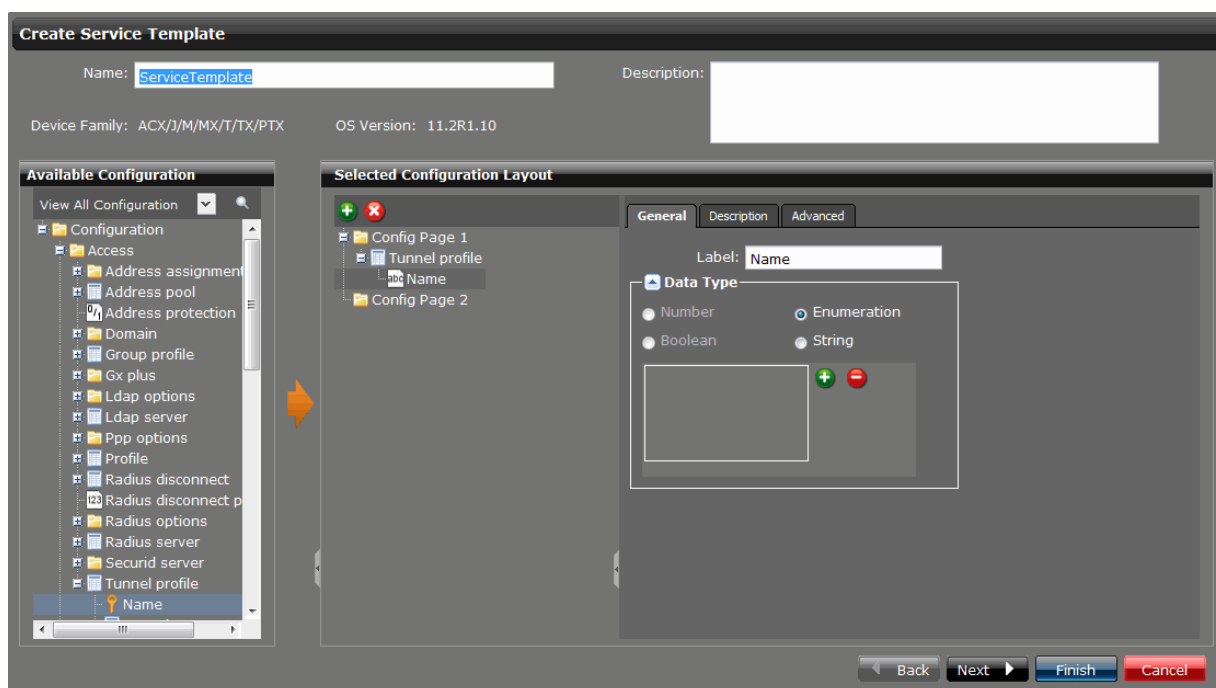
OSPF area ID: 0.0.0.0

OK

To specify service specific values in a template:

1. In the Network Activate task pane, select **Network Activate > 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 116](#)).
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 116](#).

- 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 Activate 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 115.

RELATED DOCUMENTATION

[Service Templates Overview](#) | 113

[Service Templates Workflow](#) | 114

[Creating a Service Template](#) | 116

[Modifying a Service Template](#) | 127

[Importing a Service Template](#) | 125

[Exporting a Service Template](#) | 121

[Creating a Service Order Based on a Service Definition with a Template](#) | 756

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

[Service Templates Workflow](#) | 114

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. Select **Service Design > Manage Service Templates > Create Dynamic Attributes**.

The Create Dynamic Attributes window appears.

Dynamic		XPath
Outer	<input checked="" type="checkbox"/>	/device/configuration/interfaces/interface/unit/name
Inner choices	<input checked="" type="checkbox"/>	/device/configuration/routing-instances/instance/vlan-tags/inner
Description	<input type="checkbox"/>	

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**.

While creating a service order, when you click the **Flexible Service Attribute** link, the dynamic service attributes lists the values from a specific device.

RELATED DOCUMENTATION

[Configuring Flexible Service Attributes to Modify Service Template Attributes | 938](#)

[Creating a Point-to-Point ATM or TDM Pseudowire Service Order | 578](#)

[Creating a Point-to-Point Service Order | 586](#)

[Creating a Multipoint-to-Multipoint VPLS Service Order | 660](#)

[Creating a Point-to-Multipoint VPLS Service Order | 678](#)

[Creating a Full Mesh Layer 3 VPN Ethernet Service Order | 718](#)

[Creating a Hub-and-Spoke Layer 3 VPN Service Order | 733](#)

11

CHAPTER

Layer 2 Services

[Junos Space Layer 2 Services Overview | 142](#)

[Service Attributes Overview | 152](#)

[Redundant Pseudowires for Layer 2 Circuits and VPLS | 165](#)

[VPLS over GRE Overview | 166](#)

[Multichassis Link Aggregation Group Overview | 168](#)

[Multi-Chassis Automatic Protection Switching Overview | 169](#)

Junos Space Layer 2 Services Overview

Junos Space Network Activate software 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 Network Activate software 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 (dot1.q)—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 7 on page 142](#) provides a guide to selecting the appropriate type of Layer 2 service for a specific customer need.

Table 7: 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
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 Network Activate software enables you to provision a range of services from the following service families for your enterprise customers:

- [Point-to-Point Services on page 143](#)
- [VPLS Services on page 147](#)

Point-to-Point Services

IN THIS SECTION

- [Port-to-Port Service | 143](#)
- [Single VLAN Service Using 802.1Q Interfaces | 144](#)
- [All Traffic Service Using Q-in-Q Interface | 145](#)
- [Range of VLANs Service with Q-in-Q Interfaces | 145](#)

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

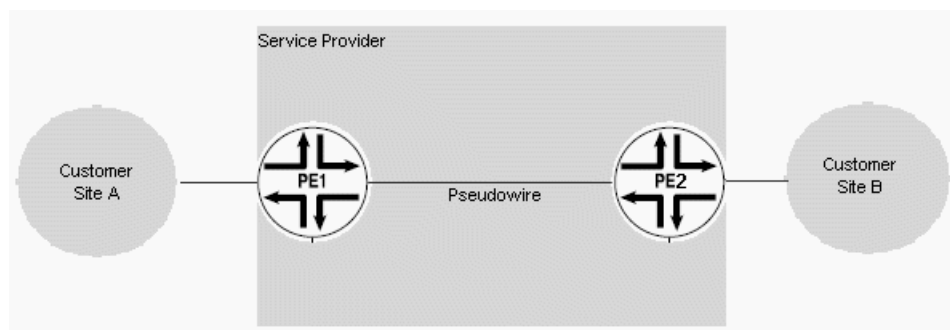
A port-to-port service transports all traffic on a port on a provider edge (N-PE) router across the network to a port of another N-PE router. enterprise customers needs to purchase only a single physical port for

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 144](#) 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

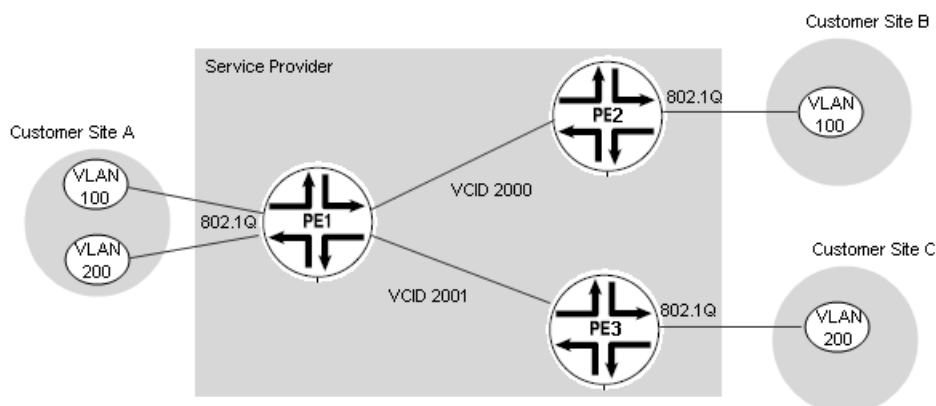


Single VLAN Service Using 802.1Q Interfaces

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 145](#). 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

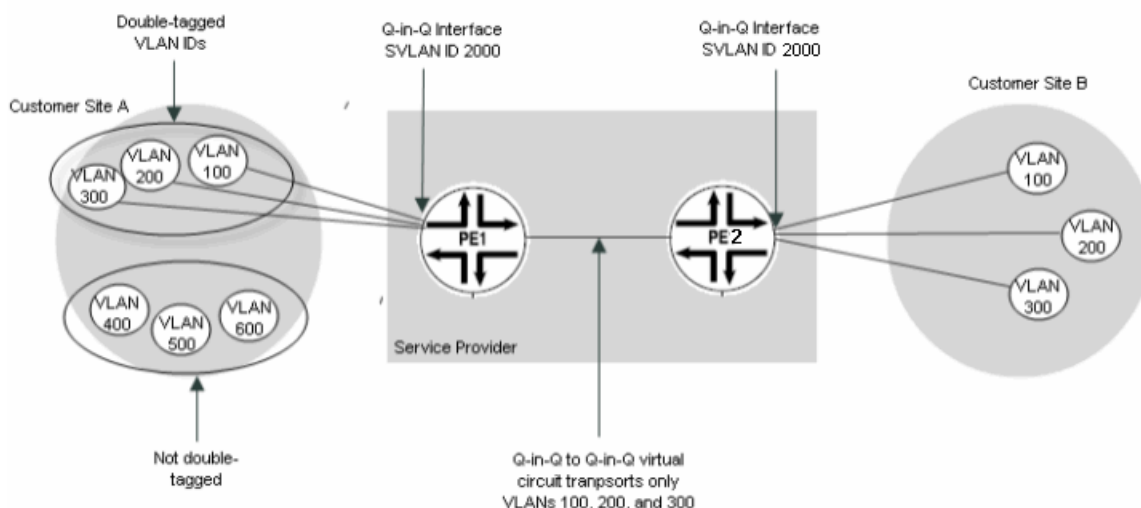
This type of point-to-point Ethernet (LDP) service uses Q-in-Q interfaces and transports all customer traffic from one site to another across the network. The Q-in-Q interface adds a service provider tag to the frame, which isolates the enterprise customer's VLAN tags. The service provider does not need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

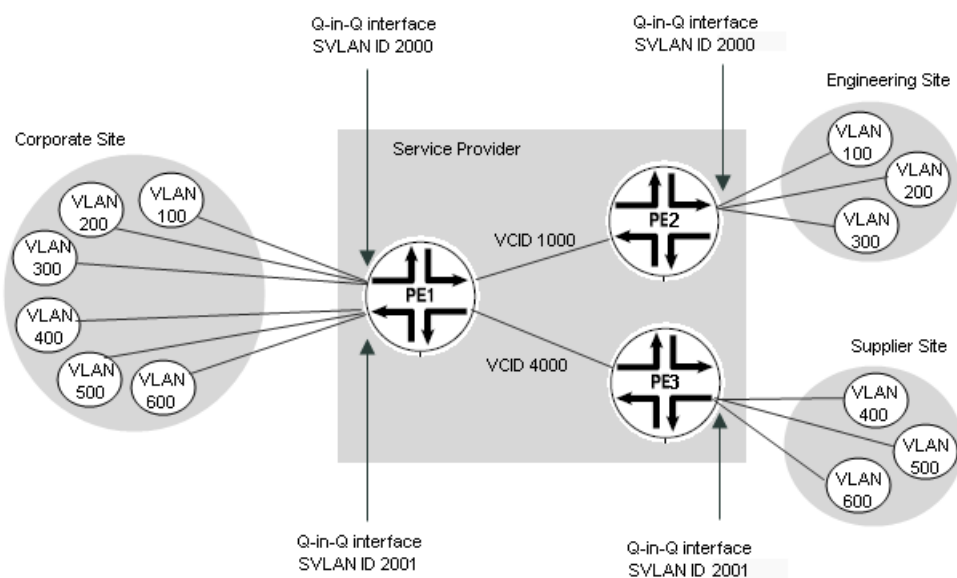
[Figure 8 on page 146](#) shows an example in which an enterprise customer has six VLANs with VLAN IDs 100, 200, 300, 400, 500, and 600. The service is provisioned to carry only VLANs 100, 200, and 300 by tagging them with the service provider VLAN ID of 2000. VLANs 400, 500, and 600 do not cross the 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 146](#).

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



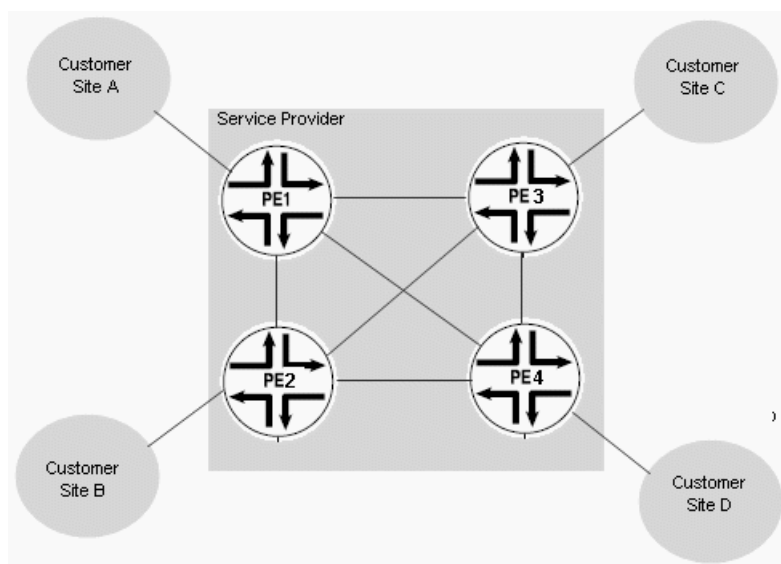
VPLS Services

The Network Activate software 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 147](#) shows an example of a multipoint service connecting four customer sites.

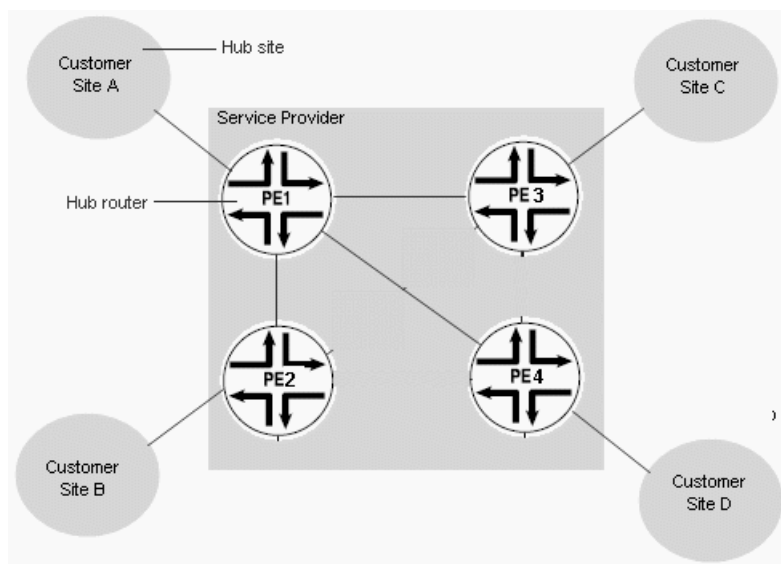
Figure 10: Multipoint-to-Multipoint VPLS Service—Full Mesh



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 148](#) 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.

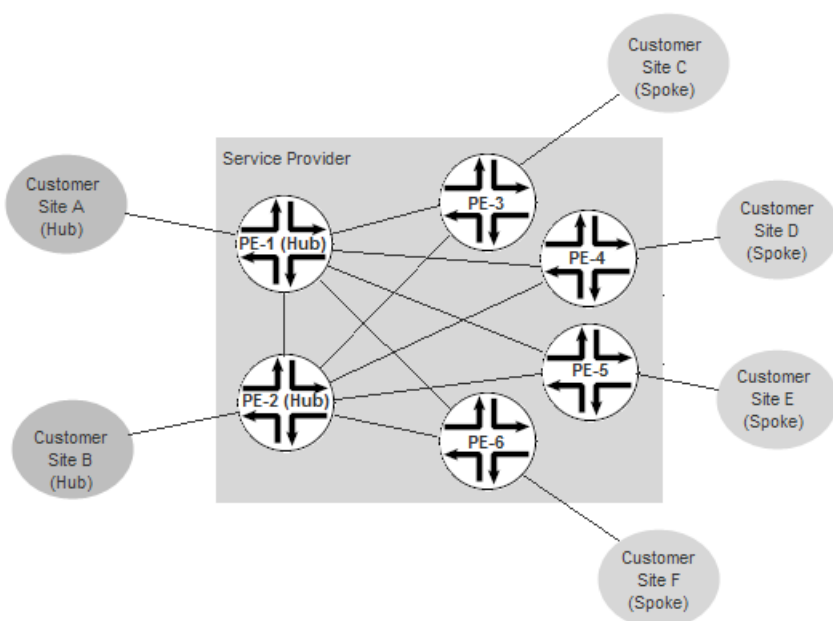
Figure 11: Point-to-Multipoint VPLS Service with Single Hub



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 148](#) 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.

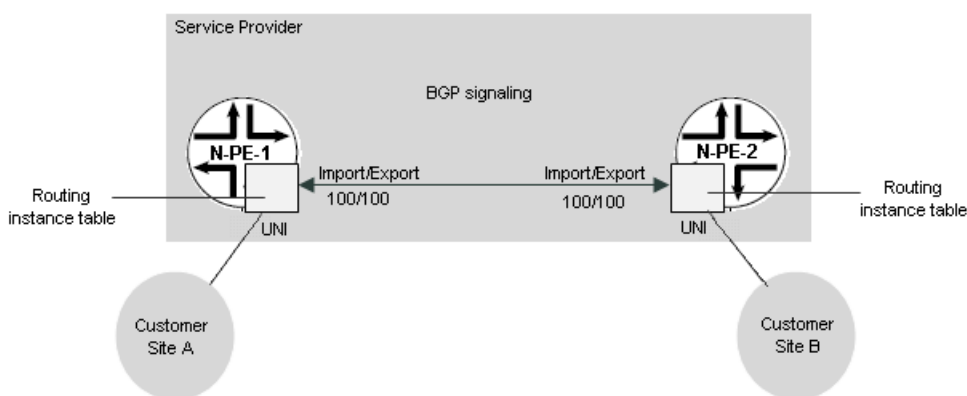
For all VPLS topologies, route targets and route distinguishers designate the multipoint connectivity among the participating endpoints.

Service Autodiscovery

BGP uses autodiscovery to establish connectivity among the N-PE routers quickly and efficiently.

[Figure 13 on page 149](#) shows an example.

Figure 13: Autodiscovery of Service Connectivity

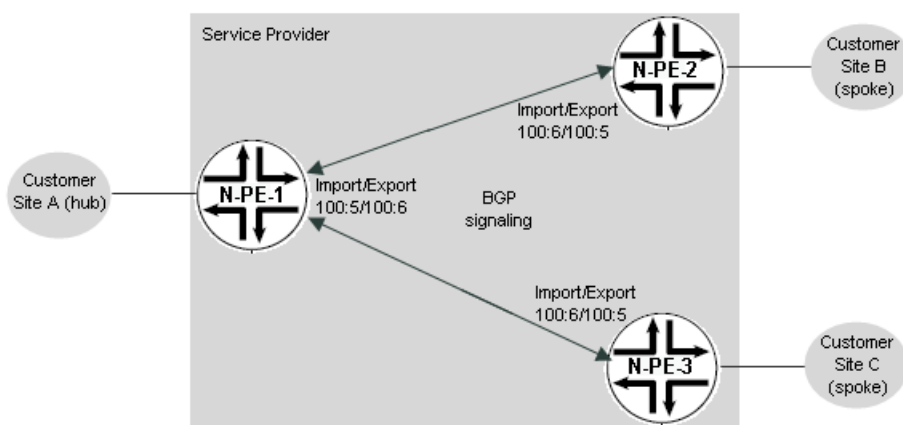


In this example, device N-PE-1 is the first to be added to the service. It exports route target 100 and imports route target 100. When N-PE-2 is added to the service, it also exports and imports route target 100. The Junos OS on the device automatically makes the association and creates the connectivity 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 150](#) 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 Network Activate software 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 710](#).

- 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 710](#).

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 211](#)

RELATED DOCUMENTATION

[Service Attributes Overview](#) | 152

[Provisioning Process Overview](#) | 176

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 Network Activate 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

IN THIS SECTION

- [Service Type | 153](#)
- [Signaling | 153](#)
- [Signaling | 153](#)
- [Signaling | 153](#)
- [Signaling | 153](#)
- [Enabling Additional Features | 154](#)

●	Customer 154
●	Enable QoS 154

The following general attributes are defined for each service:

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.

Signaling

The **Comments** attribute .

Signaling

The **Service Template** attribute .

Signaling

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 not configurable in the service order.

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

UNI Settings

IN THIS SECTION

- [Ethernet Options | 155](#)
- [Interface | 156](#)
- [MTU | 156](#)
- [Customer Traffic Type | 156](#)
- [Customer VLAN ID | 156](#)
- [Service VLAN ID and VLAN ID Range | 157](#)
- [Physical Encapsulation | 157](#)
- [Logical Encapsulation | 158](#)
- [Rate Limiting and Bandwidth | 158](#)
- [UNI Settings for TDM Interfaces | 159](#)
- [UNI Settings for ATM Interfaces | 159](#)

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

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 Network Activate 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 Network Activate 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 Network Activate 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 Network Activate 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 8 on page 158](#) defines the logical encapsulation types that are valid for each physical encapsulation type in a point-to-point Ethernet service.

Table 8: 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 9 on page 158](#) defines the logical encapsulation types that are valid for each physical encapsulation type in multipoint Ethernet services.

Table 9: 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 cannot 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
 - BX7000 Gateway: 2K through 32K
- **Idle pattern**—0 through 255
- **Excessive packet loss rate**—1 through 100%
- **Payload size**
 - M Series: 64 through 1024
 - BX7000 Gateway: 24 through 1440

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

IN THIS SECTION

- [Virtual Private LAN Service Identifier \(VPLS ID\) | 160](#)
- [Auto Discovery | 160](#)
- [Virtual Circuit Identifier \(VCID\) \(Point-to-Point Services Only\) | 160](#)
- [Route Targets and Route Distinguishers | 160](#)
- [Normalized VLAN \(Multipoint Services Only\) | 161](#)
- [Multihoming | 162](#)
- [MAC Learning | 162](#)

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

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 Network Activate software 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 710](#).
- **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 710](#).
- **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 Network Activate software manipulates VLANs, see [“Understanding VLAN Manipulation \(Normalization and VLAN Mapping\) on Ethernet Services”](#) on page 710.

Multihoming

You can enable multihoming to connect a customer site to multiple PE devices to provide redundant connectivity while preventing the formation of Layer 2 loops in the service provider’s network. A VPLS site that is multihomed to multiple PE devices provides redundant connectivity in the event of a PE device to CE device link failure or the failure of a PE device.

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

IN THIS SECTION

- [Tunnel Services | 163](#)
- [Local Switching | 163](#)
- [Fast Reroute Priority | 163](#)
- [Label Block Size | 164](#)
- [Connectivity Type | 164](#)

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

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.

RELATED DOCUMENTATION

Redundant Pseudowires for Layer 2 Circuits and VPLS

IN THIS SECTION

- [Types of Redundant Pseudowire Configurations | 165](#)
- [Pseudowire Failure Detection | 166](#)

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

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 an E-Line Service Definition | 188](#)

[Creating a Multipoint-to-Multipoint VPLS Service Definition | 214](#)

[Creating a Point-to-Multipoint VPLS Service Definition | 237](#)

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 GRE Definition

Creating a GRE Service Order

Multichassis Link Aggregation Group Overview

Multi-chassis link aggregation group (MC-LAG), is a type of LAG with constituent ports that terminate on separate chassis, thereby providing node-level redundancy. MC-LAG adds node-level redundancy to the normal link-level redundancy that a LAG provides. This allows two or more nodes to share a common LAG endpoint. The multiple nodes present a single logical LAG to the remote end.

The MC-LAG enables a client device to form a logical LAG interface between two MC-LAG peers. An MC-LAG provides redundancy and load balancing between the two MC-LAG peers, multi-homing support, and a loop-free Layer 2 network without running the Spanning Tree Protocol (STP). It is an HA solution involving multiple protocols: LACP, ICCP, VRRP, BFD, SNOOPING

On one end of an MC-LAG, there is an MC-LAG client device, such as a server, that has one or more physical links in a link aggregation group. This client device does not need to have an MC-LAG configured. On the other side of the MC-LAG, there are two MC-LAG peers. Each of the MC-LAG peers has one or more physical links connected to a single client device.

The MC-LAG peers use the Inter-chassis Control Protocol (ICCP) to exchange control information and coordinate with each other to ensure that data traffic is forwarded properly. ICCP runs over TCP and is monitored by Bidirectional Forwarding Detection (BFD). It requires an Inter-Chassis link (ICL) for L2 connectivity.

Following are the two types of MC-LAG:

- **Active-Active Mode**—In active-active mode, all member links are active on the MC-LAG. In this mode, MAC addresses learned on one MC-LAG peer are propagated to the other MC-LAG peer. Active-active mode is the only mode supported at this time.
- **Active-Standby Mode**—In active-standby mode, one node is active at any given time. In this mode, the MC-LAG peers act as virtual routers. The virtual routers share the virtual IP address that corresponds to the default route configured on the host or server connected to the MC-LAG.

You can configure MC-LAG in the following scenarios:

- MC-LAG with multi-segmented point-to-point service in Active-Standby mode
- MC-LAG with point-to-point service in Active-Standby mode
- MC-LAG with multi-segmented Layer 3 VPN in Active-Standby mode

RELATED DOCUMENTATION

[Creating a Point-to-Point Service Order | 586](#)

[Creating a Full Mesh Layer 3 VPN Ethernet Service Order | 718](#)

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 Order](#) | 578

12

CHAPTER

Layer 3 Services

[Junos Space Layer 3 Services Overview | 171](#)

[Multicast L3VPN Overview | 173](#)

Junos Space Layer 3 Services Overview

IN THIS SECTION

- [Overview | 171](#)
- [Layer 3 VPN Platform Support | 172](#)
- [Layer 3 VPN Attributes | 172](#)
- [Device Configuration for a Layer 3 VPN | 172](#)

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

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 Network Activate software 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

Network Activate software 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

[Creating a Full Mesh Layer 3 VPN Service Definition | 376](#)

[Creating a Full Mesh Layer 3 VPN Ethernet Service Order | 718](#)

Multicast L3VPN Overview

The Junos Space Network Activate 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. Network Activate 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 Network Activate 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, Network Activate 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.

RELATED DOCUMENTATION

[Creating a Multicast VPN Service Definition | 404](#)

[Creating a Multicast VPN Service Order | 748](#)

13

CHAPTER

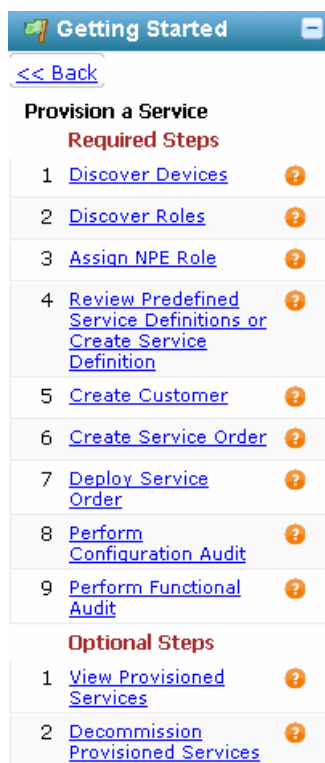
Service Provisioning

Provisioning Process Overview | **176**

Provisioning Process Overview

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

The Getting Started panel in the Junos Space user interface provides 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 following example shows the Service Provisioning assistant in the Getting Started panel:



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 pre-staging actions including discovering and assigning device roles (steps 2 and 3).
- The Service Designer roles 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 pre-staging tasks. Pre-staging 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” on page 36](#) for more information about pre-staging devices.

Service Designer Tasks

The service designer is responsible for the service definitions that the service provisioner will use 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 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

[Discovering and Assigning All N-PE Devices | 68](#)

[Discovering and Assigning N-PE Devices with Exceptions | 71](#)

[Predefined Point-to-Point Service Definitions | 477](#)

[Predefined Multipoint-to-Multipoint Ethernet Service Definitions | 521](#)

[Predefined Point-to-Multipoint Ethernet Service Definitions | 554](#)

[Creating an E-Line Service Definition | 188](#)

[Creating a Multipoint-to-Multipoint VPLS Service Definition | 214](#)

[Creating a Point-to-Multipoint VPLS Service Definition | 237](#)

[Unpublishing a Custom Service Definition | 309](#)

[Adding a New Customer | 1056](#)

[Creating a Point-to-Point Service Order | 586](#)

[Creating a Multipoint-to-Multipoint VPLS Service Order | 660](#)

[Creating a Point-to-Multipoint VPLS Service Order | 678](#)

[Deploying a Service Order | 631](#)

[Understanding Service Validation | 875](#)

Predefined Roles Overview in the Junos Space Network Application Platform User Guide

2

PART

Service Definitions

Layer 2 Ethernet and ATM or TDM Service Definitions | **181**

VPLS Service Definitions | **311**

Layer 3 VPN Service Definitions | **376**

Predefined Service Definitions | **408**

Layer 2 Ethernet and ATM or TDM Service Definitions

IN THIS CHAPTER

- [Choosing a Predefined Service Definition or Creating a New Service Definition | 181](#)
- [Viewing Service Definitions | 267](#)
- [Creating a Point-to-Point ATM or TDM Pseudowire Service Definition | 270](#)
- [Creating an E-Line Service Definition | 279](#)
- [Creating a Cross Provisioning Platform Service Definition | 305](#)
- [Publishing a Custom Service Definition | 308](#)
- [Unpublishing a Custom Service Definition | 309](#)
- [Deleting a Customized Service Definition | 309](#)

Choosing a Predefined Service Definition or Creating a New Service Definition

The Network Activate 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.

The following topics review the predefined service definitions and provide instructions on creating your own.

- [Choosing a Predefined Service Definition | 182](#)
- [Creating an E-Line Service Definition | 188](#)
- [Creating a Multipoint-to-Multipoint VPLS Service Definition | 214](#)
- [Creating a Point-to-Multipoint VPLS Service Definition | 237](#)

Choosing a Predefined Service Definition

Table 10 on page 182 lists the predefined service definitions that Junos Space provides for Ethernet point-to-point services that use LDP in the network core. Table 11 on page 185 lists the predefined service definitions for multipoint-to-multipoint (full mesh) services. Table 12 on page 187 lists the predefined service definitions for point-to-multipoint (hub and spoke) services.

Table 10: 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

Table 10: Standard Ethernet Point-to-Point Service Definitions (*continued*)

Standard Service Definition Name	Service Attributes
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
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

Table 10: Standard Ethernet Point-to-Point Service Definitions (*continued*)

Standard Service Definition Name	Service Attributes
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
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 11: 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
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

Table 11: Standard Multipoint-to-Multipoint Service Definitions (*continued*)

Standard Service Definition Name	Service Attributes
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
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 12: 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 Activate task 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 408](#)

SEE ALSO

| [Predefined Service Definitions | 408](#)

Creating an E-Line Service Definition

Use this procedure to create a definition for an E-Line 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 E-Line 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 an E-Line service definition, complete these tasks, in the order shown:

1. [Specifying General Information | 188](#)
2. [Specifying UNI Settings | 192](#)
3. [Specifying Connectivity Information When Signaling Is LDP | 208](#)
4. [Specifying Connectivity Information When Signaling Is BGP | 211](#)

Specifying General Information

To specify the general information for an E-Line service definition:

1. In the Network Activate task pane, select **Service Design > Manage Service Definitions > Create E-Line Service Definition**. The **General** settings window appears.

General

Name: LDP-Service-Definition

Service type: Point-to-Point Pseudowire

Signaling: LDP

Comments:

Service Template: Flexi_Temp× Flexi_Temp_Inner_Outer× × ▾

Default Service Template: Flexi_Temp× Flexi_Temp_Inner_Outer× × ▾

Threshold alarm profile: Please select ... ▾

☒ Enable QoS

Interface type: ☒ Ethernet

☐ TDM
 ☐ ATM
 ☐ Static pseudowire
 ☐ Enable PW access to L3 VPN network
 ☐ Enable Multi Segment Pseudowire
 ☐ Enable PW Resiliency
 ☐ Decouple Service Status From Port Status

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 E-Line .
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>

Field	Action
Comments (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 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>
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>

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 E-Line 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 E-Line pseudowire stitching, see “Stitching Two Point-to-Point Pseudowires” on page 645.</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 165.</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, not the jnxVpnIfVpn traps.</p>

Field	Action
Service Template	<p>(Optional) To include a service template for the service, select a service template from the Service Template list.</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 116.</p>

3. Click **Next** to save the information. Continue with [“Specifying UNI Settings” on page 192](#).

SEE ALSO

[Service Templates Overview | 113](#)

[Creating a Service Template | 116](#)

[Importing a Service Template | 125](#)

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 | 193](#)

- [Specifying UNI Settings for Services with 802.1Q Interface Types | 196](#)

- Specifying UNI Settings for Services with Q-in-Q Interface Types | 201
- UNI Settings for Services with Flexible VLAN Tagging (Asymmetric Interface Types) | 204

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.

UNI Settings

▲ Traffic Treatment

Ethernet option:

port-port

Customer traffic type:

N/A

VLAN ID selection:

N/A

☐ Editable in Service Order

VLAN range for auto-pick:

VLAN range for manual input:

Outer Tag protocol ID:

Please select ...

☐ Editable in Service Order

Inner Tag protocol ID:

Please select ...

☐ Editable in Service Order

▲ Interface Settings

Physical IF encapsulation:

ethernet-ccc

Logical IF encapsulation:

N/A

▲ MTU Settings

Default MTU (Bytes):

1522

☐ Editable in Service Order

MTU range (Bytes):

1522

9192

▲ Bandwidth Settings

☒ Enable rate limiting

Default bandwidth (Mbps):

10

☐ Editable in Service Order

Min Bandwidth (Kbps):

1000

Max Bandwidth (Mbps):

100

Increment (Kbps):

1000

▲ Calculation of Burst-Size

Calculate Burst Size:

MTU Based

MTU Factor:

10

☐ Editable in Service Order

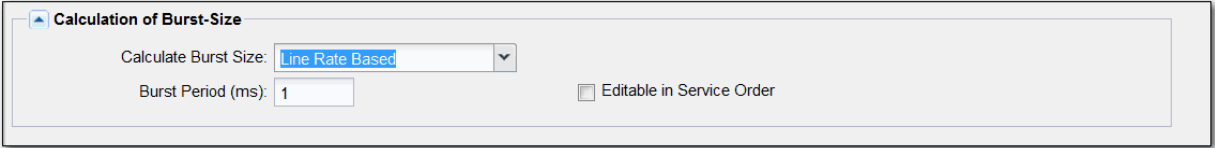
2. Fill in the fields in the **UNI Settings** window according to the following table.

Field	Action
Traffic Treatment Settings	
<hr/>	

Field	Action
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	

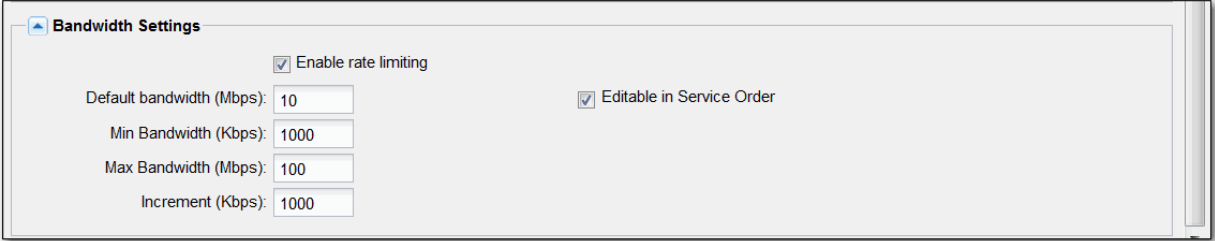
Field	Action
Calculate Burst Size	<p>Select the preferred option for calculating the burst size:</p> <ul style="list-style-type: none">• MTU Based If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902. The default value for MTU Factor is 1.• Line Rate 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 checkbox.</p>

The following illustration shows the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.



Bandwidth Settings

The following illustration shows the Bandwidth Settings panel, which appears if you do not select the **Enable QoS** check box in the preceding **General** settings window.



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>

Field	Action
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 13: 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.							

3. 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.

1. Enter information in the UNI Settings window.

UNI Settings

▲

Traffic Treatment

Ethernet option:

dot1q

▼

Customer traffic type:

Transport single vlan

▼

VLAN ID selection:

Auto pick

▼

VLAN range for auto-pick:

10

1000

VLAN range for manual input:

Outer Tag protocol ID:

0x88a8

✕

▼

Inner Tag protocol ID:

Please select ...

▼

☐

Editable in Service Order

☐

Editable in Service Order

☐

Editable in Service Order

▲

Interface Settings

Physical IF encapsulation:

flexible-ethernet-services

▼

Logical IF encapsulation:

vlan-ccc

▼

▲

MTU Settings

Default MTU (Bytes):

1522

9192

MTU range (Bytes):

1522

9192

☐

Editable in Service Order

▲

Calculation of Burst-Size

Calculate Burst Size:

MTU Based

▼

MTU Factor:

1

☐

Editable in Service Order

2. 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 Ethernet option you choose determines the other options you can select and specify on the page.

Field	Action
Customer traffic type	<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 ID selection	<p>Indicate how the VLAN ID is determined:</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.</p>
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</pre> <pre>set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x88a8</pre> <pre>set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x8100</pre>
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>
----------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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

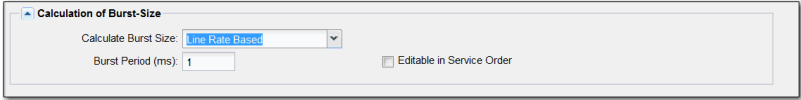
Specify the default bandwidth value, in Mbps.

Default: 10 Mbps

Range: 1 Mbps through 100,000 Mbps

Calculate Burst Size	<p>Select the preferred option for calculating the burst size:</p> <ul style="list-style-type: none"> MTU Based <p>If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902.</p> <p>The default value for MTU Factor is 1.</p> Line Rate Based <p>If you select the option Line Rate Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds.</p> <p>The default value for Burst Period is 1.</p> <p>NOTE: The Calculate Burst Size list is enabled only when you select the Enable rate limiting checkbox.</p>
-----------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The following illustration shows the appearance of the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.



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:

UNI Settings

▲ Traffic Treatment

Ethernet option:

qinq

Customer traffic type:

Transport vlan range

VLAN ID selection:

Select manually

10

1000

VLAN range for auto-pick:

VLAN range for manual input:

Outer Tag protocol ID:

0x88a8

✕ ▾

Editable in Service Order

Inner Tag protocol ID:

0x8100

✕ ▾

Editable in Service Order

▲ Interface Settings

Physical IF encapsulation:

flexible-ethernet-services

Logical IF encapsulation:

vlan-ccc

▲ MTU Settings

Default MTU (Bytes):

1522

Editable in Service Order

MTU range (Bytes):

1522

9192

▲ Calculation of Burst-Size

Calculate Burst Size:

MTU Based

MTU Factor:

1

Editable in Service Order

- 2. Fill in the fields in the **UNI Settings** window according to the following table:

Field	Action
Traffic Treatment Settings	
Ethernet option	Select qinq from the list. The window expands to include options specific to Q-in-Q interfaces.

Field	Action
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>
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</pre> <pre>set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x88a8</pre> <pre>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	

Field	Action
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 <p>If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902.</p> <p>The default value for MTU Factor is 1.</p> Line Rate Based <p>If you select the option Line Rate Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds.</p> <p>The default value for Burst Period is 1.</p> <p>NOTE: The Calculate Burst Size list is enabled only when you select the Enable rate limiting checkbox.</p>
-----------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The following illustration shows the appearance of the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.

The screenshot shows a panel titled "Calculation of Burst-Size". Inside the panel, there is a label "Calculate Burst Size:" followed by a dropdown menu with "Line Rate Based" selected. Below this, there is a label "Burst Period (ms):" followed by a text input field containing the value "1". To the right of the input field is a checkbox labeled "Editable in Service Order", which is currently unchecked.

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.

UNI Settings

⌵ Traffic Treatment

Ethernet option:

asymmetric tag depth

Customer traffic type:

Transport all traffic

VLAN ID selection:

Select manually

☐ Editable in Service Order

VLAN range for auto-pick:

236

1024

VLAN range for manual input:

1310

2609

Outer Tag protocol ID:

Please select ...

☐ Editable in Service Order

Inner Tag protocol ID:

☐ Editable in Service Order

⌵ Interface Settings

Physical IF encapsulation:

vlan-ccc

Logical IF encapsulation:

vlan-ccc

⌵ MTU Settings

Default MTU (Bytes):

1522

☐ Editable in Service Order

MTU range (Bytes):

1522

9192

⌵ Calculation of Burst-Size

Calculate Burst Size:

MTU Based

MTU Factor:

1

☐ Editable in Service Order

2. Specify the UNI Settings for asymmetric tag depth according to the following table:

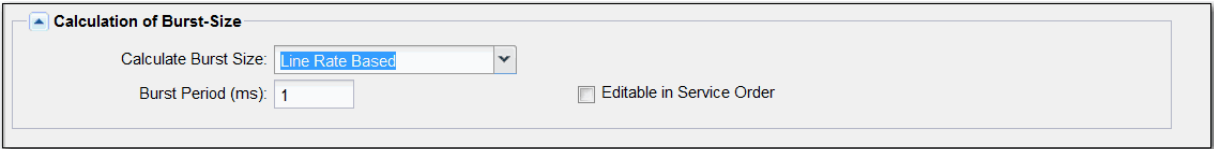
Field	Action
Traffic Treatment Settings	
Ethernet option	Select asymmetric tag depth from the list.
Customer traffic type	<div>Select the customer traffic type:</div> <ul style="list-style-type: none">● Transport all traffic—Transports the traffic from all VLANs across the network. When you select this 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. 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. <div>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</div>

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>
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</pre> <pre>set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x88a8</pre> <pre>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	

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 1.• 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 checkbox.</p>

The following illustration shows the appearance of the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.



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.

To specify connectivity between sites across the network when signaling is LDP:

Connectivity

Connectivity Settings

VC ID selection:

Auto pick

Default MTU (Bytes):

1522

MTU range (Bytes):

1522

Revert time (sec):

5

Switch Over Delay (sec):

0

VLAN normalization:

Normalization not required

Outgoing label selection:

Select manually

Editable in Service Order

☒

Editable in Service Order

9192

Editable in Service Order

Editable in Service Order

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>

Field	Action
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	The options available in the VLAN normalization are based on the value set for the Ethernet interface.
Outgoing label selection	<p>This field is available if you selected the Static pseudowire check box in the General settings.</p> <p>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>
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>

Ethernet Option	Customer Traffic Type	VLAN Normalization
	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)

- 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:

The screenshot shows the 'Connectivity' window with the 'Connectivity Settings' tab selected. The settings are as follows:

- Route Distinguisher: Auto pick (dropdown)
- Route Target: Auto pick (dropdown)
- Default MTU (Bytes): 1522 (text input)
- MTU range (Bytes): 1522 (text input)
- VLAN normalization: Swap (dropdown menu is open, showing options: Swap, Normalize to None, Normalize to Dot1q tag, and Normalize to QinQ tags, with 'Normalize to QinQ tags' selected)
- Editable in Service Order (checkbox, unchecked)
- Editable in Service Order (checkbox, unchecked)
- Editable in Service Order (checkbox, unchecked)
- 9192 (text input)

- 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.

NOTE: The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to <http://www.iana.org/assignments/ipv4-address-space> for the list of restricted IPv4 addresses and <http://www.iana.org/assignments/ipv6-address-space> for the list of restricted IPv6 addresses.

- **Route Target**—Allows you to distribute VPN routes to only the routers that need them.

NOTE: The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to <http://www.iana.org/assignments/ipv4-address-space> for the list of restricted IPv4 addresses and <http://www.iana.org/assignments/ipv6-address-space> for the list of restricted IPv6 addresses.

- **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 Network Activate software manipulates VLANs, see [“Understanding VLAN Manipulation \(Normalization and VLAN Mapping\) on Ethernet Services” on page 710](#).

2. Click **Finish** to complete the service definition.

RELATED DOCUMENTATION

[Publishing a Custom Service Definition | 308](#)

[Predefined Point-to-Point Service Definitions | 477](#)

[Viewing Service Definitions | 267](#)

Creating a Multipoint-to-Multipoint VPLS Service Definition

IN THIS SECTION

- [Specifying General Information for Multipoint-to-Multipoint VPLS Service Definitions | 215](#)
- [Specifying UNI Settings for Multipoint-to-Multipoint VPLS Service Definitions | 218](#)
- [UNI Settings for Port-to-Port Interfaces in VPLS Services | 218](#)
- [UNI Settings for 802.1Q Interfaces in VPLS Services | 221](#)
- [UNI Settings for Q-in-Q Interfaces in VPLS Services | 225](#)
- [UNI Settings for Services with Flexible VLAN Tagging \(Asymmetric Interface Types\) | 229](#)
- [Specifying Connectivity and MAC Security Information | 232](#)
- [Specifying Advanced Settings | 235](#)

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

To specify the general information for a multipoint-to-multipoint service definition, in the Network Activate task pane, select **Service Design > Manage Service Definitions > Create VPLS Service Definition**

The **General** window appears.

General

Name:

Test

Service type:

Multipoint-to-Multipoint Ethernet (VPLS)

▼

Signaling:

LDP

▼

Comments:

Service Template:

Please select ...

▼

Threshold alarm profile:

Please select ...

▼

☒ Enable QoS

☐ Enable L3 Access

☒ Enable Static PW Labels

To specify the general information for a multipoint-to-multipoint service definition:

1. Fill in the fields on the **General** window.

Field	Action
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 window: <ul style="list-style-type: none"> • Route target • Route distinguisher • VLAN normalization • Allow Multihoming • Mac Security Settings • LDP—If LDP signaling is selected, the following fields are available in the Connectivity window: <ul style="list-style-type: none"> • Auto Discovery • Route target, if Auto Discovery is enabled • Route distinguisher, if Auto Discovery is enabled • VPLS ID, if Auto Discovery is disabled • 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>
Comments (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 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>
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 UNI 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>

Field	Action
Service Template	<p>(Optional) To include a service template for the service, select a service template from the Service Template list.</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 116.</p>

2. Click **Next** to save the information and continue with UNI Settings.

SEE ALSO

[Service Templates Overview | 113](#)

[Creating a Service Template | 116](#)

[Importing a Service Template | 125](#)

Specifying UNI 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 Settings for Port-to-Port Interfaces in VPLS Services

The **UNI Settings** window provides four expanding or collapsing panels: Traffic Treatment, Interface Settings, MTU Settings, and Bandwidth Settings.

The screenshot shows the 'UNI Settings' window with the following sections:

- Traffic Treatment**
 - Ethernet option: **port-port** (dropdown)
 - Customer traffic type: **N/A** (dropdown)
 - VLAN ID selection: **N/A** (dropdown)
 - ☐ Editable in Service Order
 - VLAN range for auto-pick: [] []
 - VLAN range for manual input: [] []
 - Outer Tag protocol ID: **Please select ...** (dropdown)
 - ☐ Editable in Service Order
 - Inner Tag protocol ID: **Please select ...** (dropdown)
 - ☐ Editable in Service Order
- Interface Settings**
 - Physical IF encapsulation: **ethernet-vpls** (dropdown)
 - Logical IF encapsulation: **N/A** (dropdown)
- MTU Settings**
 - Default MTU (Bytes): **1522** (input)
 - ☒ Editable in Service Order
 - MTU range (Bytes): **1522** (input) **9192** (input)
- Calculation of Burst-Size**
 - Calculate Burst Size: **MTU Based** (dropdown)
 - MTU Factor: **1** (input)
 - ☐ Editable in Service Order

To specify the UNI Settings for Port-to-Port interfaces:

1. Fill in the fields on the **UNI Settings** window.

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	To allow the service provisioner to override the MTU setting, select the check box.
Interface Settings	
Physical IF encapsulation	Select ethernet-vpls , the only valid physical interface encapsulation method allowed for port-to-port services.

Field	Action
Logical IF encapsulation	You can not select a choice in this field because it is not relevant to port-to-port services.

MTU Settings

Default MTU (Bytes)	The default MTU value is 1522 bytes.
MTU Range (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.

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 1. 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 checkbox.</p>
-----------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The following illustration shows the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.

Calculation of Burst-Size

Calculate Burst Size: Line Rate Based

Burst Period (ms):

☐ Editable in Service Order

Bandwidth Settings

Enable 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 not available in the service definition when QoS Design software is installed.</p>
-----------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Field	Action
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 14 on page 221 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

The following table lists the **Max Bandwidth (Mbps)** for the M Series, MX Series, and ACX Series Routers:

Table 14: 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 **Next** to continue with Connectivity settings.

UNI Settings for 802.1Q Interfaces in VPLS Services

To specify the UNI Settings for 802.1Q interfaces:

1. Fill in the fields on the **UNI Settings** window.

Field	Action
Traffic Treatment Settings	
Ethernet option	<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>
Customer traffic type	<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 ID selection	<p>Indicate how the VLAN ID is determined.</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.</p>
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 (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	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	<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>
Calculation of Burst-Size	

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 1. 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 checkbox.</p>

The following illustration shows the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.

Bandwidth Settings

Enable 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 not available in the service definition when QoS Design software is installed.</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>

Field	Action
Max Bandwidth (Mbps)	<p>Specify the maximum bandwidth value in Mbps. For more information on maximum bandwidth see Table 14 on page 221</p> <p>Default: 100 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps/100Gbps</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>

2. Click **Next** to continue with connectivity settings.

UNI 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 **UNI Settings** window.

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>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 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>
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 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	<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 that the service provisioner can type.</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 1. • 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 checkbox.</p>

Field	Action
-------	--------

The following illustration shows the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.

Calculation of Burst-Size

Calculate Burst Size: Line Rate Based

Burst Period (ms):

☐ Editable in Service Order

Bandwidth Settings

Enable 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 not available in the service definition when QoS Design software is installed.</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 14 on page 221</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 100000 Kbps</p>

2. 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.

To specify the UNI Settings for q-in-q interfaces:

1. Fill in the fields on the **UNI Settings** window.

Field	Action
Traffic Treatment Settings	
Ethernet option	Select asymmetric tag depth from the list.
Customer traffic type	<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>
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>
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 (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>
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	<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 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.

Field	Action
MTU Settings	<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>

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 1. 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 checkbox.</p>
-----------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The following illustration shows the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.

Calculation of Burst-Size

Calculate Burst Size: **Line Rate Based**

Burst Period (ms):

☐ Editable in Service Order

Bandwidth Settings

Enable 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 not available in the service definition when QoS Design software is installed.</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>

To specify connectivity between sites across the network:

1. Fill in the fields in the **Connectivity** window.

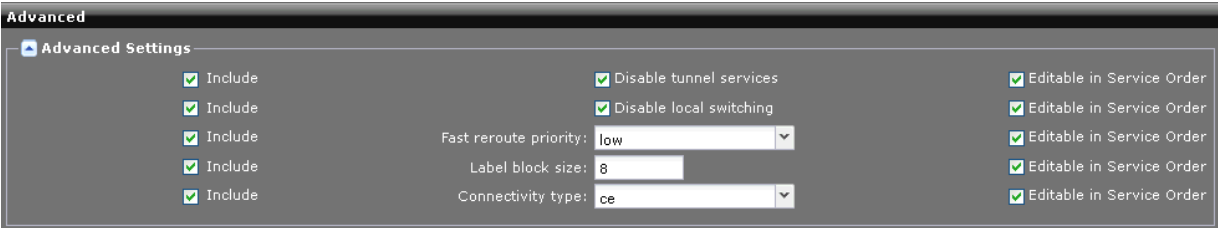
Field	Action
Route target	<p>Choose one of the following options from the list:</p> <ul style="list-style-type: none"> • Auto pick • Select manually
Route distinguisher	<p>Select a route distinguisher option:</p> <ul style="list-style-type: none"> • Select manually—The service provider specifies the route distinguisher. • Auto pick—The route distinguisher is selected automatically. <p>To override this setting in the service order, select the Editable in Service Order check box.</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. NOTE: For services that transport a range of VLAN IDs, you must set VLAN Normalization to all. You cannot transport a range of VLAN IDs without normalization. • 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 each endpoint. • 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>For more information about VLAN normalization, see “Junos Space Layer 2 Services Overview” on page 142.</p> <p>For information about VLAN manipulation, see “Understanding VLAN Manipulation (Normalization and VLAN Mapping) on Ethernet Services” on page 710.</p>
Allow Multihoming	<p>This check box is available only if the signaling type is BGP. To enable a service provisioner to define primary and backup PE devices in a multihomed group that serves as a single customer site, select Allow Multihoming.</p>

Field	Action
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 selected for 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 when the signaling type is BGP.</p> <p>If you select the Auto Discovery check box, the following fields are available:</p> <ul style="list-style-type: none"> • Route target • Route distinguisher • VPN ID <p>If you disable the Auto Discovery check box, specify the VPLS ID.</p>
VPLS 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.</p> <ul style="list-style-type: none"> • Autopick • Select manually
VPN ID	<p>This field is available only if the signaling type is LDP and auto discovery is enabled.</p> <p>Identifies the VPN ID associated with the router.</p> <ul style="list-style-type: none"> • Autopick • Select manually
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.
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>

2. Click **Next** to save the connectivity settings. [“Specifying Advanced Settings” on page 235](#)

Specifying Advanced Settings

In this step, you can specify the parameters that define advanced connectivity between sites across the service provider network. The following illustration shows the **Advanced** window.



To specify advanced settings:

1. Fill in the fields as indicated in the table.

Field	Action
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).

Field	Action
fast-reroute-priority	<p>In the fast-reroute-priority, 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 is enabled.</p>
Connectivity type	<p>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):</p> <ul style="list-style-type: none"> ● 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. <p>NOTE: This field is unavailable if the Signaling type is LDP and the Auto discovery is enabled.</p>
Editable in Service Order	<p>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.</p>

2. Click **Finish** to save the advanced settings.

The service definition is complete.

RELATED DOCUMENTATION

- [Publishing a Custom Service Definition | 308](#)
- [Predefined Multipoint-to-Multipoint Ethernet Service Definitions | 521](#)
- [Viewing Service Definitions | 267](#)
- [Creating an E-Line Service Definition | 188](#)
- [Creating a Point-to-Multipoint VPLS Service Definition | 237](#)

Creating a Point-to-Multipoint VPLS Service Definition

IN THIS SECTION

- [Specifying General Information for Point-to-Multipoint VPLS Service Definitions | 238](#)
- [Specifying UNI Settings | 242](#)
- [Specifying Connectivity and MAC Security Information | 261](#)
- [Specifying Advanced Settings | 265](#)

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

In the Network Activate task pane, select **Service Design > Manage Service Definitions > Create VPLS Service Definition**. The **General** settings window appears.

General

Name:

P-MP-VPLS-SD

Service type:

Point-to-Multipoint Ethernet (VPLS)

Signaling:

LDP

Comments:

Service Template:

Flexi_Temp_Inner_Outer×

Flexi_Temp×

×

Service_template×

Default Service Template:

Flexi_Temp_Inner_Outer×

×

Threshold alarm profile:

Please select ...

☒ Enable L3 Access

☒ Enable PW Extension

☒ Enable PW Resiliency

☒ Enable Static PW Labels

To specify the general information for a point-to-multipoint service definition:

1. Fill in the fields in the **General** window.

Field	Action
Name	Type a name for the service definition.
Service type	Select Point-to-Multipoint Ethernet (VPLS)

Field	Action
Signaling	<p>Select signaling type:</p> <ul style="list-style-type: none"> • BGP— If BGP signaling is selected, the following fields are available in the connectivity window: <ul style="list-style-type: none"> • Route target • Route distinguisher • VLAN normalization • Allow Multihoming • Mac Security Settings • VCID, if Enable PW Extension is enabled • LDP—If LDP signaling is selected, the following fields are available in the connectivity window: <ul style="list-style-type: none"> • Auto Discovery • Route target, if Auto Discovery is enabled • Route distinguisher, if Auto Discovery is enabled • VPLS ID, if Auto Discovery is disabled • VPN ID, if Auto Discovery is enabled • VLAN normalization • Mac Security Settings <p>NOTE: The Signaling is not editable in the service order.</p>
Comments (Optional)	Type a brief description or other comment that you want to appear in the Service Definition table.
Enable QoS	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.
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 UNI 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.

Field	Action
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 165.</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 checkbox enables the Enable PW Resiliency checkbox and automatically selects the Enable PW Extension checkbox.</p>
Service Template Definition	<p>(Optional) To include a service template for the service, select a service template from the Service Template list.</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 116.</p>

- Click **Next** to save the information. Continue with [“Specifying UNI Settings” on page 242](#).

SEE ALSO

[Service Templates Overview | 113](#)

[Creating a Service Template | 116](#)

[Importing a Service Template | 125](#)

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 ports, 802.1Q interfaces, or Q-in-Q interfaces:

- [Specifying UNI Settings for Port-to-Port Services | 242](#)
- [Specifying UNI Settings for Services with 802.1Q Interface Types | 246](#)
- [Specifying UNI Settings for Services with Q-in-Q Interface Types | 251](#)
- [Specifying UNI Settings for Services with Flexible VLAN Tagging \(Asymmetric Interface Types\) | 256](#)

Specifying UNI Settings for Port-to-Port Services

NOTE: You can select the port-port option only for services that are not normalized. That is, you must select **Not Normalized** when specifying the connectivity.

UNI Settings

▲ Traffic Treatment

Ethernet option:

port-port

Customer traffic type:

N/A

VLAN ID selection:

N/A

☐ Editable in Service Order

VLAN range for auto-pick:

VLAN range for manual input:

Outer Tag protocol ID:

Please select ...

☐ Editable in Service Order

Inner Tag protocol ID:

Please select ...

☐ Editable in Service Order

▲ Interface Settings

Physical IF encapsulation:

ethernet-vpls

Logical IF encapsulation:

N/A

▲ LDP PW Extension Settings

Physical IF encapsulation:

ethernet-ccc

Logical IF encapsulation:

N/A

▲ MTU Settings

Default MTU (Bytes):

1522

☐ Editable in Service Order

MTU range (Bytes):

1522

9192

▲ Calculation of Burst-Size

To set UNI attributes for port UNIs:

1. Fill in the fields as indicated in the table.

Field	Action
Traffic Treatment Settings	

Field	Action
Ethernet option	<p>Select port-port from the drop-down 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	The VLAN ID cannot be selected. 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 MTU setting, select the check box.

Interface Settings

Physical IF encapsulation	<p>In the Physical IF encapsulation box, select ethernet-vpls, which is the only valid physical interface encapsulation method for port-to-port services.</p> <p>The Logical IF encapsulation field cannot be selected because it is not relevant to port-to-port services.</p>
Logical IF encapsulation	You cannot select a choice in this field because it is not relevant to port-to-port services.

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 window.

Physical IF 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 IF encapsulation	You can not select a choice in this field because it is not relevant to port-to-port services.
MTU Settings	In the MTU range boxes, type the lowest and highest values for MTU that the service provisioner can type.

Calculation of Burst-Size

Field	Action
Calculate Burst Size	<p>Select the preferred option for calculating the burst size:</p> <ul style="list-style-type: none"> MTU Based <p>If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902.</p> <p>The default value for MTU Factor is 1.</p> Line Rate Based <p>If you select the option Line Rate Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds.</p> <p>The default value for Burst Period is 1.</p> <p>NOTE: The Calculate Burst Size list is enabled only when you select the Enable rate limiting checkbox.</p>

The following illustration shows the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.

Bandwidth Settings

The following illustration shows the **Bandwidth Settings** panel, which appears if you do not select the **Enable QoS** check box in the preceding **General** settings window.

Enable 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 not available in the service definition when QoS Design software is installed.</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 15 on page 245 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

The following table lists the **Max Bandwidth (Mbps)** for the M Series, MX Series, and ACX Series Routers:

Table 15: 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 **Next** to save the UNI settings. Continue with [“Specifying Connectivity and MAC Security Information” on page 261](#).

Specifying UNI Settings for Services with 802.1Q Interface Types

UNI Settings

▲ Traffic Treatment

Ethernet option:

dot1q

Customer traffic type:

Transport single vlan

VLAN ID selection:

Auto pick

Editable in Service Order

VLAN range for auto-pick:

1

4094

VLAN range for manual input:

Outer Tag protocol ID:

0x88a8

Editable in Service Order

Inner Tag protocol ID:

Please select ...

Editable in Service Order

▲ Interface Settings

Physical IF encapsulation:

flexible-ethernet-services

Logical IF encapsulation:

vlan-vpls

▲ LDP PW Extension Settings

Physical IF encapsulation:

vlan-ccc

Logical IF encapsulation:

vlan-ccc

▲ MTU Settings

Default MTU (Bytes):

1522

Editable in Service Order

MTU range (Bytes):

1522

9192

▲ Calculation of Burst-Size

To set UNI attributes for 802.1Q interfaces:

- 1. Fill in the fields as indicated in the table.

Field	Action
Traffic Treatment Settings	
Ethernet option	<div>Select dot1q from the drop-down list.</div> <div>The Ethernet option you choose determines the other options you can select and specify on the page.</div>

Field	Action
Customer traffic type	<p>Select a traffic type to restrict the traffic that can be transported across the network for the service:</p> <ul style="list-style-type: none"> • Select Transport single vlan to transport the traffic for a specific VLAN across the network. Single VLAN is the only option for 802.1Q interface types. You need to specify the Outer Tag protocol ID. <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> <ul style="list-style-type: none"> • Select Transport vlan range to transport the traffic for a range of VLANs across the network. <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>In the VLAN ID selection box, specify how the VLAN ID is determined:</p> <ul style="list-style-type: none"> • To allow the service provider to specify the VLAN ID, choose Select manually. This option is used typically when no VLAN normalization is applied. <p>Specify the VLAN ID range in VLAN range for manual input.</p> <p>Range: 1 through 4094</p> <p>To enable the service provisioner to override this setting, select Editable in Service Order.</p> <ul style="list-style-type: none"> • To cause the VLAN ID to be selected automatically from the VLAN ID pool, select Auto pick. This option is used typically when VLAN normalization is applied. <p>Specify the VLAN ID pool in VLAN range for auto-pick</p> <p>Range: 1 through 4094</p> <p>To enable the service provisioner to override this setting in a service order, select Editable in Service Order.</p> <p>To enable the service provisioner to override this setting in a service order, select Editable in Service Order.</p>
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 (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	To allow the service provisioner to override the MTU setting, select the check box for those options.

Interface Settings

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 window.

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
----------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Field	Action
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>
MTU Settings	<p>In the Default MTU box, specify the MTU for each UNI.</p> <p>To allow the service provisioner to override the MTU setting, select Editable in Service Order and, in the MTU range boxes, type the highest and lowest MTU values that the service provisioner can type.</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 <p>If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902.</p> <p>The default value for MTU Factor is 1.</p> Line Rate Based <p>If you select the option Line Rate Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds.</p> <p>The default value for Burst Period is 1.</p> <p>NOTE: The Calculate Burst Size list is enabled only when you select the Enable rate limiting checkbox.</p>
-----------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The following illustration shows the appearance of the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.

The screenshot shows a panel titled "Calculation of Burst-Size". Inside the panel, there is a label "Calculate Burst Size:" followed by a dropdown menu with "Line Rate Based" selected. Below this, there is a label "Burst Period (ms):" followed by a text input field containing the value "1". To the right of the input field is a checkbox labeled "Editable in Service Order", which is currently unchecked.

Bandwidth Settings

Field	Action
-------	--------

The following illustration shows the Bandwidth Settings panel, which appears if you do not select the **Enable QoS** check box in the preceding **General** settings window.

Bandwidth Settings

☒ Enable rate limiting

☒ Editable in Service Order

Default bandwidth (Mbps):

10

Min Bandwidth (Kbps):

1000

Max Bandwidth (Mbps):

100

Increment (Kbps):

1000

Enable 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 not available in the service definition when QoS Design software is installed.</p>
Default bandwidth (Mbps)	<p>Specify the default bandwidth value in Mbps.</p> <p>Default: 10 Mbps</p> <p>Range: 1 Mbps through 100000 Mbps</p>
Min Bandwidth (Kbps)	<p>Specify the minimum bandwidth value in Kbps.</p> <p>Default: 1000 Kbps</p> <p>Range: 64 Kbps through 100000 Kbps</p>
Max Bandwidth (Mbps)	<p>Specify the maximum bandwidth value in Mbps. For more information on maximum bandwidth see Table 15 on page 245</p> <p>Default: 100 Mbps</p> <p>Range: 1 Mbps through 100000 Mbps/100Gbps</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 100000 Kbps</p>

2. Click **Next** to save the UNI settings. Continue with [“Specifying Connectivity and MAC Security Information” on page 261](#).

Specifying UNI Settings for Services with Q-in-Q Interface Types

UNI Settings

▲ Traffic Treatment

Ethernet option:

qinq

Customer traffic type:

Transport vlan range

VLAN ID selection:

Auto pick

Editable in Service Order

VLAN range for auto-pick:

1

4094

VLAN range for manual input:

Outer Tag protocol ID:

0x88a8

Editable in Service Order

Inner Tag protocol ID:

0x8100

Editable in Service Order

▲ Interface Settings

Physical IF encapsulation:

flexible-ethernet-services

Logical IF encapsulation:

vlan-vpls

▲ LDP PW Extension Settings

Physical IF encapsulation:

vlan-ccc

Logical IF encapsulation:

vlan-ccc

▲ MTU Settings

Default MTU (Bytes):

1522

Editable in Service Order

MTU range (Bytes):

1522

9192

▲ Calculation of Burst-Size

To set UNI attributes for Q-in-Q interfaces:

1. Fill in the fields as indicated in the table.

Field	Action
Traffic Treatment Settings	
Ethernet option	Select qinq from the drop-down list.
	The window expands to include options specific to Q-in-Q interfaces.

Field	Action
Customer traffic type	<p>In the Customer traffic type box:</p> <ul style="list-style-type: none"> • Select Transport all traffic to transport the traffic from all VLANs across the network. You need to specify only the Outer Tag protocol ID. <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.</p> <ul style="list-style-type: none"> • Select Transport single vlan to transport the traffic for a specific VLAN across the network. Single VLAN is the only option for 802.1Q interface types. You need to specify the Outer Tag protocol ID and the Inner Tag protocol ID. • Select Transport vlan range to limit the traffic across the network to a specific range of VLANs. <p>If you select this option, the service provisioner will be prompted for the VLAN-ID range when creating a service order based on this service definition. You need to specify the Outer Tag protocol ID and the Inner Tag protocol ID.</p>
VLAN ID selection	<p>In the VLAN ID selection box, specify how the service VLAN ID is set during service order creation:</p> <ul style="list-style-type: none"> • To cause the provisioning software to automatically select the service VLAN ID from the VLAN ID pool, select Auto pick. This option is used typically when no VLAN normalization is applied. <p>Specify the VLAN ID pool in VLAN range for auto-pick</p> <p>Range: 1 through 4094</p> <ul style="list-style-type: none"> • To allow the service provisioner to specify the service VLAN ID, choose Select manually. This option is used typically when VLAN normalization is applied. <p>Specify the VLAN ID range in VLAN range for manual input.</p> <p>Range: 1 through 4094</p> <p>To enable the service provisioner to override this setting, select the Editable in Service Order check box.</p>
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 (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>
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 MTU setting, select the check box for those options.

Interface Settings

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 Q-in-Q interfaces, the only option is flexible-ethernet-services .
Logical IF encapsulation	The Logical IF encapsulation field is constrained by your selection in the Physical Interface 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 window.

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>
MTU Settings	<p>In the Default MTU box, specify the MTU for each UNI.</p> <p>To allow the service provisioner to override the MTU setting, select the Editable in Service Order check box and, in the MTU range boxes, type the lowest and highest values for the MTU that the service provisioner can type.</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 <p>If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902.</p> <p>The default value for MTU Factor is 1.</p> • Line Rate Based <p>If you select the option Line Rate Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds.</p> <p>The default value for Burst Period is 1.</p> <p>NOTE: The Calculate Burst Size list is enabled only when you select the Enable rate limiting checkbox.</p>
-----------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The following illustration shows the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.

The screenshot shows a configuration panel titled "Calculation of Burst-Size". Inside the panel, there is a label "Calculate Burst Size:" followed by a dropdown menu currently showing "Line Rate Based". Below this, there is a label "Burst Period (ms):" followed by a text input field containing the number "1". To the right of the input field is an unchecked checkbox labeled "Editable in Service Order".

Bandwidth Settings

Field	Action
-------	--------

The following illustration shows the Bandwidth Settings panel, which appears if you do not select the **Enable QoS** check box in the preceding **General** settings window.

Bandwidth Settings

☒ Enable rate limiting

☒ Editable in Service Order

Default bandwidth (Mbps):

10

Min Bandwidth (Kbps):

1000

Max Bandwidth (Mbps):

100

Increment (Kbps):

1000

Enable 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 not available in the service definition when QoS Design software is installed.</p>
Default bandwidth (Mbps)	<p>Specify the default bandwidth value in Mbps.</p> <p>Default: 10 Mbps</p> <p>Range: 1 Mbps through 100000 Mbps</p>
Min Bandwidth (Kbps)	<p>Specify the minimum bandwidth value in Kbps.</p> <p>Default: 1000 Kbps</p> <p>Range: 64 Kbps through 100000 Kbps</p>
Max Bandwidth (Mbps)	<p>Specify the maximum bandwidth value in Mbps. For more information on maximum bandwidth see Table 15 on page 245</p> <p>Default: 100 Mbps</p> <p>Range: 1 Mbps through 100000 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 100000 Kbps</p>

2. Click **Next** to save the UNI settings. Continue with [“Specifying Connectivity and MAC Security Information” on page 261.](#)

Specifying 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.

UNI Settings

Traffic Treatment

Ethernet option: asymmetric tag depth

Customer traffic type: Transport single vlan

VLAN ID selection: Auto pick

VLAN range for auto-pick: 1

VLAN range for manual input:

Outer Tag protocol ID: 0x8100

Inner Tag protocol ID: 0x88a8

Editable in Service Order

Editable in Service Order

Editable in Service Order

Interface Settings

Physical IF encapsulation: flexible-ethernet-services

Logical IF encapsulation: vlan-vpls

LDP PW Extension Settings

Physical IF encapsulation: vlan-ccc

Logical IF encapsulation: vlan-ccc

MTU Settings

Default MTU (Bytes): 1522

MTU range (Bytes): 1522

Editable in Service Order

9192

Calculation of Burst-Size

To set UNI attributes for asymmetric interfaces:

- 1. Fill in the fields as indicated in the table.

Field	Action
Traffic Treatment Settings	
Ethernet option	Select asymmetric tag depth from the drop-down list.

Field	Action
Customer traffic type	<p>In the Customer traffic type box:</p> <ul style="list-style-type: none"> • Select Transport all traffic to transport the traffic from all VLANs across the network. You need to Specify only the Outer Tag protocol ID. <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.</p> <ul style="list-style-type: none"> • Select Transport single vlan to transport the traffic for a specific VLAN across the network. Single VLAN is the only option for 802.1Q interface types. You need to specify the Outer Tag protocol ID and the Inner Tag protocol ID. • Select Transport vlan range to limit the traffic across the network to a specific range of VLANs. <p>If you select this option, the service provisioner will be prompted for the VLAN-ID range when creating a service order based on this service definition. You need to specify the Outer Tag protocol ID and the Inner Tag protocol ID.</p>
VLAN ID selection	<p>In the VLAN ID selection box, specify how the service VLAN ID is set during service order creation:</p> <ul style="list-style-type: none"> • To cause the provisioning software to automatically select the service VLAN ID from the VLAN ID pool, select Auto pick. This option is used typically when no VLAN normalization is applied. <p>Specify the VLAN ID pool in VLAN range for auto-pick Range: 1 through 4094</p> <ul style="list-style-type: none"> • To allow the service provisioner to specify the service VLAN ID, choose Select manually. This option is used typically when VLAN normalization is applied. <p>Specify the VLAN ID range in VLAN range for manual input. Range: 1 through 4094</p> <p>To enable the service provisioner to override this setting, select the Editable in Service Order check box.</p>
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 (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>
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	<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 IF encapsulation	The Logical IF encapsulation field is constrained by your selection in the Physical Interface Encapsulation field. For the physical encapsulation mode of flexible-ethernet-services, your only option is to select vlan-vpls for the logical encapsulation method.

Field	Action
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 window.	
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>
MTU Settings	<p>In the Default MTU box, specify the MTU for each UNI.</p> <p>To allow the service provisioner to override the MTU setting, select the Editable in Service Order check box and, in the MTU range boxes, type the lowest and highest values for the MTU that the service provisioner can type.</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 <p>If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902.</p> <p>The default value for MTU Factor is 1.</p> • Line Rate Based <p>If you select the option Line Rate Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds.</p> <p>The default value for Burst Period is 1.</p> <p>NOTE: The Calculate Burst Size list is enabled only when you select the Enable rate limiting checkbox.</p>

Field	Action
-------	--------

The following illustration shows the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.

Calculation of Burst-Size

Calculate Burst Size:

Line Rate Based

Burst Period (ms):

1

☐ Editable in Service Order

Bandwidth Settings

The following illustration shows the Bandwidth Settings panel, which appears if you do not select the **Enable QoS** check box in the preceding **General** settings window.

Bandwidth Settings

☒ Enable rate limiting

☒ Editable in Service Order

Default bandwidth (Mbps):

10

Min Bandwidth (Kbps):

1000

Max Bandwidth (Mbps):

100

Increment (Kbps):

1000

Enable 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 not available in the service definition when QoS Design software is installed.</p>
Default bandwidth (Mbps)	<p>Specify the default bandwidth value in Mbps.</p> <p>Default: 10 Mbps</p> <p>Range: 1 Mbps through 100000 Mbps</p>
Min Bandwidth (Kbps)	<p>Specify the minimum bandwidth value in Kbps.</p> <p>Default: 1000 Kbps</p> <p>Range: 64 Kbps through 100000 Kbps</p>
Max Bandwidth (Mbps)	<p>Specify the maximum bandwidth value in Mbps. For more information on maximum bandwidth see Table 15 on page 245</p> <p>Default: 100 Mbps</p> <p>Range: 1 Mbps through 100000 Mbps</p>

Field	Action
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 100000 Kbps

2. Click **Next** to save the UNI settings. Continue with [“Specifying Connectivity and MAC Security Information” on page 261.](#)

Specifying Connectivity and MAC Security Information

In this step, you specify the attributes that define the connectivity among remote sites across the service provider network and the service security. The following is a sample **Connectivity** window.

Connectivity

Connectivity Settings

Route target: Select manually

Route distinguisher: Select manually

VLAN normalization: Normalize to QinQ tags

☒ Allow Multihoming

☐ Editable in Service Order

☐ Editable in Service Order

LDP PW Extension Settings

VCID: Auto pick

Revert time (sec): 5

Switch Over Delay (sec): 0

☐ Editable in Service Order

☐ Editable in Service Order

MAC Security Settings

☒ MAC learning

Interface MAC limit: 1024

☐ MAC statistics

MAC table size: 5120

☐ Editable in Service Order

☐ Editable in Service Order

☐ Editable in Service Order

☐ Editable in Service Order

To configure connectivity between sites across the network:

1. Fill in the fields in the **Connectivity** window.

Field	Action
Route target	<p>Choose one of the following options from the list:</p> <ul style="list-style-type: none"> • Auto pick • Select manually <p>This field is available in either of the following cases:</p> <ul style="list-style-type: none"> • The Signaling type is BGP. • The Signaling type is LDP and Auto Discovery is enabled.
Route distinguisher	<p>Select a route distinguisher option:</p> <ul style="list-style-type: none"> • Select manually—The service provider specifies the route distinguisher. • Auto pick—The route distinguisher is selected automatically. <p>To override this setting in the service order, select the Editable in Service Order check box.</p> <p>This field is available in either of the following cases:</p> <ul style="list-style-type: none"> • The Signaling type is BGP. • The Signaling type is LDP and Auto Discovery is enabled.
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. NOTE: For services that transport a range of VLAN IDs, you must set VLAN Normalization to all. You cannot transport a range of VLAN IDs without normalization. • 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 each endpoint • 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>For more information about VLAN normalization, see “Junos Space Layer 2 Services Overview” on page 142.</p> <p>For information about VLAN manipulation, see “Understanding VLAN Manipulation (Normalization and VLAN Mapping) on Ethernet Services” on page 710.</p>

Field	Action
Allow Multihoming	This check box is available only if the signaling type is BGP. To enable a service provisioner to define primary and backup PE devices in a multihomed group that serves a single customer site, select Allow Multihoming .
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 checkbox in the General window is checked for the LDP signaling, then the Auto Discovery checkbox is disabled in the Connectivity Settings page.</p> <p>The Auto Discovery checkbox is not available on 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>
VPLS 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.</p> <ul style="list-style-type: none"> • Autopick • Select manually
VPN ID	<p>This field is available only if the signaling type is LDP and auto discovery is enabled.</p> <p>Identifies the VPN ID associated with the router.</p> <ul style="list-style-type: none"> • Autopick • Select manually
Revert time (sec)	<p>This field is available only if the Enable PW Resiliency is enabled.</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>

Field	Action
Switch Over Delay (sec)	<p>This field is available only if the Enable PW Resiliency is enabled.</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>
VCID	<p>This field is available only if the Service type is point-to-multipoint, the Signaling is BGP, and the Enable PW Extension is enabled.</p> <p>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.</p>
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.
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 connectivity settings and continue with [“Specifying Advanced Settings” on page 235](#).

Specifying Advanced Settings

In this step, you can specify the parameters that define advanced connectivity between sites across the service provider network. The following illustration shows the **Advanced** window.

To specify advanced settings:

- Fill in the fields as indicated in the table.

Field	Action
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).

Field	Action
fast-reroute-priority	<p>In the fast-reroute-priority, 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 is enabled.</p>
Connectivity type	<p>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):</p> <ul style="list-style-type: none"> ● 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. <p>NOTE: This field is unavailable if the Signaling type is LDP and the Auto discovery is enabled.</p>
Editable in Service Order	<p>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.</p>

2. Click **Finish** to save the advanced settings.

The service definition is complete.

RELATED DOCUMENTATION

Publishing a Custom Service Definition 308
Predefined Point-to-Multipoint Ethernet Service Definitions 554
Viewing Service Definitions 267
Creating an E-Line Service Definition 188
Creating a Multipoint-to-Multipoint VPLS Service Definition 214

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. You can tag a service definition to categorize or filter it, view tags, and untag.

- [Tabular View | 267](#)
- [Searching for Service Definitions | 268](#)
- [Viewing Service Definition Details | 268](#)
- [Performing Actions on Service Definitions | 269](#)

Tabular View

In tabular view, service definition information appears in table rows and columns.

[Table 16 on page 267](#) describes the information presented in the table.

Table 16: 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 16: Service Definition Table Fields (*continued*)

Column	Meaning
Service Type	<p>One of the following:</p> <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	<p>One of the following values:</p> <ul style="list-style-type: none"> • BGP • LDP
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.

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. The following example shows a summary of the settings for a point-to-point Ethernet service definition.

Service Definition Details

General

Name: P2P_LDP_PW_Resiliency_L3VPN

Type: Point-to-Point Pseudowire

Signaling: LDP

Interface type: Ethernet

☒ Enable PW access to L3 network

Service template : None

QoS: Enabled

Comments:

☒ Enable PW Resiliency

UNI Settings

Ethernet option: port-port

Traffic type: N/A

VLAN ID selection: N/A ☐ Editable in Service Order

Auto-pick VLAN Pool Range: N/A

Manual VLAN Pool Range: N/A

Physical IF encapsulation: ethernet-ccc

Logical IF encapsulation: N/A

Default MTU (Bytes): 1522 ☐ Editable in Service Order

MTU range (Bytes): 1522-9192

Rate limiting: Not enabled

Default Bandwidth (Mbps): N/A ☐ Editable in Service Order

Bandwidth range: N/A

Increment (Kbps): 0

Connectivity Settings

VC ID selection: Auto pick ☐ Editable in Service Order

Default MTU (Bytes): 1522 ☐ Editable in Service Order

MTU range (Bytes): 1522-9192

Revert Time: 5 ☐ Editable in Service Order

Switch Over Delay: 0 ☐ Editable in Service Order

OK

For information about the meaning of each attribute, see [“Service Attributes Overview” on page 152](#).

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 308.
- **Unpublish Service Definition**—See [“Unpublishing a Custom Service Definition”](#) on page 309.
- **Delete Service Definition**—See [“Deleting a Customized Service Definition”](#) on page 309.
- **Tag It**—See *Tagging an Object*.
- **View Tags**—See *Viewing Tags for a Managed Object*.
- **Untag It**—See *Untagging Objects*.

RELATED DOCUMENTATION

Predefined Point-to-Point Service Definitions	 477
Predefined Multipoint-to-Multipoint Ethernet Service Definitions	 521
Predefined Point-to-Multipoint Ethernet Service Definitions	 554
Predefined Hub-and Spoke Layer 3 VPN Service Definitions	 572
Creating an E-Line Service Definition	 188
Creating a Multipoint-to-Multipoint VPLS Service Definition	 214
Creating a Point-to-Multipoint VPLS Service Definition	 237
Creating a Hub-and-Spoke (One Interface) Layer 3 VPN Service Definition	 386

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 | 271](#)
2. [Specifying UNI Settings for ATM and TDM Service Definitions | 274](#)
3. [Specifying UNI Settings for ATM Interfaces | 274](#)
4. [Specifying UNI Settings for TDM Interfaces | 274](#)
5. [Specifying Connectivity Information for an ATM or a TDM Service | 276](#)

Specifying General Information for the ATM or TDM Service

1. In the Network Activate task pane, select **Service Design > Manage Service Definitions > Create P2P Service Definition**.

The first **Create Service Definition** window appears.

General

Name:

Service type: **Point-to-Point Pseudowire**

Signaling: ▼

Comments:

Service Template: × × ▼

Default Service Template: × ▼

Threshold alarm profile: ▼

Interface type: ☐ Ethernet
☐ TDM
☒ ATM
☐ Static pseudowire
☐ Enable PW access to L3 VPN network
☐ Enable Multi Segment Pseudowire
☐ Enable PW Resiliency
☐ Decouple Service Status From Port Status

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 **Comments** 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, select a service template from the **Service Template** list.

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 116](#).

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 645](#).

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 165](#).
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, not the jnxVpnIfVpn traps.

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

The screenshot shows the 'UNI Settings' window with the 'ATM Options' tab selected. The settings are as follows:

Field	Value	Editable in Service Order
Physical IF encapsulation:	atm-ccc-cell-relay	<input type="checkbox"/>
VPI selection:	Select manually	<input type="checkbox"/>
VCI selection:	Select manually	<input type="checkbox"/>
Cell bundle size:	1	<input checked="" type="checkbox"/>

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 atm-ccc-cell-relay for ATM cell relay encapsulation. Use atm-ccc-cell-mux 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.
VCI 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

UNI Settings

TDM Options

Physical IF encapsulation: ▾

Jitter buffer: ☐ Editable in Service Order

Idle pattern: ☐ Editable in Service Order

Excessive packet loss rate: ☐ Editable in Service Order

Payload size: ☐ Editable in Service Order

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 DS0s on one IP circuit, and you can have more than one circuit emulation IP flow created from a single physical interface. For example, some DS0 channels from a T1 interface can go in an IP flow to destination A, and other DS0 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
	BX7000 Gateway: 2K through 32K	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%

SAToP Field	Value Range	Default Value
Payload size	M Series: 64 through 1024	192
NOTE: If the Physical IF encapsulation type is CESoPSN, the Payload size is unavailable.	BX7000 Gateway: 24 through 1440	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.

Connectivity

Connectivity Settings

VC ID selection: Auto pick

Default MTU (Bytes): 1522

MTU range (Bytes): 1522

Revert time (sec): 5

Switch Over Delay (sec): 0

Outgoing label selection: Select manually

☐ Editable in Service Order

☒ Editable in Service Order

☐ Editable in Service Order

☐ Editable in Service Order

9192

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>

Field	Action
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>NOTE: The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to http://www.iana.org/assignments/ipv4-address-space for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space for the list of restricted IPv6 addresses.</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>NOTE: The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to http://www.iana.org/assignments/ipv4-address-space for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space for the list of restricted IPv6 addresses.</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 **Finish** to create a point-to-point ATM/TDM service definition.

RELATED DOCUMENTATION

[Prestaging ATM and TDM Pseudowire Devices | 46](#)

[Prestaging ATM and TDM Pseudowire Devices | 46](#)

[Creating a Point-to-Point ATM or TDM Pseudowire Service Order | 578](#)

Creating an E-Line Service Definition

Use this procedure to create a definition for an E-Line 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 E-Line 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 an E-Line service definition, complete these tasks, in the order shown:

1. [Specifying General Information | 279](#)
2. [Specifying UNI Settings | 283](#)
3. [Specifying Connectivity Information When Signaling Is LDP | 299](#)
4. [Specifying Connectivity Information When Signaling Is BGP | 302](#)

Specifying General Information

To specify the general information for an E-Line service definition:

1. In the Network Activate task pane, select **Service Design > Manage Service Definitions > Create E-Line Service Definition**. The **General** settings window appears.

General

Name:

LDP-Service-Definition

Service type:

Point-to-Point Pseudowire

Signaling:

LDP

Comments:

Service Template:

Flexi_TempX Flexi_Temp_Inner_OuterX X ▾

Default Service Template:

Flexi_TempX Flexi_Temp_Inner_OuterX X ▾

Threshold alarm profile:

Please select ... ▾

☒ Enable QoS

Interface type:

☒ Ethernet

☐ TDM

☐ ATM

☐ Static pseudowire

☐ Enable PW access to L3 VPN network

☐ Enable Multi Segment Pseudowire

☐ Enable PW Resiliency

☐ Decouple Service Status From Port Status

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 E-Line .
Signaling	<div>Select a signaling type:<ul style="list-style-type: none">• BGP• LDP</div> <div>You cannot edit the Signaling type in the service order.</div> <div>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.</div>

Field	Action
Comments (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 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>
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>

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 E-Line 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 E-Line pseudowire stitching, see “Stitching Two Point-to-Point Pseudowires” on page 645.</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 165.</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, not the jnxVpnIfVpn traps.</p>

Field	Action
Service Template	<p>(Optional) To include a service template for the service, select a service template from the Service Template list.</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 116.</p>

3. Click **Next** to save the information. Continue with [“Specifying UNI Settings” on page 192](#).

SEE ALSO

Service Templates Overview 113
Creating a Service Template 116
Importing a Service Template 125

Specifying UNI Settings

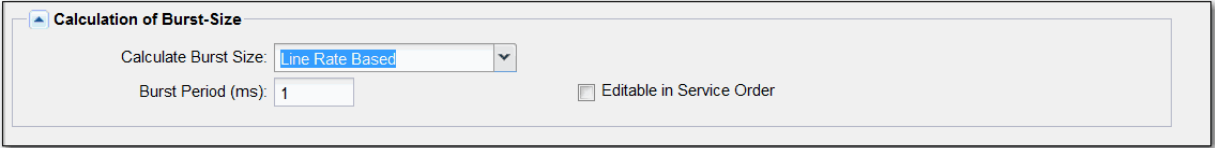
In this step, you provide the UNI service attributes for this service definition. The attributes you set depend on whether you are setting attributes for a port, an 802.1Q interface, a Q-in-Q interface, or a flexible VLAN tagging:

- [Specifying UNI Settings for Port-to-Port Services | 284](#)
- [Specifying UNI Settings for Services with 802.1Q Interface Types | 287](#)

Field	Action
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	

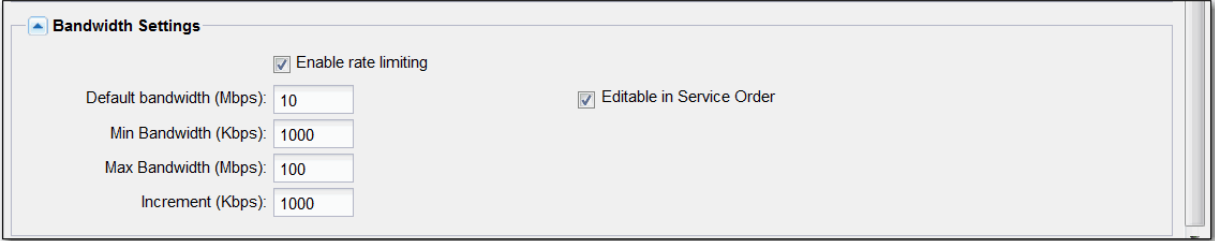
Field	Action
Calculate Burst Size	<p>Select the preferred option for calculating the burst size:</p> <ul style="list-style-type: none">• MTU Based If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902. The default value for MTU Factor is 1.• Line Rate 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 checkbox.</p>

The following illustration shows the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.



Bandwidth Settings

The following illustration shows the Bandwidth Settings panel, which appears if you do not select the **Enable QoS** check box in the preceding **General** settings window.



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>

Field	Action
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 17: 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.
------------------	---------------------------------------------------------------------------------

3. 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.

1. Enter information in the UNI Settings window.

UNI Settings

▲ Traffic Treatment

Ethernet option:

dot1q

▼

Customer traffic type:

Transport single vlan

▼

VLAN ID selection:

Auto pick

▼

VLAN range for auto-pick:

10

1000

VLAN range for manual input:

Outer Tag protocol ID:

0x88a8

✕

▼

Inner Tag protocol ID:

Please select ...

▼

☐ Editable in Service Order

☐ Editable in Service Order

☐ Editable in Service Order

▲ Interface Settings

Physical IF encapsulation:

flexible-ethernet-services

▼

Logical IF encapsulation:

vlan-ccc

▼

▲ MTU Settings

Default MTU (Bytes):

1522

9192

MTU range (Bytes):

1522

9192

☐ Editable in Service Order

▲ Calculation of Burst-Size

Calculate Burst Size:

MTU Based

▼

MTU Factor:

1

☐ Editable in Service Order

2. 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 Ethernet option you choose determines the other options you can select and specify on the page.

Field	Action
Customer traffic type	<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 ID selection	<p>Indicate how the VLAN ID is determined:</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.</p>
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</pre> <pre>set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x88a8</pre> <pre>set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x8100</pre>
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>
----------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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

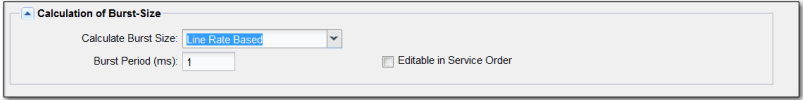
Specify the default bandwidth value, in Mbps.

Default: 10 Mbps

Range: 1 Mbps through 100,000 Mbps

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 1.• 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 checkbox.</p>
-----------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The following illustration shows the appearance of the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.



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:

UNI Settings

▲ Traffic Treatment

Ethernet option:

qinq

Customer traffic type:

Transport vlan range

VLAN ID selection:

Select manually

10

1000

VLAN range for auto-pick:

VLAN range for manual input:

Outer Tag protocol ID:

0x88a8

✕ ▾

Editable in Service Order

Inner Tag protocol ID:

0x8100

✕ ▾

Editable in Service Order

▲ Interface Settings

Physical IF encapsulation:

flexible-ethernet-services

Logical IF encapsulation:

vlan-ccc

▲ MTU Settings

Default MTU (Bytes):

1522

Editable in Service Order

MTU range (Bytes):

1522

9192

▲ Calculation of Burst-Size

Calculate Burst Size:

MTU Based

MTU Factor:

1

Editable in Service Order

- 2. Fill in the fields in the **UNI Settings** window according to the following table:

Field	Action
Traffic Treatment Settings	
Ethernet option	Select qinq from the list. The window expands to include options specific to Q-in-Q interfaces.

Field	Action
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>
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>

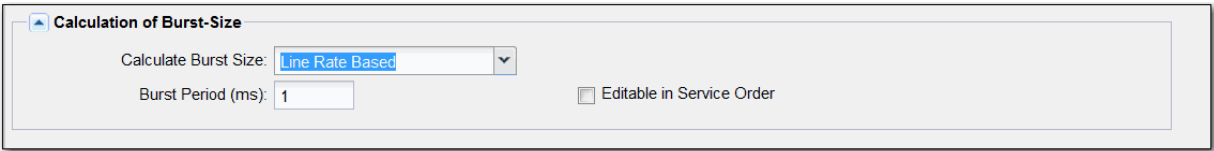
Field	Action
Outer Tag protocol ID	<p>Select the outer tag protocol ID if the Customer traffic type is Transport single VLAN:</p> <ul style="list-style-type: none"> • 0x88a8 • 0x8100 • 0x9100 <p>NOTE: For an interface, you must configure a physical port with the possible Tag Protocol Identifiers (TPIDs) 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</pre> <pre>set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x88a8</pre> <pre>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	

Field	Action
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 1.• 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 checkbox.</p>
----------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The following illustration shows the appearance of the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.



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.

UNI Settings

▲ Traffic Treatment

Ethernet option:

asymmetric tag depth

Customer traffic type:

Transport all traffic

VLAN ID selection:

Select manually

☐ Editable in Service Order

VLAN range for auto-pick:

236

1024

VLAN range for manual input:

1310

2609

Outer Tag protocol ID:

Please select ...

☐ Editable in Service Order

Inner Tag protocol ID:

☐ Editable in Service Order

▲ Interface Settings

Physical IF encapsulation:

vlan-ccc

Logical IF encapsulation:

vlan-ccc

▲ MTU Settings

Default MTU (Bytes):

1522

☐ Editable in Service Order

MTU range (Bytes):

1522

9192

▲ Calculation of Burst-Size

Calculate Burst Size:

MTU Based

MTU Factor:

1

☐ Editable in Service Order

2. Specify the UNI Settings for asymmetric tag depth according to the following table:

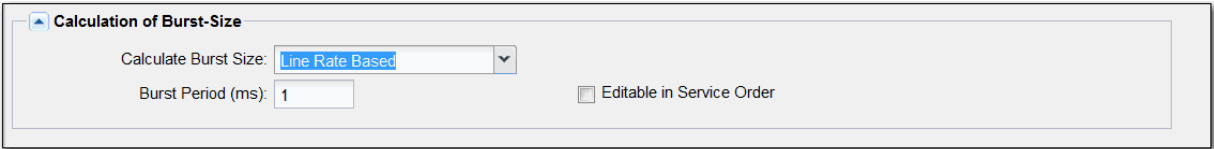
Field	Action
Traffic Treatment Settings	
Ethernet option	Select asymmetric tag depth from the list.
Customer traffic type	<div>Select the customer traffic type:</div> <ul style="list-style-type: none">● Transport all traffic—Transports the traffic from all VLANs across the network. When you select this 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. 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. <div>NOTE: Make sure to check Editable in Service Order if you want the service provisioner to be able to override this setting.</div>

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>
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</pre> <pre>set interfaces ae0 aggregated-ether-options ethernet-switch-profile tag-protocol-id 0x88a8</pre> <pre>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	

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 1.• 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 checkbox.</p>

The following illustration shows the appearance of the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.



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.

To specify connectivity between sites across the network when signaling is LDP:

Connectivity

Connectivity Settings

VC ID selection: Auto pick

Default MTU (Bytes): 1522

MTU range (Bytes): 1522

Revert time (sec): 5

Switch Over Delay (sec): 0

VLAN normalization: Normalization not required

Outgoing label selection: Select manually

☐ Editable in Service Order

☒ Editable in Service Order

9192

☐ Editable in Service Order

☐ Editable in Service Order

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>

Field	Action
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	The options available in the VLAN normalization are based on the value set for the Ethernet interface.
Outgoing label selection	<p>This field is available if you selected the Static pseudowire check box in the General settings.</p> <p>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>
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>

Ethernet Option	Customer Traffic Type	VLAN Normalization
	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:

The screenshot shows the 'Connectivity' window with the following fields and options:

- Connectivity Settings** (expanded):
 - Route Distinguisher: Auto pick (dropdown)
 - Route Target: Auto pick (dropdown)
 - Default MTU (Bytes): 1522 (text input)
 - MTU range (Bytes): 1522 (text input)
 - VLAN normalization: Swap (dropdown menu is open, showing options: Swap, Normalize to None, Normalize to Dot1q tag, and Normalize to QinQ tags (highlighted)).
- On the right side:
 - Editable in Service Order (checkbox, unchecked)
 - Editable in Service Order (checkbox, unchecked)
 - Editable in Service Order (checkbox, unchecked)
 - 9192 (text input)

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.

NOTE: The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to <http://www.iana.org/assignments/ipv4-address-space> for the list of restricted IPv4 addresses and <http://www.iana.org/assignments/ipv6-address-space> for the list of restricted IPv6 addresses.

- **Route Target**—Allows you to distribute VPN routes to only the routers that need them.

NOTE: The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to <http://www.iana.org/assignments/ipv4-address-space> for the list of restricted IPv4 addresses and <http://www.iana.org/assignments/ipv6-address-space> for the list of restricted IPv6 addresses.

- **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 Network Activate software manipulates VLANs, see [“Understanding VLAN Manipulation \(Normalization and VLAN Mapping\) on Ethernet Services” on page 710](#).

2. Click **Finish** to complete the service definition.

RELATED DOCUMENTATION

[Publishing a Custom Service Definition | 308](#)

[Predefined Point-to-Point Service Definitions | 477](#)

[Viewing Service Definitions | 267](#)

Creating a Cross Provisioning Platform Service Definition

Before you create a Cross Provisioning Platform (CPP) service order, you must complete the following tasks:

- Import into the system the scripts that define the Juniper Networks devices.
- Import into the system the scripts that define the third-party devices.

To create a CPP service definition:

1. In the **Cross Provisioning Platform** task pane, select **CPP > Service Definitions**.
2. In the **CPP > Service Definition** window, click on the + button. The **Create Service Definition** window appears.

Create CPP Service Definition

General

Name: SD-LDP Description:

ID: 10435

Type: PW-LDP

Service Script Selections

Operation Type: Please Select

Select Scripts

Name	Vendor Type	Version
<input type="checkbox"/> PD_P2P_LDP_Create_Script_JNPR	Juniper	1
<input type="checkbox"/> PD_P2P_LDP_Modify_Script_JNPR	Juniper	1
<input type="checkbox"/> PD_P2P_LDP_Create_Script_ALU	Alcatel	1
<input type="checkbox"/> PD_P2P_LDP_Modify_Script_ALU	Alcatel	1
<input type="checkbox"/> PD_L3VPN_Create_Script_JNPR	Juniper	1
<input type="checkbox"/> PD_L3VPN_Modify_Script_JNPR	Juniper	1
<input type="checkbox"/> PD_L3VPN_Create_Script_ALU	Alcatel	1

Page 1 of 1 Displaying 1 - 47 of 47

Add Script

Selected Scripts

Name	Vendor Type	Operation Type	Action
<input type="checkbox"/> PD_P2P_LDP_Create_Script_JNPR	Juniper	Create	
<input type="checkbox"/> PD_P2P_LDP_Create_Script_ALU	Alcatel	Create	

Create Cancel

3. Enter information in the **Create Service Definition** window according to the descriptions in the following table.

Parameter	Description
Name	Enter a name for the service definition.
ID	<p>Enter a unique ID to associate with this service definition in the range 1 through 2147483647.</p> <p>NOTE: The service definition ID is optional. If you do not provide any value in this field, the default value is -1. In the service definition selection grid, no value is displayed in the ID column. Each service definition is assigned a unique ID. If you give an existing ID value while creating a new service definition, exception occurs.</p>
Description	Enter a description of the service to distinguish its operation from others.

Parameter	Description
Type	<p>Select the service type from the list of available types:</p> <ul style="list-style-type: none"> • Predefined service types <ul style="list-style-type: none"> • PW-LDP • PW-BGP • VPLS • L3VPN • NPS • Device • Report • VLAN-PATH • PW-LDP-IPASO • L3VPN-IPASO • Customized service types <p>NOTE: You can create service types in CPP > Service Types.</p>
Operation Type	<p>Select one of the following operation type:</p> <ul style="list-style-type: none"> • Create—If you select this option, the create scripts are executed. • Modify—If you select this option, the modify scripts are executed.
Select Scripts	<p>Select a script.</p> <p>The Select Scripts section lists the scripts that belong to various vendors along with the script version number. To find the script that you want to add, you can perform a search in the search box.</p>
Add Script	<p>Click Add Scripts to add a script to the service definition.</p>
Selected Script	<p>The Selected Scripts section lists the scripts that you have selected. The scripts are listed based on the vendor type and operation type.</p> <p>To delete a script, in the Action column click the delete icon.</p>

4. Click **Create**.
5. In the **Cross Provisioning Platform** task pane, select **CPP > Service Definitions**.
6. Select the service definition you just created and select **Action > Publish Service Definition**. The **State** column indicates when the service definition is published.

The value in the **ID** field is associated with a service definition. This identifier can be used when you are searching for a particular service definition while creating a service order. You can search the service definition by its name, type or unique ID. You can modify the ID only during the migration of old service definition IDs.

RELATED DOCUMENTATION

[Creating a Cross Provisioning Platform Service Order | 616](#)

[Viewing Cross Provisioning Platform Service Order Details | 622](#)

Publishing a Custom Service Definition

The service designer must publish a customized service definition before a service provisioner can use that definition to create a service request.

NOTE: Predefined service definitions are already in the Published state.

To publish a service definition:

1. In the Network Activate task pane, select **Service Design > Manage Service Definitions**.
2. In the **Manage Service Definitions** page, select the service definition you want to publish.
In the table, the State column lists unpublished service definitions.
3. Select the unpublished service definition that you want to publish.
4. Open the **Actions** menu and select **Publish Service Definition**.
The **Publish Service Definitions** window appears and prompts you to confirm your action.
5. Click **Publish**.

The **Manage Service Definitions** page reappears. The selected service definition is now in the published state.

RELATED DOCUMENTATION

Unpublishing a Custom Service Definition

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.

To unpublish a service definition:

1. In the **Network Activate** task pane, select **Service Design > Manage Service Definitions**.
2. In the **Manage Service Definitions** window, select the service definition you want to unpublish.
In table, the **State** column lists published service definitions.
3. Select the published service definition that you want to unpublish.
4. Open the **Actions** menu and select **Unpublish Service Definition**.
The **Unpublish Service Definitions** window appears and prompts you to confirm your action.
5. Click **Unpublish**.

The **Manage Service Definitions** screen reappears. The selected service definition is now in the unpublished state.

RELATED DOCUMENTATION

[Publishing a Custom Service Definition | 308](#)

Deleting a Customized Service Definition

NOTE: Before you can delete a service definition, it must be in the unpublished state.

You cannot delete a predefined service definition.

To delete a customized service definition:

1. In the **Network Activate** task pane, select **Service Design > Manage Service Definitions**.

In the **Manage Service Definitions** window, select the customized service definition you want to delete.

2. Open the **Actions** menu and select **Delete Service Definition**.

3. In the confirmation window, click **Delete**.

The **Manage Service Definitions** window refreshes with the selected service definition removed.

RELATED DOCUMENTATION

| [Unpublishing a Custom Service Definition](#) | 309

VPLS Service Definitions

IN THIS CHAPTER

- Creating a VPLS Service Definition in Cross Provisioning Platform | 311
- Creating a Multipoint-to-Multipoint VPLS Service Definition | 314
- Creating a Point-to-Multipoint VPLS Service Definition | 338
- Creating a Service Definition for VPLS Access into Layer 3 Networks | 369

Creating a VPLS Service Definition in Cross Provisioning Platform

Cross Provisioning Platform is an extension of the Network Activate application within Junos Space, which provides a single pane of interaction to deploy services across vendor network devices. This topic discusses how a VPLS service definition is created and deployed across the devices of Juniper Networks involved in the Cross Provisioning Platform.

To create a VPLS service definition, you need to create a configuration script in XSLT format and upload this script to Cross Provisioning Platform from the local system. You can add the script by selecting **Cross Provisioning Platform > CPP > Scripts > Add Script**.

NOTE: Junos Space server scripts are mandatory to create a VPLS service definition.

To create a VPLS service definition:

1. In the **Cross Provisioning Platform** task pane, select **CPP > Service Definitions**.

The **Service Definitions** page that appears displays a list of the existing service definitions.

2. Click **Create CPP Service Definition** above the tool grid.

The **Create Service Definition** page appears.

Create CPP Service Definition

General

Name: SD-VPLS

ID: 10435

Type: VPLS

Description:

Service Script Selections

Operation Type: Please Select

Select Scripts

Name	Vendor Type	Version
PD_P2P_BGP_Create_Script_JNPR	Juniper	1
PD_P2P_BGP_Modify_Script_JNPR	Juniper	1
PD_VPLS_Create_Script_JNPR	Juniper	1
PD_VPLS_Modify_Script_JNPR	Juniper	1
PD_VLAN-PATH_Create_Script_IPASO	Juniper	1
PD_VLAN-PATH_Modify_Script_IPASO	Juniper	1
PD_Interface_Migration_Script_JNPR	Juniper	1

Page 1 of 1

Displaying 1 - 47 of 47

Add Script

Selected Scripts

Name	Vendor Type	Operation Type	Action
PD_VLAN-PATH_Create_Script_IPASO	Juniper	Create	

Create Cancel

3. Perform the following steps:

- In the **General** section:
 - In the **Name** field, type 3 through 128 alphanumeric characters to identify the name of the service definition.
 - In the **ID** field, type 1 through 2147483647 integers to identify the service definition by a unique value.

NOTE: The service definition ID is optional. If you do not provide any value in this field, the default value is -1. In the service definition selection grid, no value is displayed in the **ID** column. Each service definition is assigned a unique ID. If you give an existing ID value while creating a new service definition, exception occurs.

- c. In the **Description** field, type 3 through 256 alphanumeric characters to further identify the service definition you named.
 - d. From the **Type** drop-down list, select **VPLS**.
- Select one of the following operation type:
 - Create
 - Modify
 - In the **Select Scripts**, select a script.

The **Select Scripts** section lists the scripts that belong to various vendors along with the script version number. To find the script that you want to add, you can perform a search in the search box.
 - Click **Add Scripts** to add a script to the service definition.

The **Selected Scripts** section lists the scripts that you have selected. The scripts are listed based on the vendor type and operation type.

To delete a script, in the **Action** column click the delete icon.
4. Click **Create** to create the service definition.

The **Service Definitions** page that appears displays the list of existing service definitions along with the service definition that you created.
 5. Right-click the service definition you created from the **Service Definitions** window and select **Publish Service Definition**.

The **Publish Service Definitions** dialog box that appears asks you to confirm the selection.
 6. Click **Publish** in the **Publish Service Definitions** window.

The **Service Definitions** page that appears displays the list of existing service definitions along with the service definition that you created.
 7. Double-click the service definition to view the details.

The **Service Definition Details** page that appears displays the details of the service definition along with the scripts that you uploaded.

RELATED DOCUMENTATION

[Adding Scripts Created for Cross Provisioning Platform | 775](#)

[Creating a VPLS Service Order in Cross Provisioning Platform | 705](#)

Creating a Multipoint-to-Multipoint VPLS Service Definition

IN THIS SECTION

- [Specifying General Information for Multipoint-to-Multipoint VPLS Service Definitions | 315](#)
- [Specifying UNI Settings for Multipoint-to-Multipoint VPLS Service Definitions | 319](#)
- [UNI Settings for Port-to-Port Interfaces in VPLS Services | 319](#)
- [UNI Settings for 802.1Q Interfaces in VPLS Services | 322](#)
- [UNI Settings for Q-in-Q Interfaces in VPLS Services | 326](#)
- [UNI Settings for Services with Flexible VLAN Tagging \(Asymmetric Interface Types\) | 330](#)
- [Specifying Connectivity and MAC Security Information | 333](#)
- [Specifying Advanced Settings | 336](#)

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

To specify the general information for a multipoint-to-multipoint service definition, in the Network Activate task pane, select **Service Design > Manage Service Definitions > Create VPLS Service Definition**

The **General** window appears.

General

Name:

Test

Service type:

Multipoint-to-Multipoint Ethernet (VPLS)

▼

Signaling:

LDP

▼

Comments:

Service Template:

Please select ...

▼

Threshold alarm profile:

Please select ...

▼

☒ Enable QoS

☐ Enable L3 Access

☒ Enable Static PW Labels

To specify the general information for a multipoint-to-multipoint service definition:

1. Fill in the fields on the **General** window.

Field	Action
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 window: <ul style="list-style-type: none"> • Route target • Route distinguisher • VLAN normalization • Allow Multihoming • Mac Security Settings • LDP—If LDP signaling is selected, the following fields are available in the Connectivity window: <ul style="list-style-type: none"> • Auto Discovery • Route target, if Auto Discovery is enabled • Route distinguisher, if Auto Discovery is enabled • VPLS ID, if Auto Discovery is disabled • 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>
Comments (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 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>
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 UNI 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>

Field	Action
Service Template	<p>(Optional) To include a service template for the service, select a service template from the Service Template list.</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 116.</p>

2. Click **Next** to save the information and continue with UNI Settings.

SEE ALSO

Service Templates Overview 113
Creating a Service Template 116
Importing a Service Template 125

Specifying UNI 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 Settings for Port-to-Port Interfaces in VPLS Services

The **UNI Settings** window provides four expanding or collapsing panels: Traffic Treatment, Interface Settings, MTU Settings, and Bandwidth Settings.

The screenshot shows the 'UNI Settings' window with four expandable panels. The 'Traffic Treatment' panel is expanded, showing settings for Ethernet option (port-port), Customer traffic type (N/A), VLAN ID selection (N/A), and checkboxes for 'Editable in Service Order'. The 'Interface Settings' panel is collapsed. The 'MTU Settings' panel is expanded, showing Default MTU (Bytes) as 1522, MTU range (Bytes) as 1522, and a checkbox for 'Editable in Service Order'. The 'Calculation of Burst-Size' panel is collapsed.

Panel	Setting	Value	Editable in Service Order
Traffic Treatment	Ethernet option:	port-port	
	Customer traffic type:	N/A	
	VLAN ID selection:	N/A	
	VLAN range for auto-pick:		
	VLAN range for manual input:		
	Outer Tag protocol ID:	Please select ...	
Interface Settings	Physical IF encapsulation:	ethernet-vpls	
	Logical IF encapsulation:	N/A	
MTU Settings	Default MTU (Bytes):	1522	<input checked="" type="checkbox"/>
	MTU range (Bytes):	1522	9192
	Calculate Burst Size:	MTU Based	
Calculation of Burst-Size	MTU Factor:	1	<input type="checkbox"/>

To specify the UNI Settings for Port-to-Port interfaces:

1. Fill in the fields on the **UNI Settings** window.

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	To allow the service provisioner to override the MTU setting, select the check box.
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 can not select a choice in this field because it is not relevant to port-to-port services.
MTU Settings	
Default MTU (Bytes)	The default MTU value is 1522 bytes.
MTU Range (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>
Calculation of Burst-Size	

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 1. 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 checkbox.</p>

The following illustration shows the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.

Calculation of Burst-Size

Calculate Burst Size: Line Rate Based

Burst Period (ms):

☐ Editable in Service Order

Bandwidth Settings

Enable 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 not available in the service definition when QoS Design software is installed.</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>

Field	Action
Max Bandwidth (Mbps)	<p>Specify the maximum bandwidth value in Mbps. For more information on maximum bandwidth see Table 14 on page 221</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>

The following table lists the **Max Bandwidth (Mbps)** for the M Series, MX Series, and ACX Series Routers:

Table 18: 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 **Next** to continue with Connectivity settings.

UNI Settings for 802.1Q Interfaces in VPLS Services

To specify the UNI Settings for 802.1Q interfaces:

1. Fill in the fields on the **UNI Settings** window.

Field	Action
Traffic Treatment Settings	

Field	Action
Ethernet option	<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>
Customer traffic type	<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 ID selection	<p>Indicate how the VLAN ID is determined.</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.</p>
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 (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	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	<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>
Calculation of Burst-Size	

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 1. 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 checkbox.</p>

The following illustration shows the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.

Calculation of Burst-Size

Calculate Burst Size: Line Rate Based

Burst Period (ms):

☐ Editable in Service Order

Bandwidth Settings

Enable 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 not available in the service definition when QoS Design software is installed.</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>

Field	Action
Max Bandwidth (Mbps)	<p>Specify the maximum bandwidth value in Mbps. For more information on maximum bandwidth see Table 14 on page 221</p> <p>Default: 100 Mbps</p> <p>Range: 1 Mbps through 100,000 Mbps/100Gbps</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>

2. Click **Next** to continue with connectivity settings.

UNI 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 **UNI Settings** window.

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>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 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>
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 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	<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 that the service provisioner can type.</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 1. • 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 checkbox.</p>

Field	Action
-------	--------

The following illustration shows the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.

Calculation of Burst-Size

Calculate Burst Size:

Line Rate Based

▼

Burst Period (ms):

1

☐ Editable in Service Order

Bandwidth Settings

Enable 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 not available in the service definition when QoS Design software is installed.</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 14 on page 221</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 100000 Kbps</p>

2. 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.

To specify the UNI Settings for q-in-q interfaces:

1. Fill in the fields on the **UNI Settings** window.

Field	Action
Traffic Treatment Settings	
Ethernet option	Select asymmetric tag depth from the list.
Customer traffic type	<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>
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>
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 (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>
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	<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 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.

Field	Action
MTU Settings	<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>

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 1. 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 checkbox.</p>
-----------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The following illustration shows the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.

Calculation of Burst-Size

Calculate Burst Size: Line Rate Based

Burst Period (ms):

☐ Editable in Service Order

Bandwidth Settings

Enable 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 not available in the service definition when QoS Design software is installed.</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 14 on page 221 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

2. Click **Next** to continue with Connectivity settings.

Specifying Connectivity and MAC Security Information

In this step, you specify the attributes that define the connectivity among remote sites across the service provider network and the service security. The following is a sample **Connectivity** window.

Connectivity

Connectivity Settings

Route target:
Route distinguisher:
VLAN normalization:
☒ Allow Multihoming

☐ Editable in Service Order
☐ Editable in Service Order

LDP PW Extension Settings

VCID:

☐ Editable in Service Order

MAC Security Settings

☒ MAC learning
Interface MAC limit:
☐ MAC statistics
MAC table size:

☐ Editable in Service Order
☐ Editable in Service Order
☐ Editable in Service Order
☐ Editable in Service Order

To specify connectivity between sites across the network:

1. Fill in the fields in the **Connectivity** window.

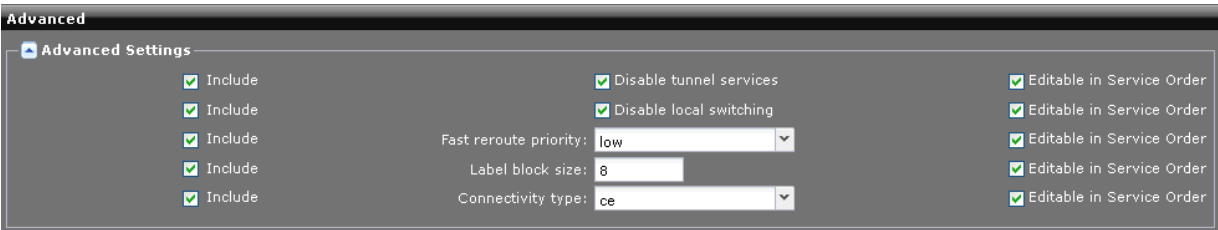
Field	Action
Route target	<p>Choose one of the following options from the list:</p> <ul style="list-style-type: none"> • Auto pick • Select manually
Route distinguisher	<p>Select a route distinguisher option:</p> <ul style="list-style-type: none"> • Select manually—The service provider specifies the route distinguisher. • Auto pick—The route distinguisher is selected automatically. <p>To override this setting in the service order, select the Editable in Service Order check box.</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. NOTE: For services that transport a range of VLAN IDs, you must set VLAN Normalization to all. You cannot transport a range of VLAN IDs without normalization. • 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 each endpoint. • 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>For more information about VLAN normalization, see “Junos Space Layer 2 Services Overview” on page 142.</p> <p>For information about VLAN manipulation, see “Understanding VLAN Manipulation (Normalization and VLAN Mapping) on Ethernet Services” on page 710.</p>
Allow Multihoming	<p>This check box is available only if the signaling type is BGP. To enable a service provisioner to define primary and backup PE devices in a multihomed group that serves as a single customer site, select Allow Multihoming.</p>

Field	Action
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 selected for 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 when the signaling type is BGP.</p> <p>If you select the Auto Discovery check box, the following fields are available:</p> <ul style="list-style-type: none"> • Route target • Route distinguisher • VPN ID <p>If you disable the Auto Discovery check box, specify the VPLS ID.</p>
VPLS 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.</p> <ul style="list-style-type: none"> • Autopick • Select manually
VPN ID	<p>This field is available only if the signaling type is LDP and auto discovery is enabled.</p> <p>Identifies the VPN ID associated with the router.</p> <ul style="list-style-type: none"> • Autopick • Select manually
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.
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>

2. Click **Next** to save the connectivity settings. [“Specifying Advanced Settings” on page 235](#)

Specifying Advanced Settings

In this step, you can specify the parameters that define advanced connectivity between sites across the service provider network. The following illustration shows the **Advanced** window.



To specify advanced settings:

1. Fill in the fields as indicated in the table.

Field	Action
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).

Field	Action
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 the fast-reroute-priority, 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 is enabled.</p>
Connectivity type	<p>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):</p> <ul style="list-style-type: none"> • 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. <p>NOTE: This field is unavailable if the Signaling type is LDP and the Auto discovery is enabled.</p>

Field	Action
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 **Finish** to save the advanced settings.

The service definition is complete.

RELATED DOCUMENTATION

[Publishing a Custom Service Definition | 308](#)

[Predefined Multipoint-to-Multipoint Ethernet Service Definitions | 521](#)

[Viewing Service Definitions | 267](#)

[Creating an E-Line Service Definition | 188](#)

[Creating a Point-to-Multipoint VPLS Service Definition | 237](#)

Creating a Point-to-Multipoint VPLS Service Definition

IN THIS SECTION

- [Specifying General Information for Point-to-Multipoint VPLS Service Definitions | 340](#)
- [Specifying UNI Settings | 344](#)
- [Specifying Connectivity and MAC Security Information | 363](#)
- [Specifying Advanced Settings | 367](#)

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

In the Network Activate task pane, select **Service Design > Manage Service Definitions > Create VPLS Service Definition**. The **General** settings window appears.

General

Name:

P-MP-VPLS-SD

Service type:

Point-to-Multipoint Ethernet (VPLS)

Signaling:

LDP

Comments:

Service Template:

Flexi_Temp_Inner_Outer×

Flexi_Temp×

×

Service_template×

Default Service Template:

Flexi_Temp_Inner_Outer×

×

Threshold alarm profile:

Please select ...

☒ Enable L3 Access

☒ Enable PW Extension

☒ Enable PW Resiliency

☒ Enable Static PW Labels

To specify the general information for a point-to-multipoint service definition:

1. Fill in the fields in the **General** window.

Field	Action
Name	Type a name for the service definition.
Service type	Select Point-to-Multipoint Ethernet (VPLS)

Field	Action
Signaling	<p>Select signaling type:</p> <ul style="list-style-type: none"> • BGP— If BGP signaling is selected, the following fields are available in the connectivity window: <ul style="list-style-type: none"> • Route target • Route distinguisher • VLAN normalization • Allow Multihoming • Mac Security Settings • VCID, if Enable PW Extension is enabled • LDP—If LDP signaling is selected, the following fields are available in the connectivity window: <ul style="list-style-type: none"> • Auto Discovery • Route target, if Auto Discovery is enabled • Route distinguisher, if Auto Discovery is enabled • VPLS ID, if Auto Discovery is disabled • VPN ID, if Auto Discovery is enabled • VLAN normalization • Mac Security Settings <p>NOTE: The Signaling is not editable in the service order.</p>
Comments (Optional)	Type a brief description or other comment that you want to appear in the Service Definition table.
Enable QoS	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.
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 UNI 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.

Field	Action
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 165.</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 checkbox enables the Enable PW Resiliency checkbox and automatically selects the Enable PW Extension checkbox.</p>
Service Template Definition	<p>(Optional) To include a service template for the service, select a service template from the Service Template list.</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 116.</p>

2. Click **Next** to save the information. Continue with [“Specifying UNI Settings” on page 242](#).

SEE ALSO

[Service Templates Overview | 113](#)

[Creating a Service Template | 116](#)

[Importing a Service Template | 125](#)

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 ports, 802.1Q interfaces, or Q-in-Q interfaces:

- [Specifying UNI Settings for Port-to-Port Services | 344](#)
- [Specifying UNI Settings for Services with 802.1Q Interface Types | 348](#)
- [Specifying UNI Settings for Services with Q-in-Q Interface Types | 353](#)
- [Specifying UNI Settings for Services with Flexible VLAN Tagging \(Asymmetric Interface Types\) | 358](#)

Specifying UNI Settings for Port-to-Port Services

NOTE: You can select the port-port option only for services that are not normalized. That is, you must select **Not Normalized** when specifying the connectivity.

The screenshot displays the 'UNI Settings' configuration window. It is organized into several sections, each with expandable/collapsible icons on the left:

- Traffic Treatment:**
 - Ethernet option:
 - Customer traffic type:
 - VLAN ID selection:
 - ☐ Editable in Service Order
 - VLAN range for auto-pick:
 - VLAN range for manual input:
 - Outer Tag protocol ID:
 - Inner Tag protocol ID:
 - ☐ Editable in Service Order
- Interface Settings:**
 - Physical IF encapsulation:
 - Logical IF encapsulation:
- LDP PW Extension Settings:**
 - Physical IF encapsulation:
 - Logical IF encapsulation:
- MTU Settings:**
 - Default MTU (Bytes):
 - MTU range (Bytes):
 - ☐ Editable in Service Order
- Calculation of Burst-Size:** (This section is partially visible at the bottom)

To set UNI attributes for port UNIs:

1. Fill in the fields as indicated in the table.

Field	Action
Traffic Treatment Settings	
Ethernet option	<p>Select port-port from the drop-down 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	The VLAN ID cannot be selected. 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 MTU setting, select the check box.
Interface Settings	
Physical IF encapsulation	<p>In the Physical IF encapsulation box, select ethernet-vpls, which is the only valid physical interface encapsulation method for port-to-port services.</p> <p>The Logical IF encapsulation field cannot be selected because it is not relevant to port-to-port services.</p>
Logical IF encapsulation	You cannot select a choice in this field because it is not relevant to port-to-port services.
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 window.</p>	
Physical IF 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 IF encapsulation	You can not select a choice in this field because it is not relevant to port-to-port services.
MTU Settings	In the MTU range boxes, type the lowest and highest values for MTU that the service provisioner can type.
Calculation of Burst-Size	

Field	Action
Calculate Burst Size	<p>Select the preferred option for calculating the burst size:</p> <ul style="list-style-type: none"> MTU Based <p>If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902.</p> <p>The default value for MTU Factor is 1.</p> Line Rate Based <p>If you select the option Line Rate Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds.</p> <p>The default value for Burst Period is 1.</p> <p>NOTE: The Calculate Burst Size list is enabled only when you select the Enable rate limiting checkbox.</p>

The following illustration shows the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.

Bandwidth Settings

The following illustration shows the **Bandwidth Settings** panel, which appears if you do not select the **Enable QoS** check box in the preceding **General** settings window.

Enable 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 not available in the service definition when QoS Design software is installed.</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 15 on page 245 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

The following table lists the **Max Bandwidth (Mbps)** for the M Series, MX Series, and ACX Series Routers:

Table 19: 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 **Next** to save the UNI settings. Continue with [“Specifying Connectivity and MAC Security Information” on page 261](#).

Specifying UNI Settings for Services with 802.1Q Interface Types

UNI Settings

▲ Traffic Treatment

Ethernet option:

dot1q

Customer traffic type:

Transport single vlan

VLAN ID selection:

Auto pick

Editable in Service Order

VLAN range for auto-pick:

1

4094

VLAN range for manual input:

Outer Tag protocol ID:

0x88a8

Editable in Service Order

Inner Tag protocol ID:

Please select ...

Editable in Service Order

▲ Interface Settings

Physical IF encapsulation:

flexible-ethernet-services

Logical IF encapsulation:

vlan-vpls

▲ LDP PW Extension Settings

Physical IF encapsulation:

vlan-ccc

Logical IF encapsulation:

vlan-ccc

▲ MTU Settings

Default MTU (Bytes):

1522

Editable in Service Order

MTU range (Bytes):

1522

9192

▲ Calculation of Burst-Size

To set UNI attributes for 802.1Q interfaces:

- 1. Fill in the fields as indicated in the table.

Field	Action
Traffic Treatment Settings	
Ethernet option	<div>Select dot1q from the drop-down list.</div> <div>The Ethernet option you choose determines the other options you can select and specify on the page.</div>

Field	Action
Customer traffic type	<p>Select a traffic type to restrict the traffic that can be transported across the network for the service:</p> <ul style="list-style-type: none"> • Select Transport single vlan to transport the traffic for a specific VLAN across the network. Single VLAN is the only option for 802.1Q interface types. You need to specify the Outer Tag protocol ID. <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> <ul style="list-style-type: none"> • Select Transport vlan range to transport the traffic for a range of VLANs across the network. <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>In the VLAN ID selection box, specify how the VLAN ID is determined:</p> <ul style="list-style-type: none"> • To allow the service provider to specify the VLAN ID, choose Select manually. This option is used typically when no VLAN normalization is applied. <p>Specify the VLAN ID range in VLAN range for manual input.</p> <p>Range: 1 through 4094</p> <p>To enable the service provisioner to override this setting, select Editable in Service Order.</p> <ul style="list-style-type: none"> • To cause the VLAN ID to be selected automatically from the VLAN ID pool, select Auto pick. This option is used typically when VLAN normalization is applied. <p>Specify the VLAN ID pool in VLAN range for auto-pick</p> <p>Range: 1 through 4094</p> <p>To enable the service provisioner to override this setting in a service order, select Editable in Service Order.</p> <p>To enable the service provisioner to override this setting in a service order, select Editable in Service Order.</p>
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 (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	To allow the service provisioner to override the MTU setting, select the check box for those options.

Interface Settings

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 window.

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
----------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Field	Action
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>
MTU Settings	<p>In the Default MTU box, specify the MTU for each UNI.</p> <p>To allow the service provisioner to override the MTU setting, select Editable in Service Order and, in the MTU range boxes, type the highest and lowest MTU values that the service provisioner can type.</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 <p>If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902.</p> <p>The default value for MTU Factor is 1.</p> Line Rate Based <p>If you select the option Line Rate Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds.</p> <p>The default value for Burst Period is 1.</p> <p>NOTE: The Calculate Burst Size list is enabled only when you select the Enable rate limiting checkbox.</p>
-----------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The following illustration shows the appearance of the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.

The screenshot shows a panel titled "Calculation of Burst-Size". Inside the panel, there is a label "Calculate Burst Size:" followed by a dropdown menu with "Line Rate Based" selected. Below this, there is a label "Burst Period (ms):" followed by a text input field containing the value "1". To the right of the input field is a checkbox labeled "Editable in Service Order", which is currently unchecked.

Bandwidth Settings

Field	Action
-------	--------

The following illustration shows the Bandwidth Settings panel, which appears if you do not select the **Enable QoS** check box in the preceding **General** settings window.

Bandwidth Settings

☒ Enable rate limiting

☒ Editable in Service Order

Default bandwidth (Mbps):

10

Min Bandwidth (Kbps):

1000

Max Bandwidth (Mbps):

100

Increment (Kbps):

1000

Enable 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 not available in the service definition when QoS Design software is installed.</p>
Default bandwidth (Mbps)	<p>Specify the default bandwidth value in Mbps.</p> <p>Default: 10 Mbps</p> <p>Range: 1 Mbps through 100000 Mbps</p>
Min Bandwidth (Kbps)	<p>Specify the minimum bandwidth value in Kbps.</p> <p>Default: 1000 Kbps</p> <p>Range: 64 Kbps through 100000 Kbps</p>
Max Bandwidth (Mbps)	<p>Specify the maximum bandwidth value in Mbps. For more information on maximum bandwidth see Table 15 on page 245</p> <p>Default: 100 Mbps</p> <p>Range: 1 Mbps through 100000 Mbps/100Gbps</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 100000 Kbps</p>

2. Click **Next** to save the UNI settings. Continue with [“Specifying Connectivity and MAC Security Information” on page 261.](#)

Specifying UNI Settings for Services with Q-in-Q Interface Types

UNI Settings

▲ Traffic Treatment

Ethernet option:

qinq

Customer traffic type:

Transport vlan range

VLAN ID selection:

Auto pick

Editable in Service Order

VLAN range for auto-pick:

1

4094

VLAN range for manual input:

Outer Tag protocol ID:

0x88a8

Editable in Service Order

Inner Tag protocol ID:

0x8100

Editable in Service Order

▲ Interface Settings

Physical IF encapsulation:

flexible-ethernet-services

Logical IF encapsulation:

vlan-vpls

▲ LDP PW Extension Settings

Physical IF encapsulation:

vlan-ccc

Logical IF encapsulation:

vlan-ccc

▲ MTU Settings

Default MTU (Bytes):

1522

Editable in Service Order

MTU range (Bytes):

1522

9192

▲ Calculation of Burst-Size

To set UNI attributes for Q-in-Q interfaces:

1. Fill in the fields as indicated in the table.

Field	Action
Traffic Treatment Settings	
Ethernet option	Select qinq from the drop-down list. The window expands to include options specific to Q-in-Q interfaces.

Field	Action
Customer traffic type	<p>In the Customer traffic type box:</p> <ul style="list-style-type: none"> • Select Transport all traffic to transport the traffic from all VLANs across the network. You need to specify only the Outer Tag protocol ID. <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.</p> <ul style="list-style-type: none"> • Select Transport single vlan to transport the traffic for a specific VLAN across the network. Single VLAN is the only option for 802.1Q interface types. You need to specify the Outer Tag protocol ID and the Inner Tag protocol ID. • Select Transport vlan range to limit the traffic across the network to a specific range of VLANs. <p>If you select this option, the service provisioner will be prompted for the VLAN-ID range when creating a service order based on this service definition. You need to specify the Outer Tag protocol ID and the Inner Tag protocol ID.</p>
VLAN ID selection	<p>In the VLAN ID selection box, specify how the service VLAN ID is set during service order creation:</p> <ul style="list-style-type: none"> • To cause the provisioning software to automatically select the service VLAN ID from the VLAN ID pool, select Auto pick. This option is used typically when no VLAN normalization is applied. <p>Specify the VLAN ID pool in VLAN range for auto-pick Range: 1 through 4094</p> <ul style="list-style-type: none"> • To allow the service provisioner to specify the service VLAN ID, choose Select manually. This option is used typically when VLAN normalization is applied. <p>Specify the VLAN ID range in VLAN range for manual input. Range: 1 through 4094</p> <p>To enable the service provisioner to override this setting, select the Editable in Service Order check box.</p>
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 (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>
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 MTU setting, select the check box for those options.

Interface Settings

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 Q-in-Q interfaces, the only option is flexible-ethernet-services .
Logical IF encapsulation	The Logical IF encapsulation field is constrained by your selection in the Physical Interface 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 window.

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>
MTU Settings	<p>In the Default MTU box, specify the MTU for each UNI.</p> <p>To allow the service provisioner to override the MTU setting, select the Editable in Service Order check box and, in the MTU range boxes, type the lowest and highest values for the MTU that the service provisioner can type.</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 <p>If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902.</p> <p>The default value for MTU Factor is 1.</p> • Line Rate Based <p>If you select the option Line Rate Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds.</p> <p>The default value for Burst Period is 1.</p> <p>NOTE: The Calculate Burst Size list is enabled only when you select the Enable rate limiting checkbox.</p>
-----------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The following illustration shows the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.

The screenshot shows a configuration panel titled "Calculation of Burst-Size". Inside the panel, there is a label "Calculate Burst Size:" followed by a dropdown menu currently showing "Line Rate Based". Below this, there is a label "Burst Period (ms):" followed by a text input field containing the number "1". To the right of the input field is an unchecked checkbox labeled "Editable in Service Order".

Bandwidth Settings

Field	Action
-------	--------

The following illustration shows the Bandwidth Settings panel, which appears if you do not select the **Enable QoS** check box in the preceding **General** settings window.

Enable 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 not available in the service definition when QoS Design software is installed.</p>
Default bandwidth (Mbps)	<p>Specify the default bandwidth value in Mbps.</p> <p>Default: 10 Mbps</p> <p>Range: 1 Mbps through 100000 Mbps</p>
Min Bandwidth (Kbps)	<p>Specify the minimum bandwidth value in Kbps.</p> <p>Default: 1000 Kbps</p> <p>Range: 64 Kbps through 100000 Kbps</p>
Max Bandwidth (Mbps)	<p>Specify the maximum bandwidth value in Mbps. For more information on maximum bandwidth see Table 15 on page 245</p> <p>Default: 100 Mbps</p> <p>Range: 1 Mbps through 100000 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 100000 Kbps</p>

- Click **Next** to save the UNI settings. Continue with [“Specifying Connectivity and MAC Security Information” on page 261.](#)

Specifying 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.

UNI Settings

Traffic Treatment

Ethernet option: asymmetric tag depth

Customer traffic type: Transport single vlan

VLAN ID selection: Auto pick

VLAN range for auto-pick: 1

VLAN range for manual input:

Outer Tag protocol ID: 0x8100

Inner Tag protocol ID: 0x88a8

Editable in Service Order

Editable in Service Order

Editable in Service Order

Interface Settings

Physical IF encapsulation: flexible-ethernet-services

Logical IF encapsulation: vlan-vpls

LDP PW Extension Settings

Physical IF encapsulation: vlan-ccc

Logical IF encapsulation: vlan-ccc

MTU Settings

Default MTU (Bytes): 1522

MTU range (Bytes): 1522

Editable in Service Order

9192

Calculation of Burst-Size

To set UNI attributes for asymmetric interfaces:

1. Fill in the fields as indicated in the table.

Field	Action
Traffic Treatment Settings	
Ethernet option	Select asymmetric tag depth from the drop-down list.

Field	Action
Customer traffic type	<p>In the Customer traffic type box:</p> <ul style="list-style-type: none"> • Select Transport all traffic to transport the traffic from all VLANs across the network. You need to Specify only the Outer Tag protocol ID. <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.</p> <ul style="list-style-type: none"> • Select Transport single vlan to transport the traffic for a specific VLAN across the network. Single VLAN is the only option for 802.1Q interface types. You need to specify the Outer Tag protocol ID and the Inner Tag protocol ID. • Select Transport vlan range to limit the traffic across the network to a specific range of VLANs. <p>If you select this option, the service provisioner will be prompted for the VLAN-ID range when creating a service order based on this service definition. You need to specify the Outer Tag protocol ID and the Inner Tag protocol ID.</p>
VLAN ID selection	<p>In the VLAN ID selection box, specify how the service VLAN ID is set during service order creation:</p> <ul style="list-style-type: none"> • To cause the provisioning software to automatically select the service VLAN ID from the VLAN ID pool, select Auto pick. This option is used typically when no VLAN normalization is applied. <p>Specify the VLAN ID pool in VLAN range for auto-pick Range: 1 through 4094</p> <ul style="list-style-type: none"> • To allow the service provisioner to specify the service VLAN ID, choose Select manually. This option is used typically when VLAN normalization is applied. <p>Specify the VLAN ID range in VLAN range for manual input. Range: 1 through 4094</p> <p>To enable the service provisioner to override this setting, select the Editable in Service Order check box.</p>
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 (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>
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	<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 IF encapsulation	The Logical IF encapsulation field is constrained by your selection in the Physical Interface Encapsulation field. For the physical encapsulation mode of flexible-ethernet-services, your only option is to select vlan-vpls for the logical encapsulation method.

Field	Action
-------	--------

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 window.

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>
MTU Settings	<p>In the Default MTU box, specify the MTU for each UNI.</p> <p>To allow the service provisioner to override the MTU setting, select the Editable in Service Order check box and, in the MTU range boxes, type the lowest and highest values for the MTU that the service provisioner can type.</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 <p>If you select the option MTU Based, you can specify a value for MTU Factor in the range 1 through 1087902.</p> <p>The default value for MTU Factor is 1.</p> • Line Rate Based <p>If you select the option Line Rate Based, you can specify a value for Burst Period in the range 1 through 7450 milliseconds.</p> <p>The default value for Burst Period is 1.</p> <p>NOTE: The Calculate Burst Size list is enabled only when you select the Enable rate limiting checkbox.</p>
-----------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Field	Action
-------	--------

The following illustration shows the **Calculate Burst-Size** panel parameters if you select the **Line Rate Based** option.

Calculation of Burst-Size

Calculate Burst Size:

Line Rate Based

Burst Period (ms):

1

☐ Editable in Service Order

Bandwidth Settings

The following illustration shows the Bandwidth Settings panel, which appears if you do not select the **Enable QoS** check box in the preceding **General** settings window.

Bandwidth Settings

☒ Enable rate limiting

Default bandwidth (Mbps):

10

Min Bandwidth (Kbps):

1000

Max Bandwidth (Mbps):

100

Increment (Kbps):

1000

☒ Editable in Service Order

Enable 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 not available in the service definition when QoS Design software is installed.</p>
Default bandwidth (Mbps)	<p>Specify the default bandwidth value in Mbps.</p> <p>Default: 10 Mbps</p> <p>Range: 1 Mbps through 100000 Mbps</p>
Min Bandwidth (Kbps)	<p>Specify the minimum bandwidth value in Kbps.</p> <p>Default: 1000 Kbps</p> <p>Range: 64 Kbps through 100000 Kbps</p>
Max Bandwidth (Mbps)	<p>Specify the maximum bandwidth value in Mbps. For more information on maximum bandwidth see Table 15 on page 245</p> <p>Default: 100 Mbps</p> <p>Range: 1 Mbps through 100000 Mbps</p>

Field	Action
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 100000 Kbps

- Click **Next** to save the UNI settings. Continue with [“Specifying Connectivity and MAC Security Information” on page 261.](#)

Specifying Connectivity and MAC Security Information

In this step, you specify the attributes that define the connectivity among remote sites across the service provider network and the service security. The following is a sample **Connectivity** window.

Connectivity

Connectivity Settings

Route target:
Route distinguisher:
VLAN normalization:
☒ Allow Multihoming

☐ Editable in Service Order
☐ Editable in Service Order

LDP PW Extension Settings

VCID:

☐ Editable in Service Order

Revert time (sec):
Switch Over Delay (sec):

☐ Editable in Service Order
☐ Editable in Service Order

MAC Security Settings

☒ MAC learning
Interface MAC limit:
☐ MAC statistics
MAC table size:

☐ Editable in Service Order
☐ Editable in Service Order
☐ Editable in Service Order
☐ Editable in Service Order

To configure connectivity between sites across the network:

1. Fill in the fields in the **Connectivity** window.

Field	Action
Route target	<p>Choose one of the following options from the list:</p> <ul style="list-style-type: none"> • Auto pick • Select manually <p>This field is available in either of the following cases:</p> <ul style="list-style-type: none"> • The Signaling type is BGP. • The Signaling type is LDP and Auto Discovery is enabled.
Route distinguisher	<p>Select a route distinguisher option:</p> <ul style="list-style-type: none"> • Select manually—The service provider specifies the route distinguisher. • Auto pick—The route distinguisher is selected automatically. <p>To override this setting in the service order, select the Editable in Service Order check box.</p> <p>This field is available in either of the following cases:</p> <ul style="list-style-type: none"> • The Signaling type is BGP. • The Signaling type is LDP and Auto Discovery is enabled.
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. NOTE: For services that transport a range of VLAN IDs, you must set VLAN Normalization to all. You cannot transport a range of VLAN IDs without normalization. • 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 each endpoint • 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>For more information about VLAN normalization, see “Junos Space Layer 2 Services Overview” on page 142.</p> <p>For information about VLAN manipulation, see “Understanding VLAN Manipulation (Normalization and VLAN Mapping) on Ethernet Services” on page 710.</p>

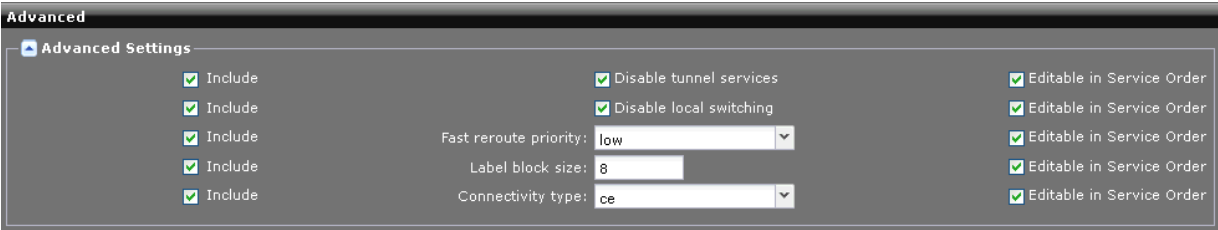
Field	Action
Allow Multihoming	This check box is available only if the signaling type is BGP. To enable a service provisioner to define primary and backup PE devices in a multihomed group that serves a single customer site, select Allow Multihoming .
Auto Discovery	<p>You cannot enable or disable the 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 checkbox in the General window is checked for the LDP signaling, then the Auto Discovery checkbox is disabled in the Connectivity Settings page.</p> <p>The Auto Discovery checkbox is not available on 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>
VPLS 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.</p> <ul style="list-style-type: none"> • Autopick • Select manually
VPN ID	<p>This field is available only if the signaling type is LDP and auto discovery is enabled.</p> <p>Identifies the VPN ID associated with the router.</p> <ul style="list-style-type: none"> • Autopick • Select manually
Revert time (sec)	<p>This field is available only if the Enable PW Resiliency is enabled.</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>

Field	Action
Switch Over Delay (sec)	<p>This field is available only if the Enable PW Resiliency is enabled.</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>
VCID	<p>This field is available only if the Service type is point-to-multipoint, the Signaling is BGP, and the Enable PW Extension is enabled.</p> <p>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.</p>
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.
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>

2. Click **Next** to save the connectivity settings and continue with [“Specifying Advanced Settings” on page 235.](#)

Specifying Advanced Settings

In this step, you can specify the parameters that define advanced connectivity between sites across the service provider network. The following illustration shows the **Advanced** window.



To specify advanced settings:

1. Fill in the fields as indicated in the table.

Field	Action
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).

Field	Action
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 the fast-reroute-priority, 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 is enabled.</p>
Connectivity type	<p>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):</p> <ul style="list-style-type: none"> • 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. <p>NOTE: This field is unavailable if the Signaling type is LDP and the Auto discovery is enabled.</p>

Field	Action
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 **Finish** to save the advanced settings.

The service definition is complete.

RELATED DOCUMENTATION

[Publishing a Custom Service Definition | 308](#)

[Predefined Point-to-Multipoint Ethernet Service Definitions | 554](#)

[Viewing Service Definitions | 267](#)

[Creating an E-Line Service Definition | 188](#)

[Creating a Multipoint-to-Multipoint VPLS Service Definition | 214](#)

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 Activate** task pane, select **Service Design** > **Manage Service Definitions** > **Create VPLS Service Definition**.

General

Name:

VPLS-MP-MP-SD

Service type:

Multipoint-to-Multipoint Ethernet (VPLS)

Signaling:

BGP

Comments:

Service Template:

Please select ...

☒ Enable QoS

☒ Enable L3 Access

Field	Action
Name	Provide a name for the VPLS service definition you want to create.
Service Type	<div>Select the type of service from the menu list. To create the VPLS into Layer 3 service, use either of the following service type:</div> <div><div>• Multipoint-to-Multipoint Ethernet (VPLS)</div><div>• Point-to-Multipoint Ethernet (VPLS)</div></div>
Comments	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.

1. Click **Next** to display the next screen, **UNI Settings**, and continue creating the service definition.

Specifying UNI Settings

UNI Settings

Traffic Treatment

Ethernet option: dot1q

Customer traffic type: Transport single vlan

VLAN ID selection: Select manually Editable in Service Order

Pick VLAN within this range:

Interface Settings

Physical IF encapsulation: flexible-ethernet-services

Logical IF encapsulation: vlan-vpls

MTU Settings

Default MTU (Bytes): 1522 Editable in Service Order

MTU range (Bytes): 1522 9192

UNI Settings Field	Action
Traffic Treatment Settings	
Ethernet option	Indicate the Ethernet option to use for this VPLS service definition. Choices are qinq or dot1q .
Customer traffic type	The only option for VPLS service definitions is Transport single VLAN .
VLAN ID selection	The only option for VPLS service definitions is Select manually .
Interface Settings	
Physical IF encapsulation	The only option for VPLS service definitions is flexible-ethernet-services
Logical IF encapsulation	The only option for VPLS service definitions is vlan-vpls .
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.

1. Click **Next** to continue creating the VPLS service definition and specify the connectivity settings.

Specifying Connectivity Settings

Connectivity Settings Field	Action
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.
VLAN normalization	All VPLS service definitions require VLAN normalization.
Allow Multihoming	If you are using multihoming features, check the box.
MAC Security 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 **Finish** to see the service definition inventory list.

Service Design > **Manage Service Definitions**

Search:

Actions ▾

Name	State	Service Type	Signaling	Created By	Created Date ▾
testhsnew	→ Published	VPLS (Point-MultiPoint)	BGP	super	Nov 2, 2012 10:01:04 AM EDT
vpls11_HS	→ Published	VPLS (MultiPoint-MultiPoint)	BGP	super	Nov 2, 2012 9:55:52 AM EDT
VPLS10	→ Published	VPLS (MultiPoint-MultiPoint)	BGP	super	Nov 2, 2012 9:53:47 AM EDT
TestAsymtagde...	→ Published	VPLS (MultiPoint-MultiPoint)	BGP	super	Nov 2, 2012 9:25:04 AM EDT
LDP_qinq_ext-vlanccc	→ Published	Point-to-Point Pseudowire	LDP	super	Nov 2, 2012 7:40:15 AM EDT
LDP_portbased	→ Published	Point-to-Point Pseudowire	LDP	super	Nov 2, 2012 7:35:16 AM EDT
ldp_dot1q	→ Published	Point-to-Point Pseudowire	LDP	super	Nov 2, 2012 6:36:16 AM EDT
HS_Advanced	→ Published	VPLS (Point-MultiPoint)	BGP	super	Nov 2, 2012 6:29:58 AM EDT
LDP_qinq_red_...	→ Published	Point-to-Point Pseudowire	LDP	super	Nov 2, 2012 6:15:16 AM EDT
multihome3	→ Published	VPLS (MultiPoint-MultiPoint)	BGP	super	Nov 2, 2012 5:36:35 AM EDT
multihome2	→ Published	VPLS (MultiPoint-MultiPoint)	LDP	super	Nov 2, 2012 5:33:34 AM EDT
UD SD BGP do...	→ Published	Point-to-Point	BGP	super	Nov 2, 2012

Page 1 of 2 | Displaying 1 - 30 of 58 | Show 30 items

2. Click on the unpublished service definition you just created.
3. Right-click on the selected service definition to choose publishing options.

Service Design > **Manage Service Definitions**

Search Actions

Name	State	Service Type	Signaling
testDef	Unpublished	VPLS (MultiPoint-MultiPoint)	BGP
test2P2P		Point-to-Point Pseudowire	LDP
testP2P		Point-to-Point Pseudowire	LDP
ddd		Point-to-Point Pseudowire	LDP
mySD		Point-to-Point Pseudowire	LDP
MPMP_BGP_SD		VPLS (MultiPoint-MultiPoint)	BGP
P2P_LDP_PW_Resiliency_		Point-to-Point Pseudowire	LDP
TDM		Point-to-Point Pseudowire	LDP
p2p_ldp_atm_pw	Published	Point-to-Point Pseudowire	LDP
l3vpn_test	Published	L3 VPN (Full Mesh)	
p2p_test	Published	Point-to-Point Pseudowire	LDP
user_def	Published	L3 VPN (Full Mesh)	
l3vpn_def	Published	L3 VPN (Full Mesh)	
ServicePw_def	Published	Point-to-Point Pseudowire	LDP
LDP_L3Access	Published	VPLS (Point-MultiPoint)	LDP
l3vpn_ldf_pw_ext	Published	VPLS (Point-MultiPoint)	LDP
bgpdef	Published	Point-to-Point Pseudowire	BGP
VPLS_BGP_PW_EXT	Published	VPLS (Point-MultiPoint)	BGP
VPLS_LDP_PW_EXT	Published	VPLS (Point-MultiPoint)	LDP

Page 1 of 2 | Displaying 1 - 30 of 55 | Show 30 items

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 Activate** task pane, select **Service Provisioning**.

RELATED DOCUMENTATION

- [Seamless MPLS Support in Junos Space Overview | 708](#)
- [Creating a Service Order for VPLS Access into Layer 3 Networks | 698](#)

Layer 3 VPN Service Definitions

IN THIS CHAPTER

- [Creating a Full Mesh Layer 3 VPN Service Definition | 376](#)
- [Creating a Hub-and-Spoke \(One Interface\) Layer 3 VPN Service Definition | 386](#)
- [Creating a Service Definition for Point-to-Point Pseudowire Access into a Layer 3 VPN | 395](#)
- [Creating a Layer 3 VPN Service Definition in Cross Provisioning Platform for Third-Party Devices | 400](#)
- [Creating a Multicast VPN Service Definition | 404](#)

Creating a Full Mesh Layer 3 VPN Service Definition

This procedure provides the steps to create a definition for a full mesh Layer 3 VPN Ethernet service.

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.

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 full mesh Ethernet services on the network.

The screens 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 full mesh Layer 3 VPN service definition:

1. [Specifying General Information | 376](#)
2. [Specifying UNI Settings | 378](#)
3. [Specifying Connectivity Information | 382](#)

Specifying General Information

In the **Network Activate** task pane, select **Service Design > Manage Service Definitions > Create L3 VPN Service Definition**.

The **Create Service Definition** window appears.

To specify general information for a full mesh service definition:

The screenshot shows the 'General' tab of a configuration window. It contains the following elements:

- Name:** A text input field containing 'SD-L3VPN-Fullmesh'.
- Service type:** A dropdown menu with 'L3 VPN (Full Mesh)' selected.
- Comments:** A large text area for entering comments.
- Service Template:** A dropdown menu with 'Please select ...' as the current selection.
- Checkboxes:** Three checkboxes are located below the service template:
 - ☒ **Enable MVPN**
 - ☒ **Enable QoS**
 - ☒ **Decouple Service Status From Port Status**

1. Fill in the fields on the General page as indicated in the following table:

Field	Action
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) .
Comments	Type a comment that identifies or describes the definition. Range: 1 through 200 characters
Decouple Service Status From Port Status	Select this check box to isolate the events related to an interface in OpenNMS. NOTE: When you select this check box, only the MPLS traps are monitored, not the jnxVpnIfVpn traps. By default, all events are saved in the OpenNMS database.
Enable QoS	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 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. NOTE: The Enable QoS check box appears only if you have installed the QoS Design application.

Field	Action
Service Template	<p>(Optional) To include a service template for the service, select a service template from the Service Template list.</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 116.</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 page information. Continue with [“Specifying UNI Settings” on page 378](#).

Specifying UNI Settings

To provide the UNI service attributes for this service definition:

UNI Settings

Interface Settings

☒ Ethernet

VLAN ID selection: Auto pick

VLAN range for auto-pick:

VLAN range for manual input:

☐ Editable in Service Order

MTU Settings

Default MTU (Bytes): 1522

MTU range (Bytes): 1522

☐ Editable in Service Order

9192

Bandwidth Settings

☒ Enable rate limiting

Default bandwidth (Mbps): 10

Min Bandwidth (Kbps): 1000

Max Bandwidth (Mbps): 100

Increment (Kbps): 1000

☒ Editable in Service Order

Calculation of Burst-Size

Calculate Burst Size: MTU Based

MTU Factor: 10

☒ Editable in Service Order

1. Fill in the fields on the UNI Settings page as indicated in the following table:

Field	Action
Ethernet	By default, this check box is unavailable.
VLAN ID selection	<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, choose Select manually. Specify the range in VLAN range for manual input. To cause the VLAN ID to be selected automatically from the VLAN ID pool, select Auto pick. This option is used typically when VLAN normalization is applied. Specify the range in VLAN range for auto-pick <p>NOTE: Select the Editable in Service Order check box if you want to override the VLAN ID selection setting in the service order.</p>
VLAN range for auto-pick	<p>Specify the range.</p> <p>Range: 1 through 4094</p>

Field	Action
VLAN range for manual input	<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>
Default MTU (Bytes)	<p>Specify an MTU value in this field.</p> <p>To see the permitted range for the MTU value, select the Editable in Service Order check box.</p> <p>Default: 1522 bytes</p> <p>Range: 1522 bytes through 9192 bytes</p> <p>For a predefined service definition, the default MTU is 1522 bytes.</p>
MTU Range (Bytes)	<p>If you select the Editable in Service Order check box, you can specify a value range for MTU (in bytes). .</p> <p>Default: 1522 bytes</p> <p>Range: 1522 bytes through 9192 bytes</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	<p>The Bandwidth Settings pane, appears if you do not select the Enable QoS check box in the preceding General settings window. This panel includes the following fields:</p> <ul style="list-style-type: none"> • Enable rate limiting • Default bandwidth (Mbps) • Min Bandwidth (Kbps) • Max Bandwidth (Mbps) • Increment (Kbps)
Enable rate limiting	<p>If you select this check box, you can override the MTU setting.</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> <p>For a predefined service definition, the default bandwidth value is 10 Mbps.</p>

Field	Action
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>
Increment (Kbps)	<p>Specify a value in the range that is made available to the service provisioner.</p> <p>Default: 1000 Kbps</p> <p>Range: 64Kbps through 100,000 Kbps</p>
Calculate Burst Size	<p>Select the preferred option for calculating the burst size:</p> <ul style="list-style-type: none"> MTU Based <p>If you select the MTU Based option, you can specify a value for MTU Factor.</p> <p>Default: 10</p> <p>Range: 10 through 1,087,902</p> Line Rate Based <p>If you select the Line Rate Based option, you can specify a value for Burst Period.</p> <p>Default: 5 milliseconds</p> <p>Range: 5 through 7450 milliseconds</p> <p>NOTE: The Calculate Burst Size list is enabled only when you select the Enable rate limiting check box.</p>

The following table lists the **Max Bandwidth (Mbps)** for the M Series, MX Series, and ACX Series routers:

Table 20: 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)

Table 20: Maximum Bandwidth for M Series, MX Series, and ACX Series Routers (continued)

M Series IQ2E PIC		M Series IQ2 PIC		MX Series 3D PIC		MX Series Non-3D PIC		ACX 2000	
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 **Next** to save the UNI settings. Continue with [“Specifying Connectivity Information” on page 382](#).

Specifying Connectivity Information

To specify the attributes that define the connectivity among remote sites across the service provider network:

The screenshot shows the 'Connectivity' configuration page with three main sections:

- PE-Core Settings:**
 - Route target: Auto pick (dropdown)
 - Route distinguisher: Auto pick (dropdown)
 - ☒ VRF Table label
 - ☒ Export Direct Routes
 - Editable in Service Order (checkbox) - three instances
- PE-CE Settings:**
 - Allowed Routing Protocols:
 - ☒ OSPF/Static Route
 - ☐ BGP/Static Route
- IP Address Settings:**
 - PE Interface IP Address: Select manually (dropdown)
 - IP pool type: Global (dropdown)
 - Size of address block: 28 (text input)
 - Editable in Service Order (checkbox) - three instances

1. Fill in the fields on the Connectivity page as indicated in the table. In the **PE-Core Settings** box, specify whether to allow the service provider to specify the route target:

Field	Action
PE-Core Settings	

Field	Action
Route target	<p>Select a route target option:</p> <ul style="list-style-type: none"> • Select manually—Allows the service provider to specify the route target. • Auto pick—Route target is selected automatically. <p>To override this setting in the service order, you can select the Editable in Service Order check box.</p>
Route distinguisher	<p>Select a route distinguisher option:</p> <ul style="list-style-type: none"> • Select manually—Allows the service provider to specify the route distinguisher. • Auto pick—Route distinguisher is 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.
PE-CE Settings	

Field	Action
Allowed Routing Protocols	<p>Select an option to use to allow each PE router to distribute VPN-related routes to and from connected CE routers:</p> <ul style="list-style-type: none"> • OSPF/Static Route—OSPF routes IP packets based solely on the destination IP address contained in the IP packet header. OSPF quickly detects topological changes, such as when router interfaces become unavailable, and calculates new loop-free routes quickly and with a minimum of routing overhead traffic. Static routes are routes that are manually configured and entered into the routing table. • BGP/Static Route—BGP routing information includes the complete route to each destination. BGP uses the routing information to maintain a database of network reachability information, which it exchanges with other BGP systems. BGP uses the network reachability information to construct a graph of AS connectivity, thus allowing BGP to remove routing loops and enforce policy decisions at the AS level. Static routes are routes that are manually configured and entered into the routing table.
IP Address Settings	
PE Interface IP Address	<p>Select an option:</p> <ul style="list-style-type: none"> • Select manually—Allows the service provider to specify the IP address of a provider edge (PE) interface. • Auto pick— IP address of a provider edge (PE) interface is selected automatically. <p>To override this setting in the service order, you can select the Editable in Service Order check box.</p>

Field	Action
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. • 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>For more information on creation an IP pool, see “Creating an IP Address Pool” on page 106.</p>
Size of address block	<p>Specify the size of the IPv4 IP addressee block allocated for each provider edge (PE) or customer edge (CE) link.</p> <p>Range: 28 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 **Finish** to save the connectivity settings and create the Layer 3 VPN service definition.

RELATED DOCUMENTATION

[Publishing a Custom Service Definition](#) | 308

[Viewing Service Definitions](#) | 267

[Creating a Full Mesh Layer 3 VPN Ethernet Service Order](#) | 718

[Junos Space Layer 3 Services Overview](#) | 171

[Service Templates Overview](#) | 113

[Creating a Service Template](#) | 116

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 this version of the Network Activate application, using predefined service definitions located in **Service Design > Manage Service Definitions > Create L3 VPN Service Definitions**. 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. 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 572](#). 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.

You can create a service definition, using the **Create L3 VPN Service Definition General**, **UNI Settings**, or **Connectivity** window in any order by clicking the task links in the right panel. You can hide the task links by clicking the show/hide button at the top-left of any of the Create L3 VPN Service Definition windows.

1. [Specifying General Information | 387](#)
2. [Specifying UNI Settings | 388](#)
3. [Specifying Connectivity Settings | 392](#)

Specifying General Information

To specify general information for a hub-and-spoke service definition:

General

Name: SD-L3VPN-Hub-Spoke

Service type: L3 VPN (Hub-Spoke 1 Interface)

Comments:

Service Template: Please select ...

☒ Enable MVPN
 ☒ Enable QoS
 ☒ Decouple Service Status From Port Status

1. Fill in the fields on the General page as indicated in the table.

Field	Action
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) .
Comments	Type a comment that identifies or describes the definition. Range: 1 through 200 characters.
Decouple Service Status From Port Status	Select this check box to isolate the events related to an interface in OpenNMS. NOTE: When you select this check box, only the MPLS traps are monitored, not the jnxVpnIfVpn traps. By default, all events are saved in the OpenNMS database.
Enable QoS	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 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. NOTE: The Enable QoS check box appears only if you have installed the QoS Design application.

Field	Action
Service Template	<p>(Optional) To include a service template for the service, select a service template from the Service Template list.</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 116.</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 **UNI Settings-Create L3 VPN Service Definition** page appears.

Specifying UNI Settings

To specify UNI interface settings for the service definition:

UNI Settings

Interface Settings

☒ Ethernet

VLAN ID selection: Auto pick

☐ Editable in Service Order

VLAN range for auto-pick: -

VLAN range for manual input: -

MTU Settings

Default MTU (Bytes): 1522

☐ Editable in Service Order

MTU range (Bytes): 1522

9192

Bandwidth Settings

☒ Enable rate limiting

☒ Editable in Service Order

Default bandwidth (Mbps): 10

Min Bandwidth (Kbps): 1000

Max Bandwidth (Mbps): 100

Increment (Kbps): 1000

Calculation of Burst-Size

Calculate Burst Size: MTU Based

☒ Editable in Service Order

MTU Factor: 10

1. Fill in the fields on the UNI Settings page as indicated in the table as indicated in the table.

Field	Action
Ethernet	By default, this check box is unavailable.
VLAN ID selection	<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, choose Select manually. Specify the range in VLAN range for manual input. To cause the VLAN ID to be selected automatically from the VLAN ID pool, select Auto pick. This option is used typically when VLAN normalization is applied. Specify the range in VLAN 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>
VLAN range for auto-pick	<p>Specify the range.</p> <p>Range: 1 through 4094.</p>

Field	Action
VLAN range for manual input	<p>Specify the range.</p> <p>Range: 1 through 4094.</p> <p>NOTE: This parameter reserves a range of VLANs for provisioning L3VPNs. These VLANs are not used to transport data from one end of a connection to the other.</p>
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> <p>For a predefined service definition, the default MTU is 1522 bytes.</p>
MTU Range (Bytes)	<p>If you select the Editable in Service Order check box, you can specify a value range for MTU (in bytes). .</p> <p>Default: 1522 bytes</p> <p>Range: 1522 bytes through 9192 bytes</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	<p>The Bandwidth Settings panel, appears if you do not select the Enable QoS check box in the preceding General settings window. This panel includes the following fields:</p> <ul style="list-style-type: none"> • Enable rate limiting • Default bandwidth (Mbps) • Min Bandwidth (Kbps) • Max Bandwidth (Mbps) • Increment (Kbps)
Enable rate limiting	<p>If you select this check box, you can override the MTU setting.</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> <p>For a predefined service definition, the default bandwidth value is 10 Mbps.</p>

Field	Action
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>
Increment (Kbps)	Specify a value in the range that is made available to the service provisioner.
Calculate Burst Size	<p>Select the preferred option for calculating the burst size:</p> <ul style="list-style-type: none"> MTU Based <p>If you select the MTU Based option, you can specify a value for MTU Factor.</p> <p>Default: 10</p> <p>Range: 10 through 1,087,902</p> Line Rate Based <p>If you select the Line Rate Based option, you can specify a value for Burst Period.</p> <p>Default: 5 milliseconds</p> <p>Range: 5 through 7450 milliseconds</p> <p>NOTE: The Calculate Burst Size list is enabled only when you select the Enable rate limiting check box.</p>

The following table lists the **Max Bandwidth (Mbps)** for the M Series, MX Series, and ACX Series routers:

Table 21: 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 **Next** to save the UNI Settings step information.

The **Connectivity** window appears.

Specifying Connectivity Settings

On the **Connectivity>Create L3 VPN Service Definition** window, specify the attributes that define the connectivity among remote sites across the service provider network.

The Connectivity window includes two setting sections: **PE-Core** and **PE-CE**.

To specify connectivity between sites across the network:

Connectivity

PE-Core Settings

Route target:Auto pick

Route distinguisher:Auto pick

☒ VRF Table Label

☒ Export Direct Routes

☐ Editable in Service Order

☐ Editable in Service Order

☐ Editable in Service Order

PE-CE Settings

Allowed Routing Protocols:

☒ OSPF/Static Route

☐ BGP/Static Route

IP Address Settings

PE Interface IP Address:Select manually

IP pool type:Global

Size of address block:28

☐ Editable in Service Order

☐ Editable in Service Order

☐ Editable in Service Order

- 1. Fill in the fields on the Connectivity page as indicated in the table.

Field	Action
PE-Core Settings	
Route target	<div>Select a route target option:<ul style="list-style-type: none">• Select manually—Allows the service provider to specify the route target.• Auto pick—Route target is selected automatically.To override this setting in the service order, you can select the Editable in Service Order check box.</div>

Field	Action
Route distinguisher	<p>Select a route distinguisher option:</p> <ul style="list-style-type: none"> • Select manually—Allows the service provider to specify the route distinguisher. • Auto pick—Route distinguisher is 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.
PE-CE Settings	
Allowed Routing Protocols	<p>Select an option to use to allow each PE router to distribute VPN-related routes to and from connected CE routers:</p> <ul style="list-style-type: none"> • OSPF/Static Route—OSPF routes IP packets based solely on the destination IP address contained in the IP packet header. OSPF quickly detects topological changes, such as when router interfaces become unavailable, and calculates new loop-free routes quickly and with a minimum of routing overhead traffic. Static routes are routes that are manually configured and entered into the routing table. • BGP/Static Route—BGP routing information includes the complete route to each destination. BGP uses the routing information to maintain a database of network reachability information, which it exchanges with other BGP systems. BGP uses the network reachability information to construct a graph of AS connectivity, thus allowing BGP to remove routing loops and enforce policy decisions at the AS level. Static routes are routes that are manually configured and entered into the routing table.
IP Address Settings	
PE Interface IP Address	<p>Select an option:</p> <ul style="list-style-type: none"> • Select manually—Allows the service provider to specify the IP address of a provider edge (PE) interface. • Auto pick— IP address of a provider edge (PE) interface is selected automatically. <p>To override this setting in the service order, you can select the Editable in Service Order check box.</p>

Field	Action
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. • 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>For more information on creation an IP pool, see “Creating an IP Address Pool” on page 106.</p>
Size of address block	<p>Specify the size of the IPv4 IP addressee block allocated for each provider edge (PE) or customer edge (CE) link.</p> <p>Range: 28 through 32</p> <p>To override this setting in the service order, you can select the Editable in Service Order check box.</p>

2. The **VRF Table label** option is selected by default .
3. Click **Finish** to save the connectivity settings and create the Layer 3 VPN service definition.

RELATED DOCUMENTATION

[Viewing Service Definitions | 267](#)

[Predefined Hub-and Spoke Layer 3 VPN Service Definitions | 572](#)

[Publishing a Custom Service Definition | 308](#)

[Unpublishing a Custom Service Definition | 309](#)

[Deleting a Customized Service Definition | 309](#)

[Predefined Full Mesh Layer 3 VPN Service Definitions | 571](#)

[Creating a Full Mesh Layer 3 VPN Ethernet Service Order | 718](#)

[Specifying IPv4 Addressing Assignment in Layer 3 VPN Service Definitions | 110](#)

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 Activate task pane, select **Service Design > Create P2P Service Definition**.

The screenshot shows the 'Create P2P Service Definition' window with the 'General' tab selected. The 'Name' field contains 'P2Psd'. The 'Service type' is 'Point-to-Point Pseudowire'. The 'Signaling' dropdown is set to 'LDP'. The 'Comments' field is empty. The 'Interface type' has radio buttons for 'Ethernet' (selected), 'TDM', and 'ATM'. There are checkboxes for 'Enable QoS' (checked), 'Static pseudowire' (unchecked), 'Enable PW access to L3 VPN network' (unchecked), and 'Enable PW Resiliency' (unchecked). The 'Service Template' dropdown shows 'Please select ...'. At the bottom are 'Back', 'Next', 'Finish', and 'Cancel' buttons.

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.

Service Design > Manage Service Definitions > **Create P2P Service Definition**

Connectivity

Connectivity Settings

VC ID selection: ☐ Editable in Service Order

Default MTU (Bytes): ☐ Editable in Service Order

MTU range (Bytes):

Outgoing label selection: ☐ Editable in Service Order

Create P2P Service Definition

✓ General

✓ UNI Settings (*)

Connectivity (*)

◀ Back Next ▶ Finish Cancel

Field	Action
VC ID selection	Choose from Auto pick or Select Manually for VC ID assignment.
Default MTU (Bytes)	Indicate the MTU size or use the default that appears in the field.

- Click **Next** to display the **UNI 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.

Service Design > Manage Service Definitions > Create P2P Service Definition

UNI Settings

Traffic Treatment

Ethernet option:

Customer traffic type:

VLAN ID selection: ☐ Editable in Service Order

VLAN range for auto-pick:

VLAN range for manual input:

Outer Tag protocol ID: ☐ Editable in Service Order

Inner Tag protocol ID: ☐ Editable in Service Order

Interface Settings

Physical IF encapsulation:

Logical IF encapsulation:

MTU Settings

Back Next Finish Cancel

Create P2P Service Definition

- General
- UNI Settings (*)
- Connectivity (*)

UNI 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.

UNI Settings Field	Action
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:

Service Design > Manage Service Definitions > Create P2P Service Definition

UNI Settings

Traffic Treatment

Ethernet option: dot1q

Customer traffic type: Transport single vlan

VLAN ID selection: Select manually

VLAN range for auto-pick:

VLAN range for manual input:

Outer Tag protocol ID: 0x88a8 0x8100

Inner Tag protocol ID: Please select ...

Interface Settings

Physical IF encapsulation: flexible-ethernet-services

Logical IF encapsulation: vlan-ccc

MTU Settings

Create P2P Service Definition

General

UNI Settings (*)

Connectivity (*)

Back Next Finish Cancel

5. Click **Finish** and then create the service order.

RELATED DOCUMENTATION

[Creating a Point-to-Point ATM or TDM Pseudowire Service Order | 578](#)

[Creating a Point-to-Point Service Order | 586](#)

Creating a Layer 3 VPN Service Definition in Cross Provisioning Platform for Third-Party Devices

Cross Provisioning Platform is an extension of the Network Activate application within Junos Space, which provides a single pane of interaction to deploy services across vendors. This topic discusses how a Layer 3 VPN service definition is created and deployed across third-party devices involved in Cross Provisioning Platform.

To create an Layer 3 VPN service definition, you need to create a configuration script in XSLT format and GUI script in JS format and upload these scripts from the local machine to Cross Provisioning Platform. You can add the scripts by selecting **Cross Provisioning Platform > CPP > Scripts > Add Script**.

To create a Layer 3 VPN service definition:

1. From the **Cross Provisioning Platform** task pane, select **CPP > Service Definitions**.

The **Service Definitions** page that appears displays a list of the existing service definitions.

2. Click the **Create CPP Service Definition** icon above the tool grid.

The **Create Service Definition** page that appears displays **General**, the **SAM Service Scripts** and the **JUNOS Space Server Scripts** sections.

Create CPP Service Definition

General

Name: SD-L3VPN

ID: 10435

Type: L3VPN

Description:

Service Script Selections

Operation Type: Please Select

Select Scripts

	Name	Vendor Type	Version
<input type="checkbox"/>	PD_BNG_Details_Script_JNPR	Juniper	1
<input type="checkbox"/>	PD_NPS_Details_Script_JNPR	Juniper	1
<input type="checkbox"/>	PD_VLAN-PATH_Details_Script_IPASO	Juniper	1
<input type="checkbox"/>	PD_Device_Details_Script_JNPR	Juniper	1
<input type="checkbox"/>	PD_P2P_LDP_Details_Script_ALU	Alcatel	1
<input type="checkbox"/>	PD_L3VPN_Details_Script_ALU	Alcatel	1
<input type="checkbox"/>	PD_BNG_Details_Script_ALU	Alcatel	1

Page 1 of 1

Displaying 1 - 47 of 47

Add Script

Selected Scripts

	Name	Vendor Type	Operation Type	Action
<input type="checkbox"/>	PD_L3VPN_Details_Script_ALU	Alcatel	Modify	

Create

Cancel

- On the **Create Service Definition** page, perform the following steps:
 - In the **General** section:
 - In the **Name** field, type 3 through 128 alphanumeric characters to identify the name of the service definition.
 - In the **ID** field, type 1 through 2147483647 integers to identify the service definition by a unique value.

NOTE: The service definition ID is optional. If you do not provide any value in this field, the default value is -1. In the service definition selection grid, no value is displayed in the **ID** column. Each service definition is assigned a unique ID. If you give an existing ID value while creating a new service definition, exception occurs.

- c. In the **Description** field, type 3 through 256 alphanumeric characters to further identify the service definition you named.
- d. From the **Type** drop-down list, select **L3VPN**.
- Select one of the following operation type:
 - Create
 - Modify
- In the **Select Scripts**, select a script.

The **Select Scripts** section lists the scripts that belong to various vendors along with the script version number. To find the script that you want to add, you can perform a search in the search box.
- Click **Add Scripts** to add a script to the service definition.

The **Selected Scripts** section lists the scripts that you have selected. The scripts are listed based on the vendor type and operation type.

To delete a script, in the **Action** column click the delete icon.
4. Click **Create** to create the service definition.

The **Service Definitions** page that appears displays the list of existing service definitions along with the service definition that you created.
5. Right-click the service definition that you created and select **Publish Service Definition**.

The **Publish Service Definitions** dialog box that appears asks you to confirm the selection.
6. Click **Publish**.

The **Service Definitions** page that appears displays the service definition that you created along with the existing service definitions.
7. Double-click the service definition that you created to view the details.

The **Service Definition Details** page that appears displays the details of the service definition along with the scripts that you uploaded.

RELATED DOCUMENTATION

[Adding Scripts Created for Cross Provisioning Platform | 775](#)

[Creating a Layer 3 VPN Service Order in Cross Provisioning Platform for Third-Party Devices | 765](#)

Creating a Multicast VPN Service Definition

This topic describes how the Network Activate 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 376.](#)

NOTE: Multicast VPN services are supported on LN2600, SRX 550/650, and MX devices only.

To create a L3VPN Service definition upon which to base a MVPN service order, in the Network Activate task pane, select **Service Design > Manage Service Definitions > Create L3VPN Service Definition**.

1. Specify values for the parameters in the **General**, **UNI Settings**, and **Connectivity 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
Name	Type a name for this service definition.
Service type	Select L3VPN (Full Mesh)
Comments	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 **UNI Settings** window, add information in the relevant fields as described in the following table:

UNI Settings

Interface Settings

☒ Ethernet

VLAN ID selection: Auto pick

☐ Editable in Service Order

VLAN range for auto-pick:

VLAN range for manual input:

Create L3 VPN Service Definition

General

UNI Settings (*)

Connectivity (*)

Field	Description
Ethernet	Select this check box.
VLAN ID selection	Select Auto pick.
VLAN range for auto-pick	N/A
VLAN range for manual input	N/A

- 4. Click **Next**.

Connectivity

PE-Core Settings

Route target: Auto pick

☐ Editable in Service

Route distinguisher: Auto pick

☐ Editable in Service

☒ VRF Table Label

☐ Editable in Service

☒ Export Direct Routes

☐ Editable in Service

PE-CE Settings

Allowed Routing Protocols: OSPF/Static Route

☐ BGP/Static Route

IP Address Settings

PE Interface IP Address: Auto pick

☐ Editable in Service

IP pool type: Global

☐ Editable in Service

Size of address block:

☐ Editable in Service

Create L3 VPN Service Definition

General

UNI Settings (*)

Connectivity (*)

5. In the **Connectivity Settings** window, add information in the relevant fields as described in the following table:

Field	Description
Route target	A site within a VPN that a PE router services and to which the PE router will distribute routes.
Router distinguisher	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. Select Auto pick. JUNOS Space selects the route distinguisher automatically.
VRF Table label	A VRF table label distinguishes one VRF instance from another and enables double lookup and egress filtering. Select this check box.
Export Direct Routes	Select this check box.
Allowed Routing Protocols	Select BGP/Static Route
PE Interface IP Address	The IP address of the interface on the PE device. Select Auto pick.
IP pool type	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. 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.
Size of address block	The size of the IPv4 addresses block allocated for each PE/CE link. Range: 28–32

See [“Specifying IPv4 Addressing Assignment in Layer 3 VPN Service Definitions”](#) on page 110.

6. Click **Finish**.

RELATED DOCUMENTATION

[Creating a Full Mesh Layer 3 VPN Service Definition | 376](#)

[Specifying IPv4 Addressing Assignment in Layer 3 VPN Service Definitions | 110](#)

[Multicast L3VPN Overview | 173](#)

[Creating a Multicast VPN Service Order | 748](#)

Predefined Service Definitions

IN THIS CHAPTER

- [Predefined Service Definitions | 408](#)
- [Predefined Point-to-Point Service Definitions | 477](#)
- [Predefined Multipoint-to-Multipoint Ethernet Service Definitions | 521](#)
- [Predefined Point-to-Multipoint Ethernet Service Definitions | 554](#)
- [Predefined Full Mesh Layer 3 VPN Service Definitions | 571](#)
- [Predefined Hub-and Spoke Layer 3 VPN Service Definitions | 572](#)

Predefined Service Definitions

Network Activate 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 an E-Line Service Definition” on page 188](#), [“Creating a Point-to-Multipoint VPLS Service Definition” on page 237](#), or [“Creating a Multipoint-to-Multipoint VPLS Service Definition” on page 214](#).

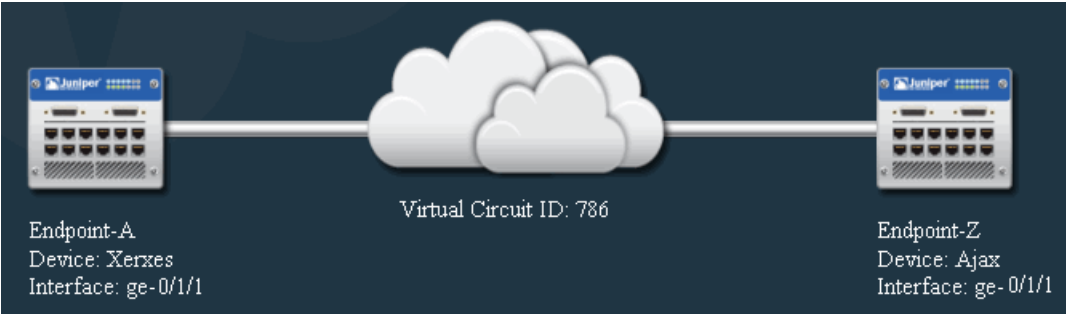
The Junos Space product provides predefined service definitions for Ethernet point-to-point services and for VPLS services. The following sections describe these service definitions:

- [Ethernet Point-to-Point Predefined Service Definitions on page 408](#)
- [Multipoint-to-Multipoint Predefined Service Definitions on page 440](#)
- [Point-to-Multipoint Service Definitions on page 473](#)

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 15 on page 409](#) shows an example of such a service.

Figure 15: 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 22 on page 409](#) 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 22: Standard Service Definitions

Standard Service Definition Name	Service Attributes
"ELine-Dot1q-SingleVLAN" on page 411	<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 414	<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 22: Standard Service Definitions (*continued*)

Standard Service Definition Name	Service Attributes
“ELine-Dot1q-SingleVLAN-Ext-CCC” on page 417	<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 420	<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 423	<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 426	<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 429	<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 22: Standard Service Definitions (*continued*)

Standard Service Definition Name	Service Attributes
“ELine-QinQ-VLANRange” on page 432	<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 435	<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 438	<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**IN THIS SECTION**

- [Configuration on Endpoint A | 412](#)
- [Configuration on Endpoint Z | 413](#)

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 15 on page 409](#):

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

IN THIS SECTION

- [Configuration on Endpoint A | 414](#)
- [Configuration on Endpoint Z | 416](#)

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 15 on page 409](#):

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

IN THIS SECTION

- Configuration on Endpoint A | 417
- Configuration on Endpoint Z | 419

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 15 on page 409](#):

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

IN THIS SECTION

- Configuration on Endpoint A | 420
- Configuration on Endpoint Z | 421

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 15 on page 409](#):

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**IN THIS SECTION**

- Configuration on Endpoint A | 423
- Configuration on Endpoint Z | 424

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 15 on page 409](#):

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***IN THIS SECTION**

- Configuration on Endpoint A | 426
- Configuration on Endpoint Z | 427

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 15 on page 409](#):

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***IN THIS SECTION**

- Configuration on Endpoint A | 429
- Configuration on Endpoint Z | 430

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 15 on page 409](#):

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***IN THIS SECTION**

- Configuration on Endpoint A | 432
- Configuration on Endpoint Z | 433

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 15 on page 409](#):

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***IN THIS SECTION**

- Configuration on Endpoint A | 435
- Configuration on Endpoint Z | 436

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 15 on page 409](#):

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**IN THIS SECTION**

- Configuration on Endpoint A | 438
- Configuration on Endpoint Z | 439

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 15 on page 409](#):

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;
      }
    }
  }
}

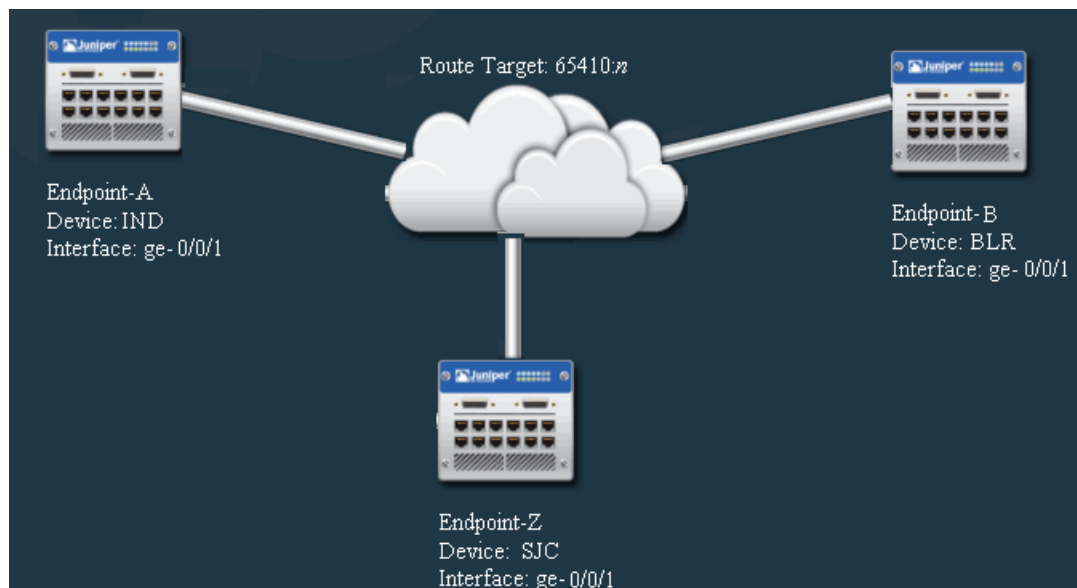
```

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 16 on page 441](#) shows an example of such a service.

Figure 16: 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 23 on page 442](#) lists each of the standard VPLS service definitions. Each standard service definition is then described in detail in the sections that follow.

Table 23: Standard Service Definitions

Standard Service Definition Name	Service Attributes
“ELAN-BGP-Dot1q-Normalized-VLAN-None” on page 443	<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 448	<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 452	<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 457	<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 23: Standard Service Definitions (*continued*)

Standard Service Definition Name	Service Attributes
“ELAN-BGP-QinQ-AllVLAN-Normalized-All” on page 461	<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 466	<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 470	<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**IN THIS SECTION**

- [Configuration on Endpoint A | 444](#)
- [Configuration on Endpoint B | 445](#)
- [Configuration on Endpoint Z | 446](#)

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 16 on page 441](#):

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

IN THIS SECTION

- Configuration on Endpoint A | 448
- Configuration on Endpoint B | 450
- Configuration on Endpoint Z | 451

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 16 on page 441](#):

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 {

```


The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 16 on page 441](#):

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;
        }
    }
}

```



```

    }

}

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

IN THIS SECTION

- Configuration on Endpoint A | 457
- Configuration on Endpoint B | 458
- Configuration on Endpoint Z | 460

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 16 on page 441](#):

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

IN THIS SECTION

- Configuration on Endpoint A | 462
- Configuration on Endpoint B | 463
- Configuration on Endpoint Z | 464

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 16 on page 441](#):

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 {

```



```

    }
    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***IN THIS SECTION**

- Configuration on Endpoint A | 466
- Configuration on Endpoint B | 467
- Configuration on Endpoint Z | 469

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 16 on page 441](#):

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

IN THIS SECTION

- [Configuration on Endpoint A | 471](#)
- [Configuration on Endpoint Z | 472](#)

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

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;
                }
            }
        }
    }
}

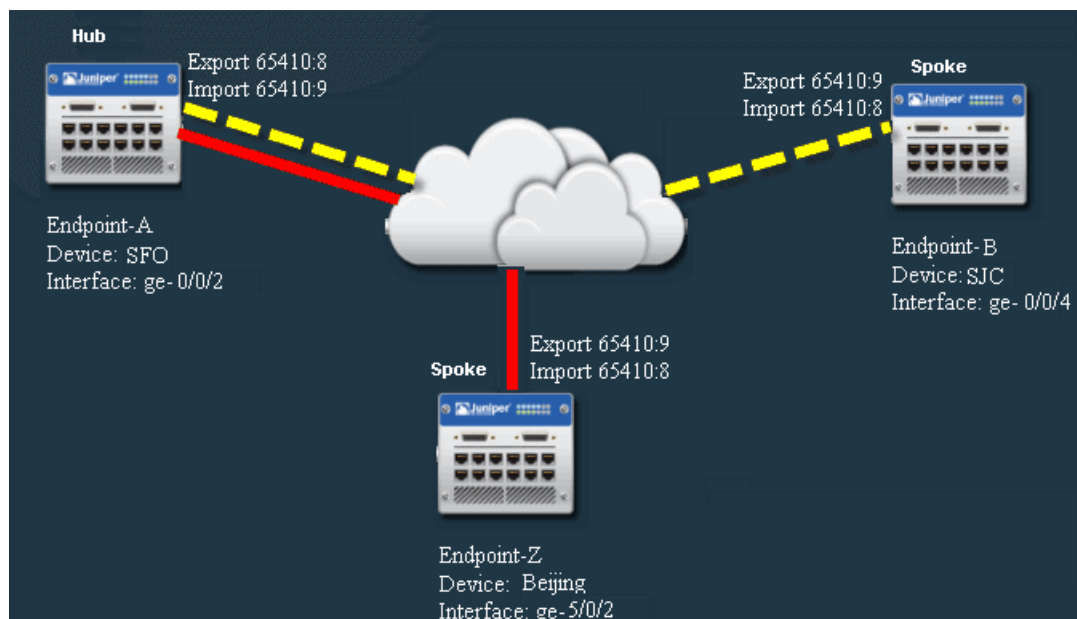
routing-instances {
    BestCustomer_ELAN-BGP-QinQ-Range-Normalized-VLAN-SR1 {
        instance-type vpls;
        vlan-id all;
        interface ge-0/0/1.1;
        route-distinguisher 65410:18;
        vrf-target target:65410:6;
        protocols {
            vpls {
                no-tunnel-services;
                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 17 on page 474](#) shows an example of such a service.

Figure 17: 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 24 on page 475](#) lists each of the standard VPLS service definitions. Each standard service definition is then described in detail in the sections that follow.

Table 24: Standard Service Definitions

Standard Service Definition Name	Service Attributes
“ELAN-Hub-Spoke-QinQ-AllVLAN” on page 475	<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 476	<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**IN THIS SECTION**

- [Configuration on Endpoint A | 476](#)
- [Configuration on Endpoint B | 476](#)
- [Configuration on Endpoint Z | 476](#)

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 17 on page 474](#):

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**IN THIS SECTION**

- [Configuration on Endpoint A | 476](#)
- [Configuration on Endpoint B | 476](#)
- [Configuration on Endpoint Z | 476](#)

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 17 on page 474](#):

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 an E-Line Service Definition | 188](#)

[Creating a Multipoint-to-Multipoint VPLS Service Definition | 214](#)

Predefined Point-to-Point Service Definitions

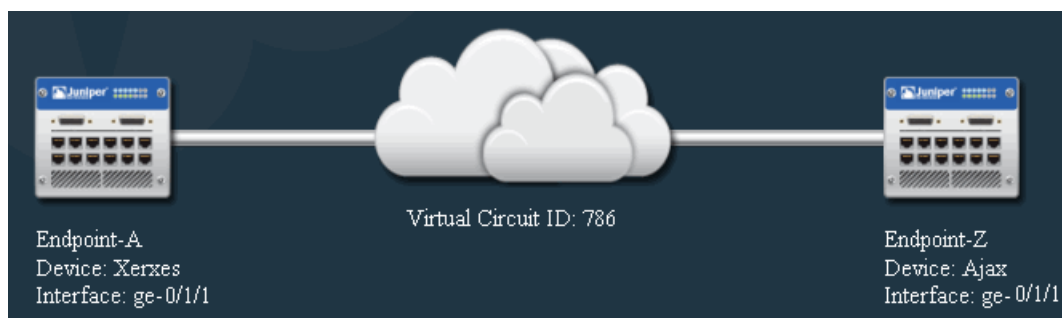
The Network Activate software provides predefined service definitions that a service provisioner can choose from when creating a service order. This section provides information about predefined service definitions used for creating Ethernet point-to-point services. For information about predefined service definitions used to create other types of service, see the following topics:

- [Predefined Multipoint-to-Multipoint Ethernet Service Definitions on page 521](#)
- [Predefined Point-to-Multipoint Ethernet Service Definitions on page 554](#)
- [Predefined Full Mesh Layer 3 VPN Service Definitions on page 571](#)
- [Predefined Hub-and Spoke Layer 3 VPN Service Definitions on page 572](#)

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 an E-Line Service Definition” on page 188](#),

The Network Activate software 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 15 on page 409](#) shows an example of such a service.

Figure 18: 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 22 on page 409 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 25: Standard Ethernet Point-to-Point Ethernet Service Definitions

Standard Service Definition Name	Service Attributes
"ELine-Dot1q-SingleVLAN" on page 411	<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 414	<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 417	<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 420	<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

Table 25: Standard Ethernet Point-to-Point Ethernet Service Definitions (*continued*)

Standard Service Definition Name	Service Attributes
“ELine-QinQ-AllVLAN” on page 423	<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
“ELine-QinQ-AllVLAN-CCC” on page 426	<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 429	<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 432	<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 435	<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

Table 25: Standard Ethernet Point-to-Point Ethernet Service Definitions (*continued*)

Standard Service Definition Name	Service Attributes
“ELine-QinQ-VLANRange-Ext-CCC” on page 438	<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 and BX7000 Gateways only • T1 interfaces • satop physical encapsulation
Static TDM pseudowire	<ul style="list-style-type: none"> • Point-to-point service for MX Series routers and BX7000 Gateways only • T1 interfaces • satop physical encapsulation • Static pseudowire
ATM pseudowire	<ul style="list-style-type: none"> • Point-to-point service for MX Series routers and BX7000 Gateways only • ATM/T1 interfaces • atm-cc-cell-relay physical encapsulation
ATM-AAL5 pseudowire	<ul style="list-style-type: none"> • Point-to-point service for MX Series routers and BX7000 Gateways 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 and BX7000 Gateways 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 and BX7000 Gateways only • ATM/T1 interfaces • atm-ccc-vc-mux / aal5 physical encapsulation • Static pseudowire

Table 25: Standard Ethernet Point-to-Point Ethernet Service Definitions (*continued*)

Standard Service Definition Name	Service Attributes
“ELine-BGP-QinQ-AllVLAN” on page 517	<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 514	<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
“ELine-BGP-Port-Based” on page 511	<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

IN THIS SECTION

- [Configuration on Endpoint A | 482](#)
- [Configuration on Endpoint Z | 483](#)

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 15 on page 409](#):

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

IN THIS SECTION

- [Configuration on Endpoint A | 484](#)
- [Configuration on Endpoint Z | 486](#)

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 15 on page 409](#):

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

IN THIS SECTION

- Configuration on Endpoint A | 487
- Configuration on Endpoint Z | 489

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 15 on page 409](#):

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

IN THIS SECTION

- Configuration on Endpoint A | [490](#)
- Configuration on Endpoint Z | [491](#)

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 15 on page 409](#):

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

IN THIS SECTION

- [Configuration on Endpoint A | 493](#)
- [Configuration on Endpoint Z | 494](#)

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 15 on page 409](#):

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

IN THIS SECTION

- Configuration on Endpoint A | 496
- Configuration on Endpoint Z | 497

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 15 on page 409](#):

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

IN THIS SECTION

- Configuration on Endpoint A | 499
- Configuration on Endpoint Z | 500

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 15 on page 409](#):

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 Service Definition

IN THIS SECTION

- Configuration on Endpoint A | 502
- Configuration on Endpoint Z | 503

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 15 on page 409](#):

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

IN THIS SECTION

- [Configuration on Endpoint A | 505](#)
- [Configuration on Endpoint Z | 506](#)

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 15 on page 409](#):

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

IN THIS SECTION

- [Configuration on Endpoint A | 508](#)
- [Configuration on Endpoint Z | 509](#)

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 15 on page 409](#):

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

IN THIS SECTION

- Configuration on Endpoint A | 511
- Configuration on Endpoint Z | 512

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 15 on page 409](#):

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

IN THIS SECTION

- Configuration on Endpoint A | 514
- Configuration on Endpoint Z | 516

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 15 on page 409](#):

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;
    }
}

```

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-0/0/3.823;
    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

IN THIS SECTION

- [Configuration on Endpoint A | 517](#)
- [Configuration on Endpoint Z | 519](#)

The following sections show the configuration data on each endpoint when you use this service definition to create the service shown in [Figure 15 on page 409](#):

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-QnQAllVlan;
            }
        }
    }
}

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-QnQAllVlan;
        }
      }
    }
  }
}

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 | 181](#)

[Creating an E-Line Service Definition | 188](#)

[Predefined Multipoint-to-Multipoint Ethernet Service Definitions | 521](#)

[Predefined Point-to-Multipoint Ethernet Service Definitions | 554](#)

Predefined Multipoint-to-Multipoint Ethernet Service Definitions

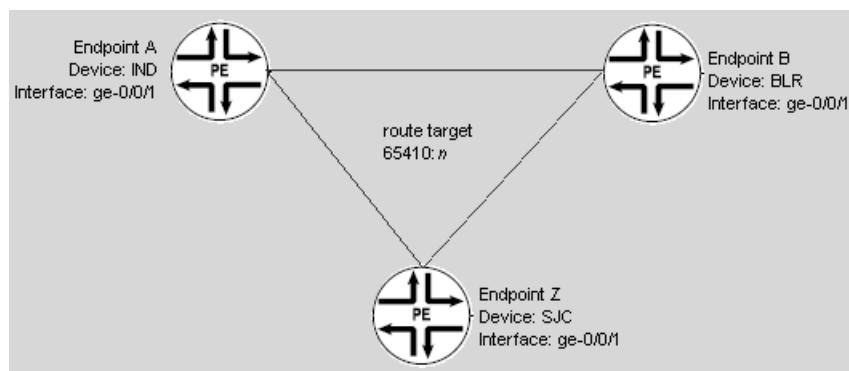
The Network Activate software provides predefined service definitions that a service provisioner can choose from when creating a service order. This section provides information about predefined service definitions used for creating multipoint-to-multipoint Ethernet services. For information about predefined service definitions used to create point-to-point service definitions or point-to-multipoint service definitions, see the following topics:

- [Predefined Point-to-Multipoint Ethernet Service Definitions on page 554](#)
- [Predefined Point-to-Point Service Definitions on page 477](#)

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 214](#).

The Network Activate 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 16 on page 441](#) shows an example of such a service.

Figure 19: 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 24 on page 475 lists each of the standard VPLS service definitions. Each standard service definition is then described in detail in the sections that follow.

Table 26: Standard Multipoint-to-Multipoint Service Definitions

Standard Service Definition Name	Service Attributes
“ELAN-BGP-Dot1q-Normalized-VLAN-None” on page 443	<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 448	<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 452	<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

Table 26: Standard Multipoint-to-Multipoint Service Definitions (*continued*)

Standard Service Definition Name	Service Attributes
“ELAN-BGP-QinQ-AllVLAN” on page 457	<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
“ELAN-BGP-QinQ-AllVLAN-Normalized-All” on page 461	<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 466	<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 470	<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

IN THIS SECTION

- Configuration on Endpoint A | 524
- Configuration on Endpoint B | 525
- Configuration on Endpoint Z | 527

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 16 on page 441](#):

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

IN THIS SECTION

- [Configuration on Endpoint A | 529](#)
- [Configuration on Endpoint B | 530](#)
- [Configuration on Endpoint Z | 531](#)

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 16 on page 441](#):

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;
                        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 Service Definition

IN THIS SECTION

- Configuration on Endpoint A | 533
- Configuration on Endpoint B | 534
- Configuration on Endpoint Z | 536

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 16 on page 441](#):

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;
    }
}
```



```

    }
  }
}

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

IN THIS SECTION

- [Configuration on Endpoint A | 537](#)
- [Configuration on Endpoint B | 539](#)
- [Configuration on Endpoint Z | 540](#)

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 16 on page 441](#):

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

IN THIS SECTION

- Configuration on Endpoint A | 542
- Configuration on Endpoint B | 543
- Configuration on Endpoint Z | 545

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 16 on page 441](#):

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

IN THIS SECTION

- [Configuration on Endpoint A | 547](#)
- [Configuration on Endpoint B | 548](#)
- [Configuration on Endpoint Z | 549](#)

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 16 on page 441](#):

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

IN THIS SECTION

- [Configuration on Endpoint A | 551](#)
- [Configuration on Endpoint Z | 553](#)

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

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

[Creating a Multipoint-to-Multipoint VPLS Service Definition | 214](#)

[Predefined Point-to-Multipoint Ethernet Service Definitions | 554](#)

[Predefined Point-to-Point Service Definitions | 477](#)

Predefined Point-to-Multipoint Ethernet Service Definitions

The Network Activate software 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 Multipoint-to-Multipoint Ethernet Service Definitions on page 521](#)
- [Predefined Point-to-Point Service Definitions on page 477](#)

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 237](#).

The Network Activate 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.

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 27 on page 555](#) lists each of the standard VPLS service definitions. Each standard service definition is then described in detail in the sections that follow.

Table 27: Standard Point-to-Multipoint Service Definitions

Standard Service Definition Name	Service Attributes
“ELAN-Hub-Spoke-QinQ-AllVLAN” on page 475	<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 476	<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

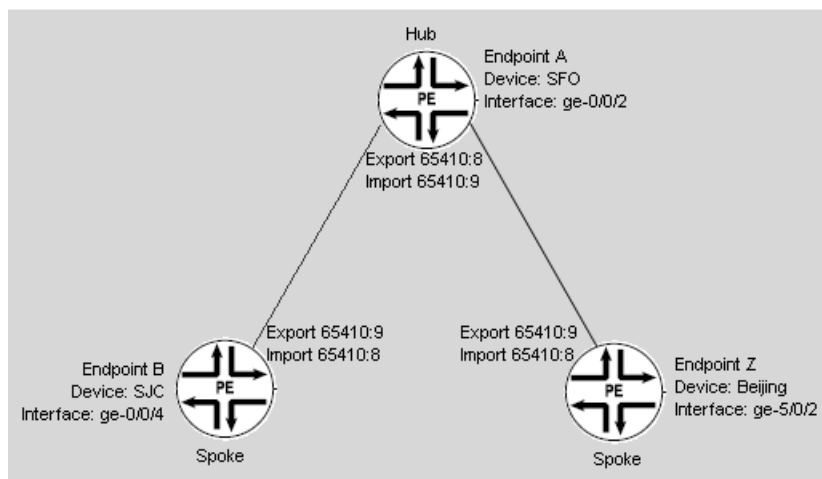
IN THIS SECTION

- Configuration on Endpoint A | 557
- Configuration on Endpoint B | 559
- Configuration on Endpoint Z | 561

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 17 on page 474](#)—a point-to-multipoint service with one hub and two spokes.

Figure 20: Point-to-Multipoint Service with One Hub



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

IN THIS SECTION

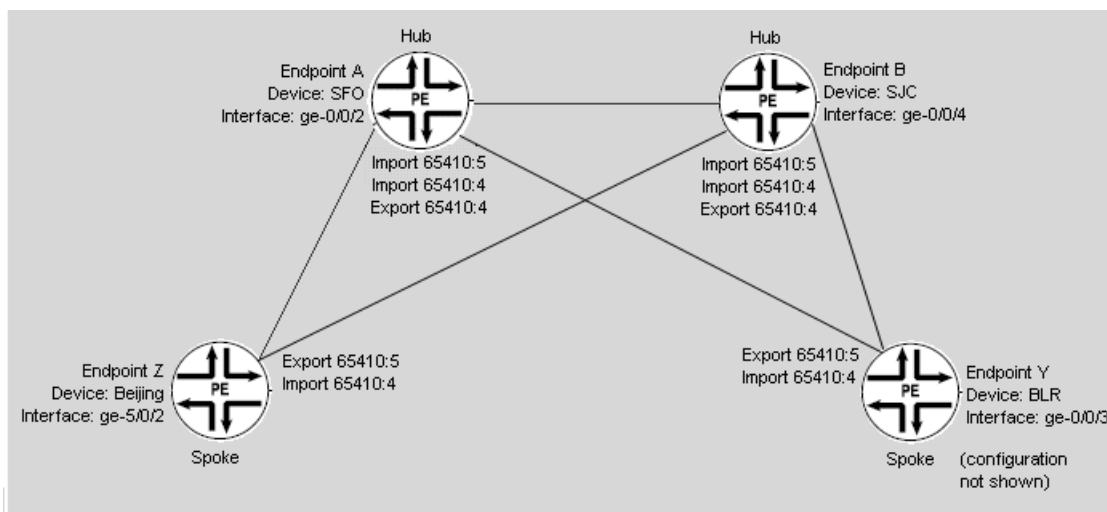
- Configuration on Endpoint A | 564
- Configuration on Endpoint B | 567
- Configuration on Endpoint Z | 569

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 21 on page 564](#) 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 21 on page 564](#)—a point-to-multipoint service with two service hubs and two spokes. The configuration for endpoint Y is not described.

Figure 21: Point-to-Multipoint Service with Two Hubs



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_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-0/0/2_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 | 237](#)

[Predefined Multipoint-to-Multipoint Ethernet Service Definitions | 521](#)

[Predefined Point-to-Point Service Definitions | 477](#)

Predefined Full Mesh Layer 3 VPN Service Definitions

The Network Activate software 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 376](#).

The Network Activate software 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 12 on page 187](#) lists each of the standard VPLS service definitions. Each standard service definition is then described in detail in the sections that follow.

Table 28: Standard Point-to-Multipoint 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 | 376](#)

[Predefined Multipoint-to-Multipoint Ethernet Service Definitions | 521](#)

[Predefined Point-to-Point Service Definitions | 477](#)

Predefined Hub-and Spoke Layer 3 VPN Service Definitions

The Network Activate software 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 double-clicking the service definition.

You can also view service instance details by selecting **Service Provisioning > Manage Service Orders**.

[Table 29 on page 573](#) 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 [Creating a Layer 3 VPN Hub-and-Spoke Service Definition](#).

Table 29: 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 | 267](#)
[Creating a Hub-and-Spoke \(One Interface\) Layer 3 VPN Service Definition | 386](#)
[Predefined Full Mesh Layer 3 VPN Service Definitions | 571](#)
[Creating a Full Mesh Layer 3 VPN Ethernet Service Order | 718](#)
[Predefined Point-to-Point Service Definitions | 477](#)
[Predefined Multipoint-to-Multipoint Ethernet Service Definitions | 521](#)
[Predefined Point-to-Multipoint Ethernet Service Definitions | 554](#)

3

PART

Service Orders

Service Order Operations | **575**

Layer 2 VPLS Service Orders | **660**

Layer 3 VPN Service Orders | **715**

Service Order Operations

IN THIS CHAPTER

- Service Order States and Service States Overview | 576
- Creating a Service Order | 577
- Creating a Point-to-Point ATM or TDM Pseudowire Service Order | 578
- Creating a Point-to-Point Service Order | 586
- Cloning Deployed Point-to-Point Services | 602
- Creating a Bulk-Provisioning Service Order for Pseudowire Services | 606
- Inverse Multiplexing for ATM Overview | 612
- Creating an Inverse Multiplexing for ATM Service Order | 613
- Creating a Cross Provisioning Platform Service Order | 616
- Viewing Service Orders | 620
- Viewing Cross Provisioning Platform Service Order Details | 622
- Service Lock for Cross Provisioning Platform | 625
- Modifying a Saved Service Order | 628
- Deploying a Service Order | 631
- Force-Deploying a Service | 632
- Viewing the Configuration of a Pending Service Order | 634
- Provisioning a Single-Ended Point-to-Point Service | 636
- Selecting Specific LSPs for Network Activate Services | 638
- Validating a Service Order | 643
- Stitching Two Point-to-Point Pseudowires | 645
- Providing Broadband Network Gateway Service Support with Cross Provisioning Platform | 648
- Deleting a Partial Configuration | 654
- Deleting a Service Order | 655
- Re-creating a Cross Provisioning Platform Service Order After a Failed Deployment | 656
- Re-creating a Cross Provisioning Platform Service Order After a Successful Deployment | 657
- Viewing the Script Output on the Service Orders Inventory Page | 658

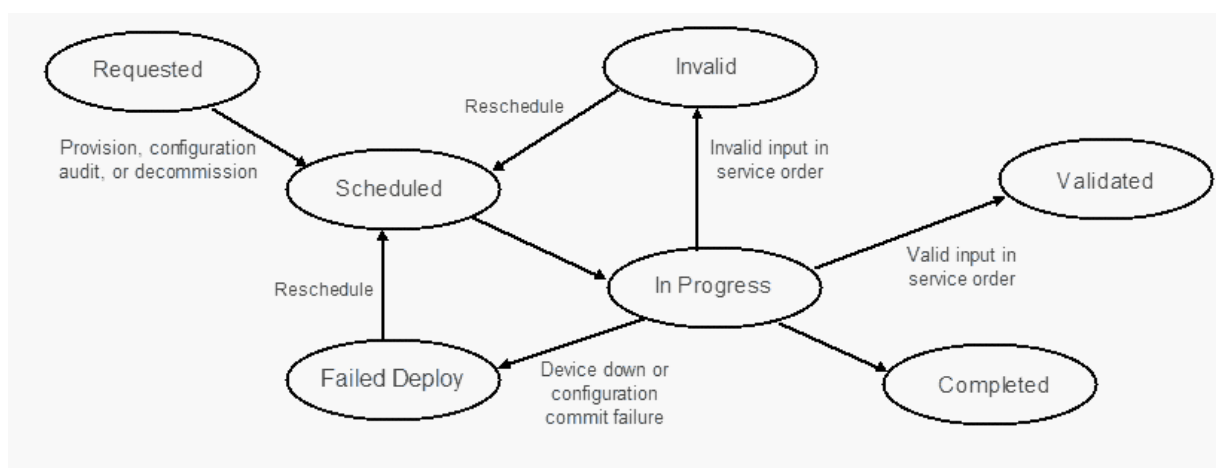
Service Order States and Service States Overview

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 22 on page 576](#).

Figure 22: 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 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.

When you cancel a job, the service order may not fail in Cross Provisioning Platform 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 **Requested** 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 **Requested**, you can modify and deploy or delete the service order.

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

[Viewing Service Orders | 620](#)

[Viewing Services | 832](#)

[Deploying a Service Order | 631](#)

[Understanding Service Validation | 875](#)

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 586](#)

To create a VPLS service order, see [“Creating a Multipoint-to-Multipoint VPLS Service Order” on page 660](#) or [“Creating a Point-to-Multipoint VPLS Service Order” on page 678](#).

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 | 578](#)
2. [Entering General/Connectivity Settings Information | 579](#)
3. [Specifying Endpoint Information | 582](#)
4. [Deploying the New Service | 585](#)

Selecting the Service Definition

To select a service definition on which to base the new service order:

1. In the Network Activate task pane, select **Service Provisioning > Manage Service Orders > Create P2P Service Order**.


The **Create P2P Service Order** page displays an inventory of all available point-to-point service definitions.

2. Select the service definition you want to base your service order on, and click **Next**.

A graphical image of a service order appears.

Service Provisioning > Manage Service Orders > Create P2P Service Order

Definition: ATM-AAL5 pseudowire



Endpoint-A

Connectivity

Endpoint-Z

General/Connectivity Settings

General Settings

Name: atm-service-order

Customer: customer_2085

Comments:

Connectivity Settings

VPI: 34

VCI: 23

Auto pick VC ID: ☒

Back Next Create Cancel

The image in the left panel of the main display area has multiple selectable elements. The right panel requests information depending on which element is selected.

If a template was attached to the service definition on which the service order is based, the link to invoke the template editor also appears in the bottom of the right panel.

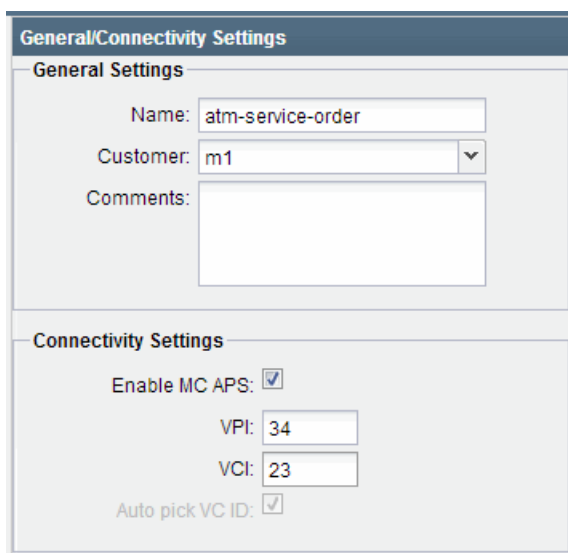
The two router images represent the two endpoints of the point-to-point service. Text above the cloud image provides general information about the service. The cloud represents the connectivity across the network between the two endpoints.

When you select the cloud or the text, the right panel requests general information about the service order as well as connectivity information.

The **General/Connectivity Settings** panel appears initially in the right panel, as shown in the example.

Entering General/Connectivity Settings Information

The **General Settings** panel is displayed on the right side of the service order window.



General/Connectivity Settings

General Settings

Name: atm-service-order

Customer: m1

Comments:

Connectivity Settings

Enable MC APS: ☒

VPI: 34

VCI: 23

Auto pick VC ID: ☒

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 1056](#).

3. In the **Comments** 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 169](#).

9. Enter the **Route Distinguisher** value.

NOTE: The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to <http://www.iana.org/assignments/ipv4-address-space> for the list of restricted IPv4 addresses and <http://www.iana.org/assignments/ipv6-address-space> for the list of restricted IPv6 addresses.

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.

NOTE: The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to <http://www.iana.org/assignments/ipv4-address-space> for the list of restricted IPv4 addresses and <http://www.iana.org/assignments/ipv6-address-space> for the list of restricted IPv6 addresses.

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.

The service templates settings are the same for both the endpoints.

To configure the endpoint settings:

1. In the **PE Device** box, 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.

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 645](#).

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 165](#).

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. If you have attached a service template in the service definition, the **Flexible Service Attributes** link appears. To enable this link, select a **PE Device**. Click the link to modify the service template attributes. For more information about configuring the flexible service attributes, see [“Configuring Flexible Service Attributes to Modify Service Template Attributes” on page 938](#)
11. 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 > Services > NA > service order name**.

For more information on topology, see [“Junos Space Network Topology Overview” on page 31](#).

Deploying the New Service

To deploy the new service:

1. Perform one of the following actions:
 - To save the request without deploying the service, select **Save only**, then click **OK**.
See [“Deploying a Service Order” on page 631](#) for information about how to deploy a saved service at a later time.
 - 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. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details.

Related Documentation

[Warning: element unresolved in stylesheets: <title> (in <related-topics>). This is probably a new element that is not yet supported in the stylesheets.]

Related Documentation

[Prestaging ATM and TDM Pseudowire Devices | 46](#)

[Prestaging ATM and TDM Pseudowire Devices | 46](#)

[Creating a Point-to-Point ATM or TDM Pseudowire Service Definition | 270](#)

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 Definition | 586](#)
2. [Entering General Settings Information | 587](#)
3. [Specifying the Connectivity | 588](#)
4. [Specifying QoS Settings | 591](#)
5. [Specifying OAM Settings | 592](#)
6. [Specifying Endpoint Information | 592](#)
7. [Specifying Connectivity and Endpoint Information for Managing VLANs | 598](#)
8. [Deploying and Monitoring the Progress of the New Service | 601](#)

Selecting the Service Definition

To select a service definition on which to base the new service order:

1. In the Network Activate task pane, select **Service Provisioning > Manage Service Orders > Create P2P Service Order**.


The **Create P2P Service Order** page displays an inventory of all available point-to-point service definitions.

2. Select the service definition you want to base your service order on, and click **Next**.

A graphical image of a service order appears.

Service Provisioning > Manage Service Orders > Create P2P Service Order

Definition: p2p_test



Endpoint-A Connectivity Endpoint-Z

General/Connectivity Settings

General Settings

Name:

Customer:

Comments:

Connectivity Settings

MTU: 1522

Auto pick VC ID: ☒

OAM Settings

CFM Definition:

Back Next Create Cancel

The image in the left part of the main display area has multiple selectable elements. The right panel requests information depending on which element is selected.

If a template is attached to the service definition on which the service order is based, the link to invoke the template editor also appears in the bottom of the right panel.

The two router images represent the two endpoints of the point-to-point service. Text above the cloud image provides general information about the service. The cloud represents the connectivity across the network between the two endpoints.

When you select the cloud or the text, the right panel requests general information about the service order as well as connectivity information.

The General/Connectivity Settings panel appears initially in the right panel, as shown in the example.

Entering General Settings Information

To enter General Settings in the **General Settings** box:

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 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.

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 1056](#).

3. In the **Comments** 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.

4. Configure connectivity settings. See [“Specifying the Connectivity” on page 588](#).

Specifying the Connectivity

In the **Connectivity Settings** box of the General/Connectivity Settings panel, specify VCID and MTU information.

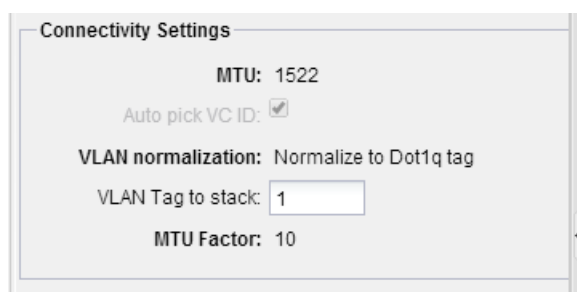
1. Specify the VCID. This is an integer that uniquely identifies the virtual circuit that the service will use.

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.



Connectivity Settings

MTU: 1522

Auto pick VC ID: ☒

VLAN normalization: Normalize to Dot1q tag

VLAN Tag to stack:

MTU Factor: 10

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 **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.

For more information on multichassis link aggregation groups (MC-LAGs), see “[Multichassis Link Aggregation Group Overview](#)” on page 168.

4. Specify the **Route Distinguisher** value.

NOTE: The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to <http://www.iana.org/assignments/ipv4-address-space> for the list of restricted IPv4 addresses and <http://www.iana.org/assignments/ipv6-address-space> for the list of restricted IPv6 addresses.

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.

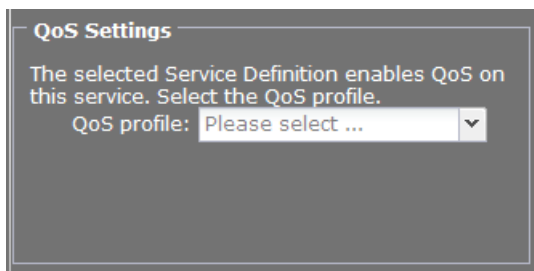
NOTE: The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to <http://www.iana.org/assignments/ipv4-address-space> for the list of restricted IPv4 addresses and <http://www.iana.org/assignments/ipv6-address-space> for the list of restricted IPv6 addresses.

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 **Outer VLAN Tag to stack** and **Inner VLAN Tag to stack** fields.
Default: 1
Range: 1 through 4094
9. To 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.
10. If you have enabled QoS, configure QoS settings. See “[Specifying QoS Settings](#)” on page 591.
If QoS is not enabled, configure endpoint settings. See “[Specifying Endpoint Information](#)” on page 592.

Specifying QoS Settings

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 QoS Design software.

A QoS profile classifies traffic into defined service groups to provide the special treatment of traffic across the network service.

NOTE: For OAM Settings, if you specify a CFM profile (for example, a CFM action profile with remote MEP), or an SLA-lterator 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.

2. In the **CIR** field, select the committed information rate (CIR) from the list.

The CIR is the guaranteed rate and specifies the minimum bandwidth available if all sources are active at the same time. Make sure that the CIR value is less than the PIR value.

NOTE: For bursty traffic, the CIR represents the average rate of traffic per unit time and the PIR represents the maximum amount of traffic that can be transmitted in a given interval.

3. In the **PIR** field, select the peak information rate (PIR) from the list. The PIR is the shaping rate.

NOTE: If the QoS profile that you selected in Step 1 is configured with a level-three scheduler and interface oversubscription is enabled, then PIR is not used.

4. Configure endpoint information. See [“Specifying Endpoint Information” on page 592](#).

Specifying OAM Settings

If OAM is enabled on the service definition, enter information in the OAM Settings of the General/Connectivity Settings panel.

1. In the **CFM Definition** 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.

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. Configure endpoint information. See [“Specifying Endpoint Information” on page 592](#).

Specifying Endpoint Information

An example **Endpoint Settings** window follows.

Endpoint Settings

PE device: PE1_re0

UNI interface: em1

UNI description:

Physical IF: vlan-ccc
encapsulation:

Traffic type: DOT1Q Transport single vlan

Logical IF Settings

Logical IF: vlan-ccc
encapsulation:

Auto Pick UnitID:

UnitID: 1

Auto pick VLAN ID:

VLAN ID: 1

MTU (Bytes): 1522

LSP name: PE1_to_P1

Outgoing label: 1000000

Enable send-oam config:

Backup settings

Enable:

PE device: PE1_re0

UNI interface: em1

MTU (Bytes): 1522

LSP name: PE1_to_PE2

Revert time (sec): 5

Switch Over Delay (sec): 0

Outgoing label:

If a service template is attached to the service definition, a link to that template is listed at the bottom of the Endpoint Settings section of the window. 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 756](#).

Some of the fields differ from one interface type to another and also differ depending on permissions assigned in the service definition.

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.

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” on page 636](#).

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 645](#).

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. To change the committed information rate (CIR) on an endpoint, click the CIR value for the endpoint and select another value from the list. Make sure the CIR value is less than the PIR value.

Only QoS-enabled services specify CIR and PIR values.

14. To change the peak information rate (PIR) on an endpoint, click the PIR value for the endpoint and select another value from the list. Make sure the CIR value is less than the PIR value.

Only QoS-enabled services specify CIR and PIR values.

15. 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**.

16. 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 165](#).

17. 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.

18. If you have attached a service template in the service definition, the **Flexible Service Attributes** link appears. To enable this link, select a **PE Device**. Click the link to modify the service template attributes. For more information about configuring the flexible service attributes, see [“Configuring Flexible Service Attributes to Modify Service Template Attributes” on page 938](#).

19. To provide endpoint information for the second endpoint, click the **Endpoint Z** graphic element (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).

20. Click **Create**.

The deployment options window appears.

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**.

For more information on topology, see [“Junos Space Network Topology Overview” on page 31](#).

Specifying Connectivity and Endpoint Information for Managing VLANs

The Network Activate application in Junos Space release 14.1 provides greater flexibility for provisioning VLANs for Point-to-Point service orders.

Network Activate release 14.1 extends the VLAN normalization options.

NOTE: Prior to release 14.1, Network Activate enabled specification of the VLAN normalization types **Swap** and **Normalize to None** only.

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.

General/Connectivity Settings

General Settings

Name:
Customer: Please select ...
Comments:

Connectivity Settings

MTU: 1522
Auto pick VC ID: ☒
VLAN normalization: Normalize to QinQ tags
Outer VLAN tag to stack:
Inner VLAN tag to stack:
MTU Factor: 10

QoS Settings

The selected Service Definition enables QoS on this service. Select the QoS profile.
QoS profile: Please select ...

OAM Settings

CFM Definition: Please select ...

◀ Back

Next ▶

Create

Cancel

Network Activate 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**.

General/Connectivity Settings

General Settings

Name:

Customer:

Please select ...

Comments:

Connectivity Settings

MTU:

1522

Enable MC LAG:

☒

Auto pick VC ID:

☒

VLAN normalization:

Normalize to Dot1q tag

VLAN Tag to stack:

1


MTU Factor:

10

OAM Settings

CFM Definition:

Please select ...



◀

▶

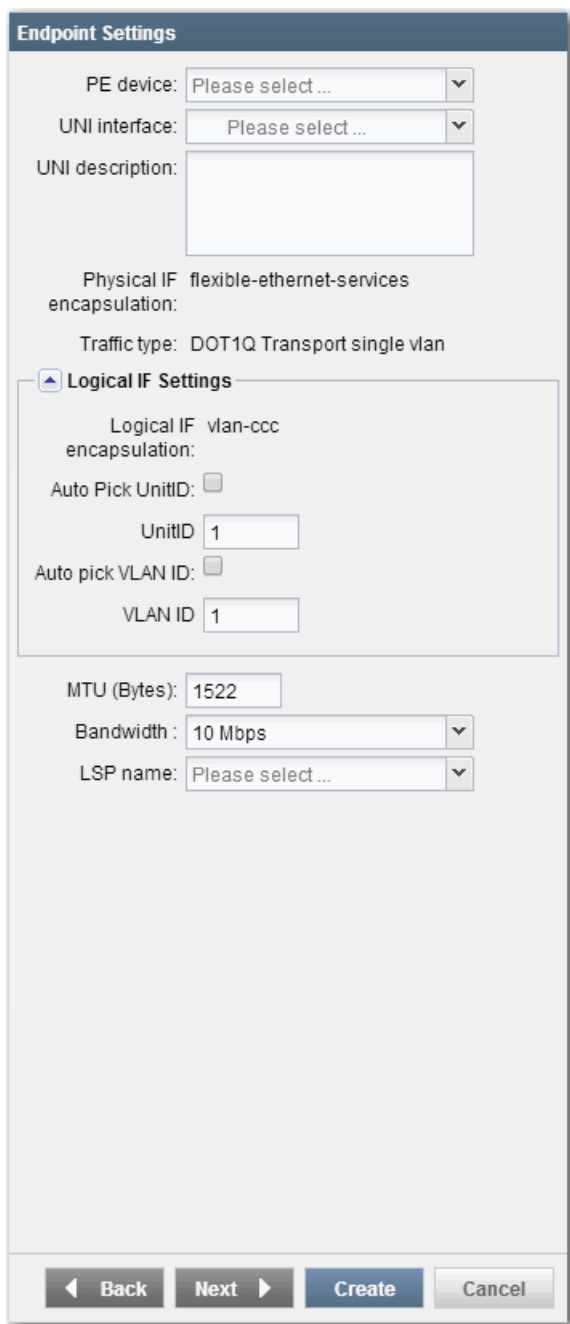
◀ Back

Next ▶

Create

Cancel

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.



Endpoint Settings

PE device:

UNI interface:

UNI description:

Physical IF flexible-ethernet-services
encapsulation:

Traffic type: DOT1Q Transport single vlan

Logical IF Settings

Logical IF vlan-ccc
encapsulation:

Auto Pick UnitID: ☐

UnitID

Auto pick VLAN ID: ☐

VLAN ID

MTU (Bytes):

Bandwidth:

LSP name:

Deploying and Monitoring the Progress of the New Service

To deploy the new service:

1. Perform one of the following actions:

- To save the request without deploying the service, select **Save only**, then click **OK**.

See [“Deploying a Service Order” on page 631](#) for information about how to deploy a saved service at a later time.

- 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.

See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details.

RELATED DOCUMENTATION

[Viewing Service Orders | 620](#)

Viewing Jobs in the *Junos Space Network Application Platform User Guide*

[Service Attributes Overview | 152](#)

[Adding a New Customer | 1056](#)

[Deploying a Service Order | 631](#)

[Creating a Point-to-Multipoint VPLS Service Order | 678](#)

[Creating a Service Order Based on a Service Definition with a Template | 756](#)

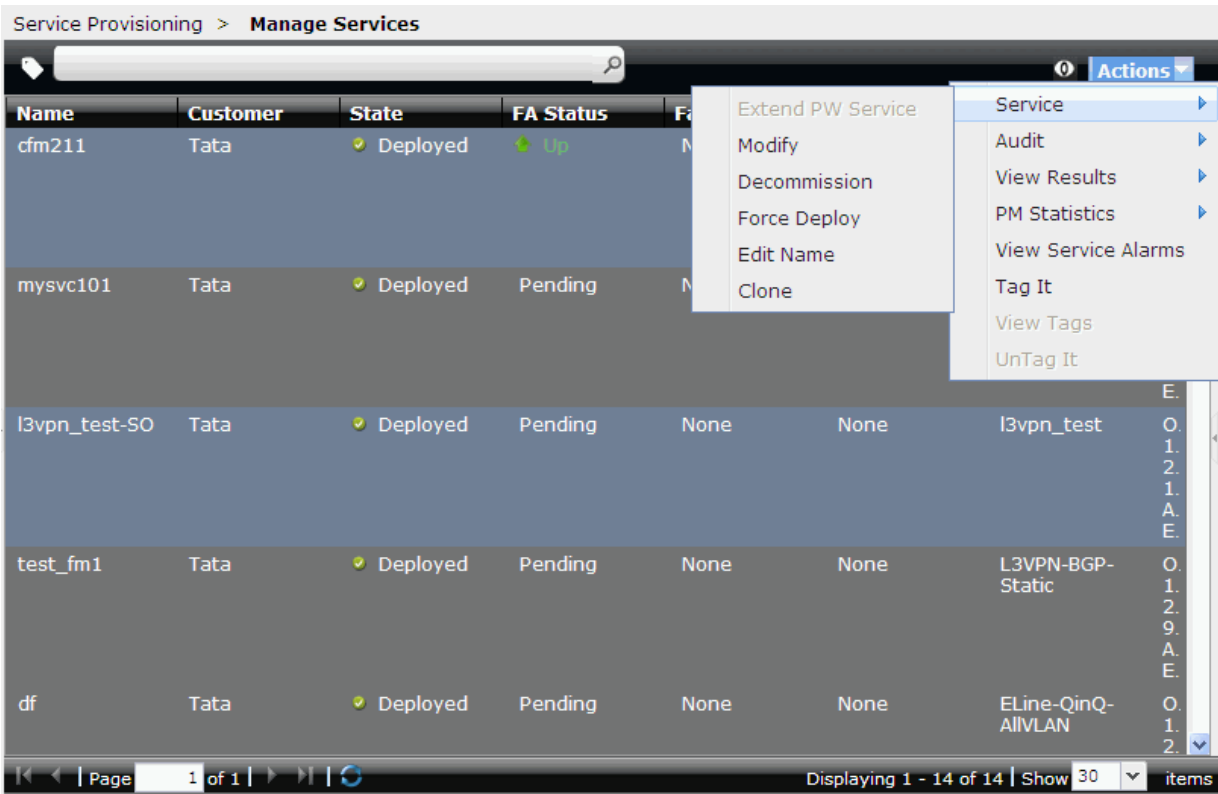
Cloning Deployed Point-to-Point Services

You can use a deployed Eline-LDP service as a template to create multiple point-to-point services. Cloning can be used to create a maximum of fifteen copies of an existing service

Prerequisites for Cloning a Deployed Service

- At least one deployed point-to-point service with two endpoints defined.

To begin the cloning service order, in the **Network Activate** task pane, select **Service Provisioning > Manage Services**. The service inventory page appears.



1. Locate the entry for a service that has two endpoints defined.
2. Right-click on the service to see the list of available actions, and select **Clone Service**. The **Clone Service** window appears in which you manage the copied instances of the service.

Service Provisioning > Manage Services

General Settings

Service definition:

mySD

Service name:

cfm211

Customer:

Tata

Signaling:

LDP

Service template:

BurstSize

CFM definition:

StdDef-CFMSERVICE

Delete

Add

5

copies

Total clones: 0

Create

Cancel

The **Clone Service** window enables you to specify the number of copies to create from the source deployed service. In this case, we are creating 3 copies of the source service.

a.

Service Provisioning > Manage Services

General Settings

Service definition: mySD
Service name: cfm211
Customer: Tata
Signaling: LDP
Service template: BurstSize
CFM definition: StdDef-CFMSERVICE

Delete
Add
 copies
Total clones: 0

General			A Endpoint			Z Endpoint				
<input type="checkbox"/>	Name	VCID	Device	Interface	Bandwidth	VLAN ID	Device	Interface	Bandwidth	V.
<input checked="" type="checkbox"/>	cfm211	211	junos-mx480-space	ge-5/0/5	64 Kbps	211	junos-space1	ge-0/1/5	64 Kbps	2

Create
Cancel

Each row in the clone table represents one point-to-point service with two endpoints. The top row is the deployed service you used to create the copies. The parameters displayed in the attributes table differ based on the definition of the source deployed service. For example, if the original service was an ATM interface definition, the parameters will include VCI and VPI as column headers.

You can edit many of the attribute values of the cloned services as necessary by clicking on the cells in the table. One of the attributes you must change is the **Interface** for each new service. You may edit the other fields as necessary. For example, the **Order name** is auto-generated from the original service name. If you want to change it, just click on the cell and enter a new name. The editable attributes are

- Name
- VCID
- Device
- Interface
- Bandwidth
- VLAN ID

All other attributes, such as MTU, are copied from the original service and will not appear in the attributes table.

You may also select one of the copies and create clones from that so that the copies have the same attributes as the clone that you selected.

Once you have finished editing the service values, click **Create** to deploy the cloned services. You will be given the standard deployment options.

RELATED DOCUMENTATION

[Creating a Point-to-Point Service Order | 586](#)

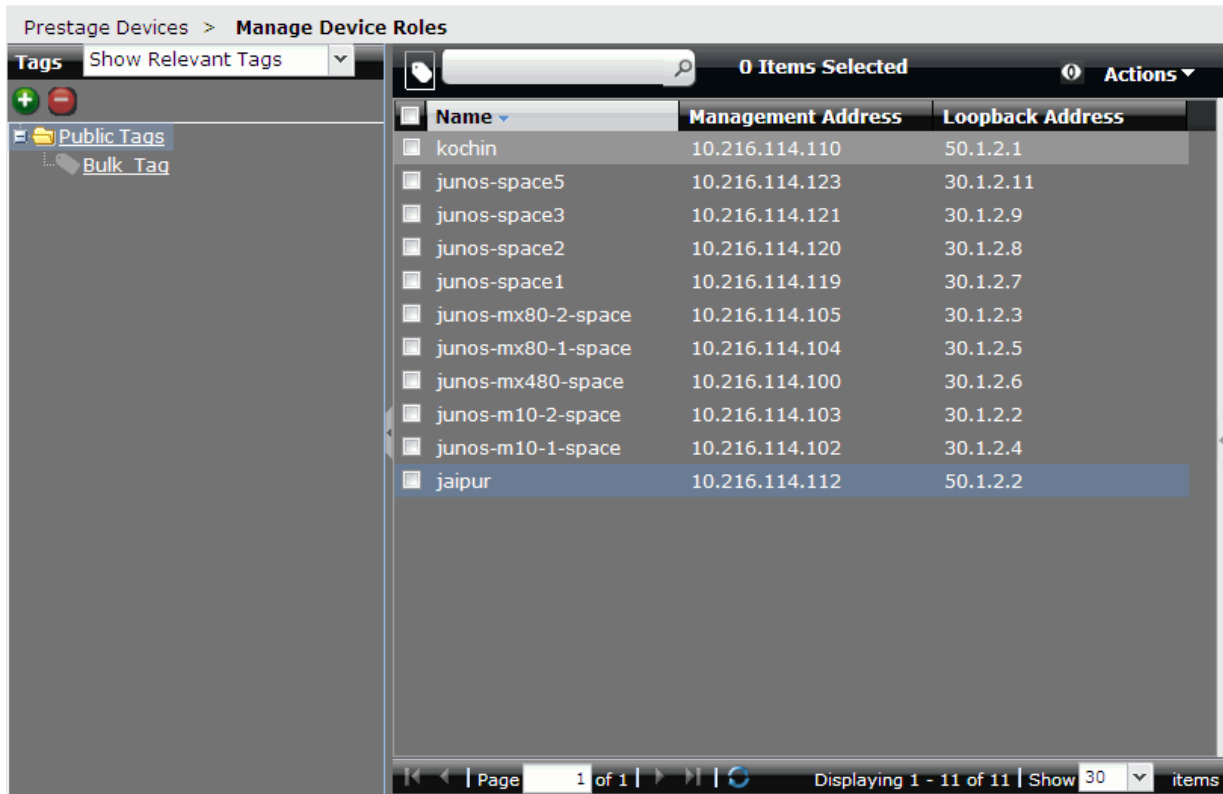
[Example: Configuring and Deploying a Point-to-Point Ethernet Service | 960](#)

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

- 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.



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.

Service Design > **Manage Service Definitions**

Search 0 Actions

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

Publish Service Definition
Unpublish Service Definition
Delete Service Definition
Create Bulk P2P Service Order
Tag It
View Tags
UnTag It

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 an E-Line Service Definition” on page 188.</p>

Field	Action
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.

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.
----------------------	-------------------------------------------------

Field	Action
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.

7. 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.

For more information on topology, see [“Junos Space Network Topology Overview” on page 31](#).

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](#) | 270

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

[Creating an Inverse Multiplexing for ATM Service Order | 613](#)

[Viewing Functional Audit Results for an Inverse Multiplexing for ATM Service | 1086](#)

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 Network Activate application.

To create an Inverse Multiplexing for ATM service order:

1. In the Network Activate task pane, select **Service Provisioning > Manage Service Orders > Create P2P Service Orders**. The **Create P2P Service Order** window appears.
2. Select the service definition upon which you want to create the service order. The **Create P2P Service Order** window appears. The left panel displays a representation of the connection you are configuring. The right panel displays the **General/Connectivity Settings**.

Service Provisioning > Manage Service Orders > Create P2P Service Order

Definition: ATM pseudowire

Endpoint-A — Connectivity — Endpoint-Z

General/Connectivity Settings

General Settings

Name: IMA-test-prov

Customer: Airtel

Comments:

Connectivity Settings

VPI: 5

VCI: 10

Auto pick VC ID: ☐

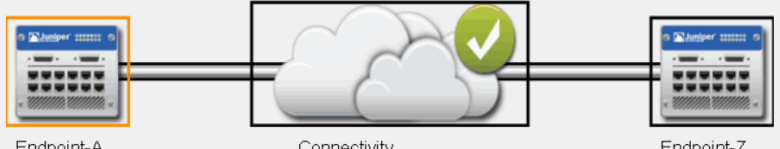
VCID: 1

Back Next Create Cancel

3. Fill in the fields in the **General/Connectivity** panel.
4. Click **Next**. The **Endpoint Settings** panel for Endpoint A appears.

Service Provisioning > Manage Service Orders > Create P2P Service Order

Definition: ATM pseudowire
Service Order Name: IMA-test-prov
Customer: Airtel



Endpoint-A

Connectivity
Virtual Circuit ID: 1

Endpoint-Z

Endpoint Settings

PE device: junos-space5

UNI interface: at-0/0/16

UNI description:

Physical IF encapsulation: atm-ccc-cell-relay

Logical IF encapsulation: atm-ccc-cell-relay

RSVP LSP name: Please select ...

Cell bundle size: 1


Back Next Create Cancel

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.

Service Provisioning > Manage Service Orders > Create P2P Service Order

Definition: ATM pseudowire
Service Order Name: IMA-test-prov
Customer: Airtel



Endpoint-A
Device: junos-space5
Interface: at-0/0/16

Connectivity
Virtual Circuit ID: 1

Endpoint-Z

Endpoint Settings

PE device: exora

UNI interface: at-0/2/0

UNI description:

Physical IF encapsulation: atm-ccc-cell-relay

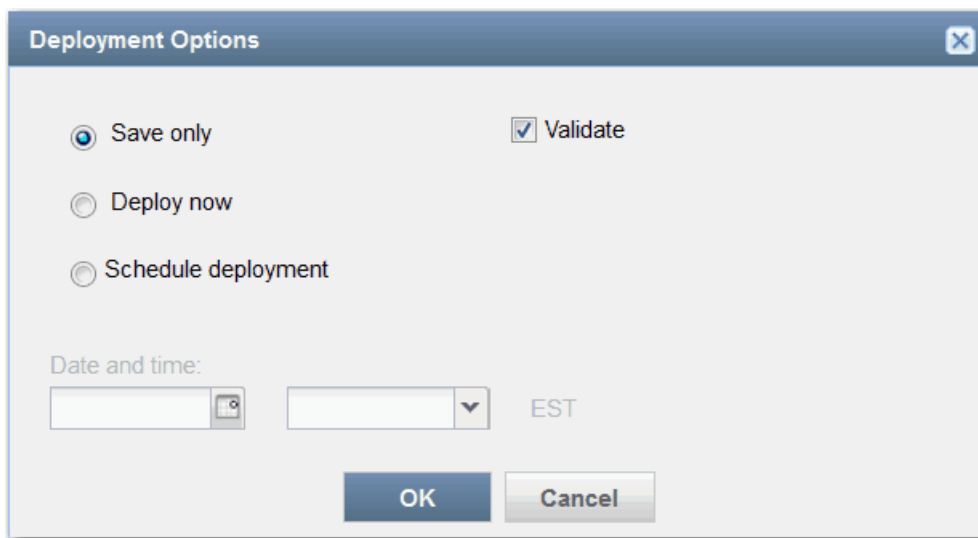
Logical IF encapsulation: atm-ccc-cell-relay

RSVP LSP name: Please select ...

Cell bundle size: 1

Back Next Create Cancel

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 **Create**. The **Deployment Options** window appears.

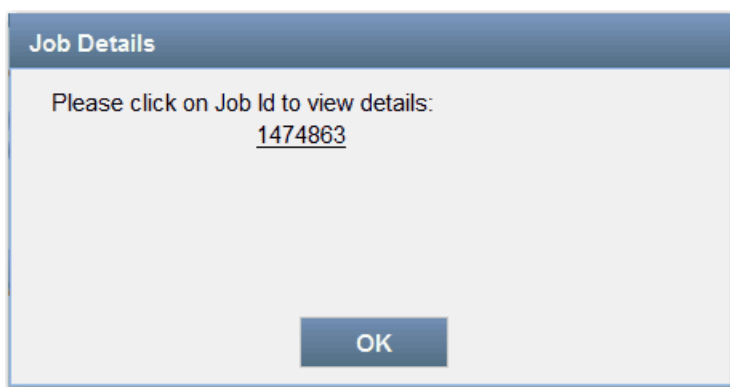


The **Deployment Options** dialog box has a title bar with a close button. It contains three radio buttons: **Save only** (selected), **Deploy now**, and **Schedule deployment**. To the right of the radio buttons is a checked checkbox labeled **Validate**. Below the radio buttons is a section labeled **Date and time:** with two input fields (one for date, one for time) and a dropdown menu currently showing **EST**. At the bottom are **OK** and **Cancel** buttons.

9. Select the deployment option you want and click **OK**:

- **Save only**
- **Deploy now**
- **Schedule deployment** (Specify the date and time.)

The Network Activate application displays the **Job Details** window, which includes a **Job Details ID** number.



The **Job Details** dialog box has a title bar. The main text says "Please click on Job Id to view details:" followed by the number 1474863. At the bottom is an **OK** button.

10. In the Network Activate task pane, select **Jobs > Job Management**.
11. In the **Job Management** window, you can view the status of the service that corresponds to the **Job Details ID** number.

RELATED DOCUMENTATION

- [Inverse Multiplexing for ATM Overview | 612](#)
- [Viewing Functional Audit Results for an Inverse Multiplexing for ATM Service | 1086](#)

Creating a Cross Provisioning Platform Service Order

Before you create a Cross Provisioning Platform service order, you must complete the following tasks:

- Import into the system the scripts that define the Juniper Networks devices.
- Import into the system the scripts that define the third-party devices.
- Create the service definition upon which to base the service order.

To create a Cross Provisioning Platform service order:

1. in the **Cross Provisioning Platform** task pane, select **CPP > Service Orders**.
2. In the **Service Orders** window, click the + button. The **Create CPP Service Order** window appears.

CPP > Service Orders > Create CPP Service Order

Create CPP Service Order

General Settings

Select Service Definition

ID	Name	Type
	VPLS_SD	VPLS
	P2P_SD	PW-LDP
5678	Test_SD_123	PW-LDP
1234	Test_123_P2P	PW-LDP
4321	Test_123_VPLS	VPLS
7654	Test_SD_L3VPN	L3VPN
	L3VPN-SD	L3VPN

Page 1 of 1 | Displaying 1 - 7 of 7 | Show 30 items

Description:

Next Cancel

3. In the **General Settings** section, select a service definition based on the unique ID, name or type.

NOTE: The value in the **ID** field is associated with a service definition. This identifier can be used when you are searching for a particular service definition while creating a device configlet order. You can search the service definition by its name, type or unique ID. You can modify the ID only during the migration of old service definition IDs.

4. In the **Order description** field, enter a description of the service that distinguishes its operation from others.
5. Click **Next**.

The Endpoint Settings window appears.

NOTE: The following representation of the Endpoint Settings window is a sample only. The appearance of this window is based on the scripts that are associated with the service definition upon which the service is based.

The screenshot displays the 'Endpoint Settings' window with the following sections:

- General**: Includes a 'Name' text field.
- Jumbo**: Contains two checkboxes, 'Jumbo frame 3900?' and 'Jumbo frame 9000?'.
- Site B Selector**: Features a 'Site B port type' dropdown menu currently set to 'Customer Facing Port'.
- Site A - Customer Facing Port**:
 - 'Site name': Dropdown menu (Please select).
 - 'Resync now': Checkbox.
 - 'Port': Dropdown menu (Please select).
 - 'Service speed': Dropdown menu (1mbs).
 - 'Canoga device?': Checked checkbox.
 - 'Anda untagged?': Unchecked checkbox.
 - 'Outer encapsulation': Text field (Please enter) with a 'Validate' checkbox.
 - 'UnTagged / 802.1q?': Unchecked checkbox.
 - 'Inner encapsulation': Text field (Please enter).
 - L2 Extension** (checked):
 - 'Site name': Dropdown menu (Please select).
 - 'UNI port': Dropdown menu (Please select).
 - 'Uplink port': Dropdown menu (Please select).
 - 'UNI encapsulation': Text field (Please enter) with a 'Validate' checkbox.
- Site B - Customer Facing Port**:
 - 'Site name': Dropdown menu (Please select).
 - 'Resync now': Checkbox.
 - 'Port': Dropdown menu (Please select).
 - 'Service speed': Dropdown menu (1mbs).
 - 'Canoga device?': Checked checkbox.
 - 'Anda untagged?': Unchecked checkbox.
 - 'Outer encapsulation': Text field (Please enter) with a 'Validate' checkbox.
 - 'UnTagged / 802.1q?': Unchecked checkbox.
 - 'Inner encapsulation': Text field (Please enter).
 - L2 Extension** (checked):
 - 'Site name': Dropdown menu (Please select).
 - 'UNI port': Dropdown menu (Please select).
 - 'Uplink port': Dropdown menu (Please select).
 - 'UNI encapsulation': Text field (Please enter) with a 'Validate' checkbox.

At the bottom, there are three buttons: 'Create', 'Create More', and 'Cancel'.

6. Enter information for the parameters of the GUI script window according to the descriptions in the following table:

Parameter	Description
General	
Name	Enter a unique name for the service order to distinguish it from others that operate differently.
Jumbo	
Jumbo frame 3900	Sets the MTU frame size to 3900
Jumbo frame 9000	Sets the MTU frame size to 9000
	Default: 1596
Site B Selector	
Site B port type	Customer Facing Port Network Facing Port
Site A – Customer Facing Port	
Site name	Select the device from the list of devices displayed.
Resync now	Resyncs the interface on the selected device. NOTE: This parameter pertains to third-party devices only.
Port	Select a port from the list of ports displayed.
Service speed	Select the appropriate bandwidth for the selected site.
Canoga device?	If you select this check box, the software checks to determine whether the device is a Canoga device.
Anda untagged?	If you select this check box, the software checks to determine whether the device is an untagged Anda device.
Outer encapsulation	Enter an integer, or select the up or down arrow to select a value for the Outer encapsulation.
Validate	If this check box is selected, the system validates the encapsulation value with the specified site and port.

Parameter	Description
Untagged/802.1q?	If this check box is selected, the software checks to determine whether 802.1q was specified as the Ethernet option in UNI Settings.
Inner encapsulation	Enter an integer, or select the up or down arrow to select a value for the Inner encapsulation.

L2 Extension

Site name	Select the device from the list of devices displayed.
UNI port	Select a UNI port from the list of ports displayed.
Uplink port	Select a NNI port from the list of ports displayed.
UNI encapsulation	Enter an integer, or select the up or down arrow to select a value for the UNI encapsulation.
Validate	If this check box is selected, the system validates the encapsulation value with the specified site and port.

Site B – Customer Facing Port

Site name	Select the device from the list of devices displayed.
Resync now	Resyncs the interface on the selected device. NOTE: This parameter pertains to third-party devices only.
Port	Select a port from the list of ports displayed.
Service speed	Select the appropriate bandwidth for the selected site.
Canoga device?	If you select this check box, the software checks to determine whether the device is a Canoga device.
Anda untagged?	If you select this check box, the software checks to determine whether the device is an untagged Anda device.
Outer encapsulation	Enter an integer, or select the up or down arrow to select a value for the Outer encapsulation.
Validate	If this check box is selected, the system validates the encapsulation value with the specified site and port.

Parameter	Description
Untagged/802.1q?	If this check box is selected, the software checks to determine whether 802.1q was specified as the Ethernet option in UNI Settings.
Inner encapsulation	Enter an integer, or select the up or down arrow to select a value for the Inner encapsulation.
L2 Extension	
Site name	Select the device from the list of devices displayed.
UNI port	Select a UNI port from the list of ports displayed.
Uplink port	Select a NNI port from the list of ports displayed.
UNI encapsulation	Enter an integer, or select the up or down arrow to select a value for the UNI encapsulation.
Validate	If this check box is selected, the system validates the encapsulation value with the specified site and port.

7. Click **Create** or click **Create More** to provision additional endpoints.

RELATED DOCUMENTATION

[Creating a Cross Provisioning Platform Service Definition | 305](#)

[Viewing Cross Provisioning Platform Service Order Details | 622](#)

Viewing Service Orders

The following topic describes how you can view service orders.

- [Viewing Service Orders in a Table | 621](#)

Viewing Service Orders in a Table

To view and determine the status of service orders in a tabular form:

1. In the Network Activate task pane, select **Service Provisioning > Manage Service Orders**.
2. In the filter bar, click the table view icon.

A table of service orders on the system appears in the main display area.

[Table 30 on page 621](#) describes the fields in the service orders table.

Table 30: Fields in the Service Orders Table

Field	Description
Name	Name of the service order assigned during service creation or edit.
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 Network Activate software was unable to push the service configuration to a device configured for the service. • In-progress—Network Activate software 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.
Customer	Name of the enterprise customer who placed an order for the service.
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
Signaling	Type of signaling: <ul style="list-style-type: none"> • BGP • LDP
Created Date	Date that the service provisioner created the request.
Created By	Screen name of the service provisioner who created the service order.

3. To view details of a specific service order, double-click the table row that summarizes the service order.

For a point-to-point service order, a graphical illustration of the service order appears. See [“Creating a Point-to-Point Service Order” on page 586](#) for information about interpreting this graphic.

For a multipoint service order, a table of information about the service order appears. See [“Creating a Point-to-Multipoint VPLS Service Order” on page 678](#) for information about interpreting this graphic.

SEE ALSO

Creating a Point-to-Point Service Order 586
Creating a Multipoint-to-Multipoint VPLS Service Order 660
Deploying a Service Order 631
Deleting a Service Order 655

RELATED DOCUMENTATION

Deploying a Service Order 631
Deleting a Service Order 655
Viewing Services 832

Viewing Cross Provisioning Platform Service Order Details

To view the details of a Cross Provisioning Platform service order:

1. In the Cross Provisioning Platform task pane, select **CPP > Services**. The **CPP > Services** window appears, which displays a list of the provisioned Cross Provisioning Platform service orders.

CPP > Services

Actions

Name	Connectivity ID	State	Service Type	Definition	Activation Date
Juni_Modify	VCID:2147467271	Deployed	PW-LDP	221_Modify	Oct 14, 2013 12:04:14 PM EST
ALU_Juni	FOREIGNSVCID:217180 VCID:179604	Deployed	PW-LDP	221_Modify	Oct 14, 2013 12:00:23 PM EST
ALU_ALU	FOREIGNSVCID:217179 VCID:179603	Deployed	PW-LDP	Script_221	Oct 14, 2013 11:10:59 AM EST
ALU_Juniper	FOREIGNSVCID:217178 VCID:179602	Deployed	PW-LDP	Script_221	Oct 14, 2013 11:10:08 AM EST
J_J_default_MTU_01	VCID:2147467268	Deployed	PW-LDP	Script_221	Oct 14, 2013 10:58:21 AM EST
J_J_3900_02	VCID:2147467270	Deployed	PW-LDP	Script_221	Oct 14, 2013 10:55:59 AM EST
J_J_canoga_Untagged	VCID:2147467272	Deployed	PW-LDP	Script_221	Oct 14, 2013 10:54:00 AM EST
J_J_canoga	VCID:2147467279	Deployed	PW-LDP	Script_221	Oct 14, 2013 10:52:29 AM EST
J_J_Andra	VCID:2147467287	Deployed	PW-LDP	Script_221	Oct 14, 2013 10:50:26 AM EST
J_J_01	VCID:2147467267	Deployed	PW-LDP	Script_221	Oct 14, 2013 10:38:12 AM EST

- Double-click a listed service order, or select a service order and click on the **View Service Details** icon. The **CPP > Service Details** window appears, which displays the details of the service.

CPP Service Details

General

Service name: ElineService_target30K_vlan1472_58_57_0_0

Description: Service Creation between VMX80-el-R125(ge-0/0/8) and VMX80-el-R126(ge-0/0/8) Service Count: 100

External ID: ElineService_target30K_vlan1472_58_57_0_0

Administrative state: Deployed

Service type: PW-LDP

Service definition: script_221

Service Version: 1

Device Name	Mgmt IP	Port	Port Status	Parent Device	Role
VMX80-el-R125	10.216.202.114	ge-0/0/8.1472	Up		N_PE
VMX80-el-R126	10.216.202.113	ge-0/0/8.1472	Up		N_PE

Advanced Details For Device : VMX80-el-R125

General **Interface** Firewall Configuration

Attribute	Value
VCID	4525
MTU	8986
PseudoWire State	OL

Page 1 of 1 | Showing 10 items

Ok Refresh

A new field **Service Version** is added in the View Service Order Details and View Service Details windows. This field indicates the total number of times a service order or a service is modified. Each time you successfully modify a service order or a service, the service version number is incremented by one.

The **Advanced Details For Device** pane includes four tabs, which provide details on additional parts of the device configuration:

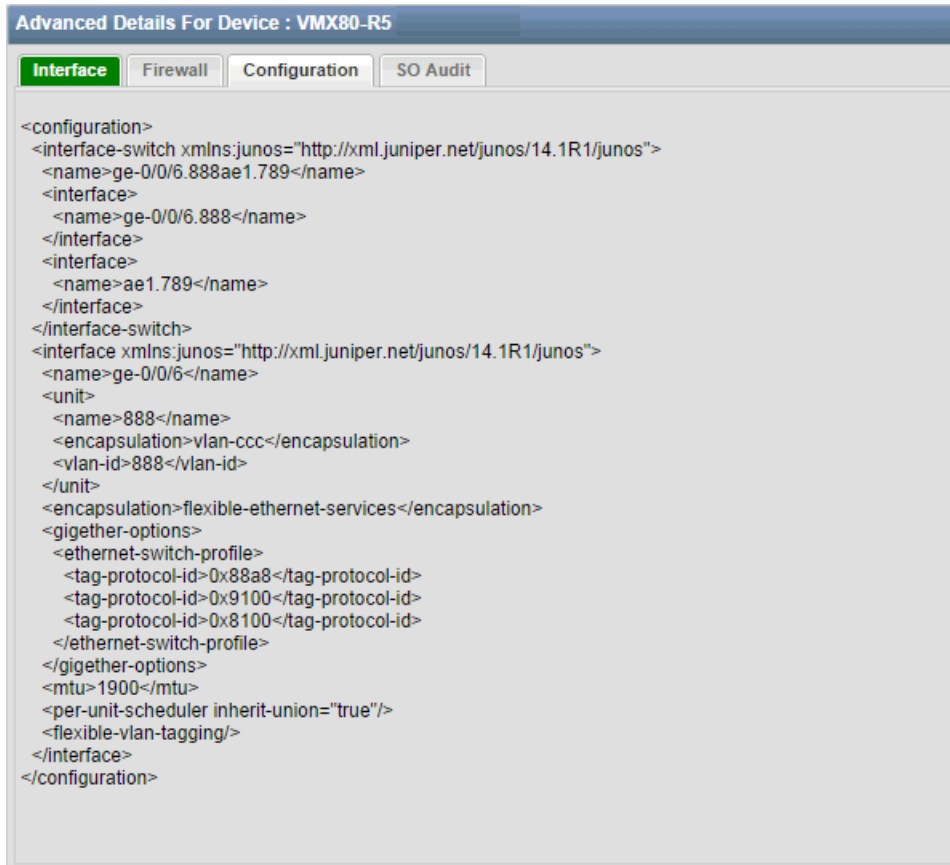
- **General** (See previous illustration.)—The **General** tab displays the **Mtu** and **Vcid** values for the device selected in the left panel.
- **Interface**—The **Interface** tab displays the **Mtu**, **OuterTag** and **VlanType** values for the device selected in the left panel.

Advanced Details For Device : junos-m10-2-space	
<div>General Interface Firewall Configuration</div>	
Attribute ▲	Value
Mtu	1596
OuterTag	3406
VlanType	q-in-q-all

- **Firewall**—The **Firewall** tab displays the **Ingress-filter** value for the device selected in the left panel.

Advanced Details For Device : junos-m10-2-space	
<div>General Interface Firewall Configuration</div>	
Attribute ▲	Value
Ingress-filter	ge-0/0/3CVLAN3406

- **Configuration**—The **Configuration** tab displays the configuration code for the device selected in the left panel.



RELATED DOCUMENTATION

[Creating a Cross Provisioning Platform Service Definition | 305](#)

[Creating a Cross Provisioning Platform Service Order | 616](#)

Service Lock for Cross Provisioning Platform

Multiple users might attempt to modify the same service at the same time. This conflict might cause another user's modifications to be overwritten. To overcome such a scenario, the Cross Provisioning Platform's service lock feature provides you the flexibility to serialize the service order creation, and allow only one operator to modify a service at any given time.

To enable the service lock feature:

1. Select **Network Management Platform > Administration > Applications**.

The Applications page displays the list of applications.

2. Right-click the Network Activate row and select **Modify Applications Settings**.

The Modify Network Activate Settings page displays the list of parameters that can be modified.

3. Select **Deployment**.

4. Select the **Check service version** check box.

5. Click **Modify**.

To identify the service order that is blocking you from modifying a service:

1. Select **Cross Provisioning Platform > CPP > Services**.

The Cross Provisioning Platform Services inventory page displays the list of services.

2. Right-click a service, and select **View Service Order**.

You are directed to the Cross Provisioning Platform Service Orders inventory page.

The Service Orders inventory page displays the list of service orders.

The Order State column helps you to decide if that service order is blocking you from modifying a service. If necessary, you can delete the failed or invalid service orders.

The **Service Version** field in the View Service Order Details and View Service Details windows indicates the total number of times a service order or a service has been modified. Each time you successfully modify a service order or a service, the service version number increases by one.

NOTE: For failed modifications the **Service Version** field does not increase.

When you create a service order, the View Service Order Details window displays the **Service Version** number as zero. When you modify a service, the **Service Version** in View Service Order Details window increases by one.

When you perform a configuration audit or view the service configuration changes, the service version in the View Service Details window does not change.

The following error messages are displayed when multiple operators attempt to modify a service at same time:

- There are multiple users trying to modify the current service concurrently. Please close the current window and try again.
- There are one or more pending service request(s) for this service. Please check the pending service order(s) for this service and take appropriate action as necessary.
- The service version in current service request is older/outdated than the latest service version. Please close the current window and try again.

RELATED DOCUMENTATION

[Creating a Cross Provisioning Platform Service Order | 616](#)

[Viewing Cross Provisioning Platform Service Order Details | 622](#)

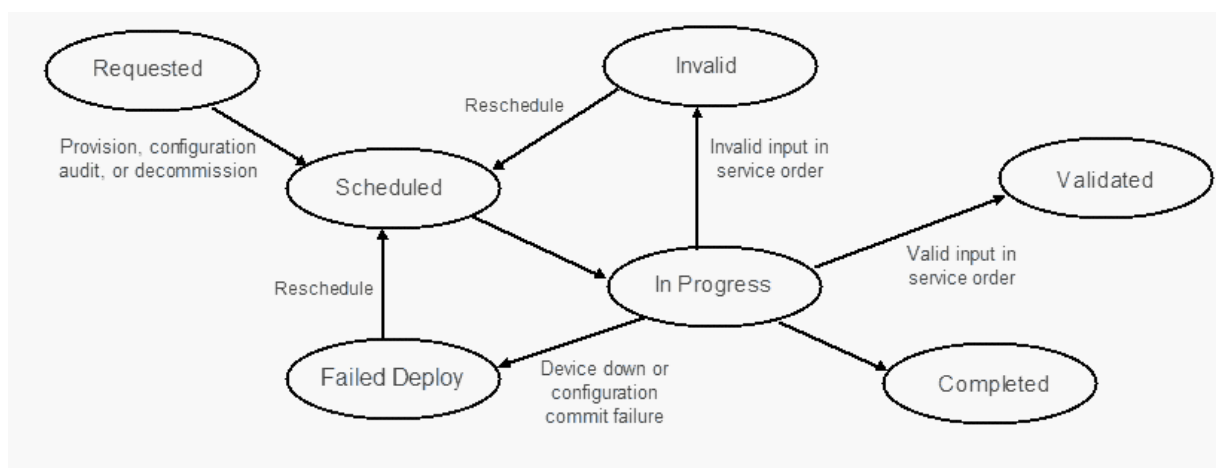
Modifying a Saved Service Order

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.

Figure 23 on page 628 illustrates the service order states.

Figure 23: Service Order States



To view the state of a service order, select **Network Activate > Service Provisioning > Manage Service Orders**. The Manage Service Orders inventory page lists the service orders and their state.

The Junos Space Network Activate 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. Select **Network Activate > Service Provisioning > Manage Service Orders**.
2. Right-click an existing service order, and then select **Service > 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.

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

Point-to-Point Service Order	VPLS Service Order	Layer 3 VPN Service Order
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	-
-	MAC table size	-
-	Disable tunnel services	-
-	Disable local switching	-
-	Fast reroute priority	-
-	Label block size	-
-	Connectivity type	-

NOTE: You can change a managed device to an unmanaged device, and an unmanaged device to a managed device. 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 | 578](#)

[Creating a Point-to-Point Service Order | 586](#)

[Creating a Multipoint-to-Multipoint VPLS Service Order | 660](#)

[Creating a Point-to-Multipoint VPLS Service Order | 678](#)

[Creating a Full Mesh Layer 3 VPN Ethernet Service Order | 718](#)

[Creating a Hub-and-Spoke Layer 3 VPN Service Order | 733](#)

Deploying a Service Order

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. In the **CPP** task pane, select **Service Orders**.
2. In the **Service Order** pie chart, click the **Requested** segment.

The **Manage Service Orders** page shows only those service orders in the Requested state.

3. Select the service order you want to deploy.

4. Open the **Actions** menu and click **Deploy Service Order**.

The **Deploy Service** window appears.

5. To deploy the service immediately, select **Deploy now**, and click **OK**.

To deploy the service at a later time, select **Deploy 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 deployment, the provisioning software begins validating the service order.

6. Use the Jobs workspace to monitor the outcome of the deployment. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details about the Jobs workspace.

RELATED DOCUMENTATION

Viewing Jobs in the *Junos Space Network Application Platform User Guide*

[Viewing Services](#) | 832

[Creating a Service Order Based on a Service Definition with a Template](#) | 756.

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.

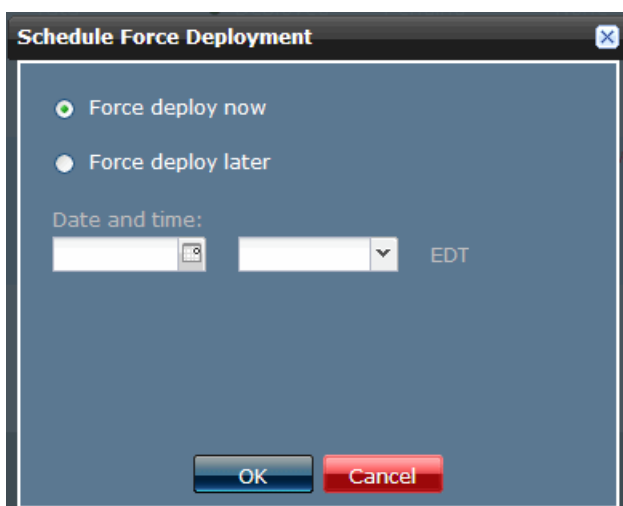
This procedure forces deployment of a service on the network.

You cannot force-deploy an invalid service order.

To schedule a service for forced deployment:

1. In the **Network Activate** task pane, select **Service Provisioning > Manage Services**.
2. In the **Manage Services** page, select the service you want to force deploy.
3. Open the **Actions** menu and click **Force Deploy Service**.

The **Schedule Force Deployment** window appears.



4. 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.

5. Use the Jobs workspace to monitor the outcome of the forced deployment. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details about the Jobs workspace.

RELATED DOCUMENTATION

[Viewing Services | 832](#)

[Deploying a Service Order | 631](#)

[Creating a Service Order Based on a Service Definition with a Template | 756](#)

Viewing the Configuration of a Pending Service Order

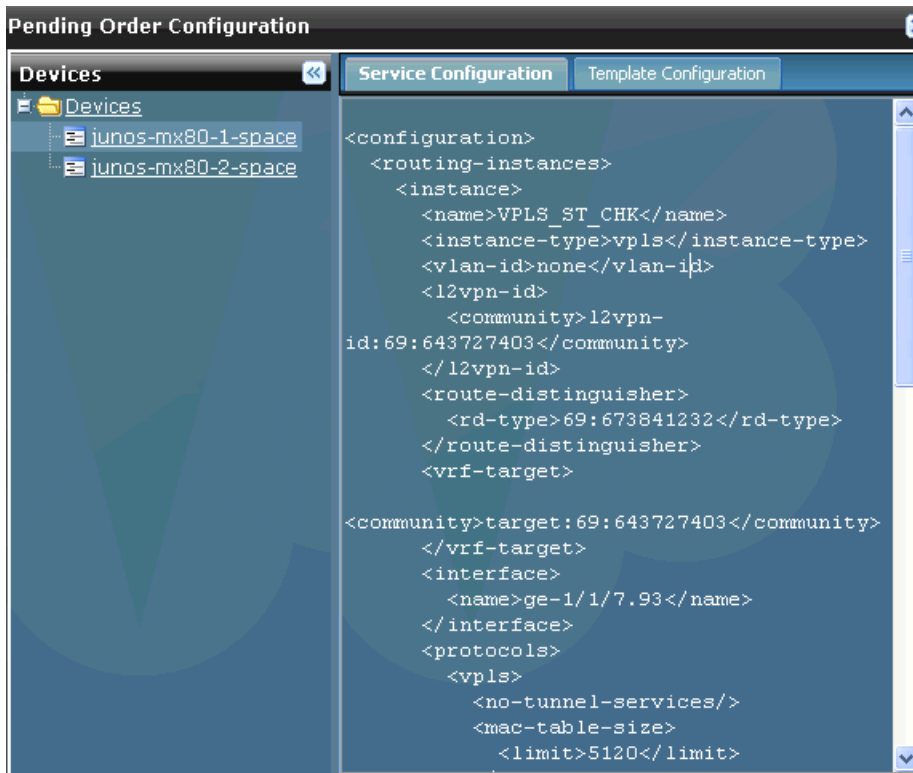
You can view the configuration of a service order that is in the requested state, the scheduled state, the invalid state, or the failed deployment state.

To view the configuration of such service orders:

1. In the **Network Activate** task pane, select **Service Provisioning > Manage Service Orders**. A list of service orders is displayed.
2. 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.

3. 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.

4. 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 > Network Activate**.
2. Right-click the Network Activate application and select **Modify Application Settings**. The Modify Network Activate Settings window is displayed.
3. Select the **show configuration in set format** check box.

RELATED DOCUMENTATION

[Service Order States and Service States Overview](#) | 576

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 device.

To create a point-to-point link to an end point that is not managed by Junos Space, in the Network Activate task pane, select **Service Provisioning** > **Manage Service Orders** > **Create P2P Service Orders**. The **Create P2P Service Orders** page displays an inventory of all available point-to-point service definitions.

1. Select the service definition upon which you want to base your service order, and click **Next**.
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 586](#)
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 586](#)
 - If this endpoint is a third-party device, select **Unmanaged device** from the **PE Device**.

Service Provisioning > Manage Service Orders > Create P2P Service Order

Definition: p2p_test
Service Order Name: p2p_test
Customer: Tata

Endpoint-A

Endpoint-Z

Endpoint Settings

PE device:

Loopback IP:

Unmanaged Interface:

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: 127.0.0.0 through 127.255.255.255
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 **Create**.

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](#) | 586

Selecting Specific LSPs for Network Activate Services

IN THIS SECTION

- [Associating an LSP with a Point-to-Point Service](#) | 639
- [Viewing LSP Details in a Service Order](#) | 640
- [Viewing LSP Details in a Service](#) | 641
- [Viewing LSP Configuration Details](#) | 642

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

To associate an LSP with a point-to-point service:

1. Create a point-to-point service order.
 - a. In the **Network Activate** task pane, select **Service Provisioning > Manage Service Orders > Create P2P Service Order**.

The **Create P2P Service Order** page displays an inventory of all available point-to-point service definitions.

 - 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**.

Service Provisioning > Manage Service Orders > Create P2P Service Order

Definition: p2p_test
Service Order Name: p2p_test
Customer: Tata

Endpoint-A

Endpoint-Z

Endpoint Settings

unit:

Physical IF: ethernet-ccc
encapsulation:

Traffic type: Transport using port

MTU (Bytes): 1522

LSP tunnel name: Please select ...

Resiliency settings

Enable: ☐

PE device: junos-m10-1-space

UNI interface: fe-0/1/1

MTU (Bytes): 1522

LSP tunnel name: M10i-1-to-fortius1

Revert time (sec): 5

Switch Over Delay (sec): 0

Back Next Create Cancel

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 **Create**.

For more information on creating a point-to-point service order, see [“Creating a Point-to-Point Service Order” on page 586](#)

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

In the **Network Activate** task pane, select **Service Provisioning > Manage Service Orders**.

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.

Endpoint Details

name:

PE device 30.1.2.3
loopback IP:

Interface ge-1/2/9
name:

UNI No description available
description: for selected UNI interface.

Physical IF flexible-ethernet-services
encapsulation:

Logical IF vlan-ccc
encapsulation:

Customer QINQ Transport all traffic
traffic type:

VLAN ID 1

MTU (Bytes): 1522

LSP tunnel Mx80-2-to-Mx80-1
name:

Community Mx80-2-to-Mx80-1
name:

Community 30507:48684
member:

Bandwidth : 10 Mbps

◀ Back Next ▶ Cancel

Viewing LSP Details in a Service

In the **Network Activate** task pane, select **Service Provisioning > Manage Services**. To view the details of a point-to-point service, double-click a point-to-point service in the **Manage 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.

Service Provisioning > Manage Service Orders > Manage Service Orders > Manage Service Orders >

Service Order Name: testlspDecommission2012-10-08 06:17:44.402
Customer: Tata
Service Definition: ELine-QinQ-AI/VLAN
Order State: Completed

Endpoint Details
name:
PE device loopback IP: 30.1.2.3
Interface name: ge-1/2/9
UNI description: No description available for selected UNI interface.
Physical IF encapsulation: flexible-ethernet-services
Logical IF encapsulation: vlan-ccc
Customer traffic type: QINQ Transport all traffic
VLAN ID 1
MTU (Bytes): 1522
LSP tunnel name: Mx80-2-to-Mx80-1
Community name: Mx80-2-to-Mx80-1
Community member: 30507:48684
Bandwidth : 10 Mbps

Back Next Cancel

NOTE: You cannot modify the LSP tunnel in a service.

Viewing LSP Configuration Details

In the **Network Activate** task pane, select **Service Provisioning > Manage Services**. Right-click a service and select **View Service Configuration Change**.

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 | 586](#)

[Viewing Service Orders | 620](#)

Validating 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.

To schedule a service order for validation, follow these steps:

1. In the **Network Activate** task pane, select **Service Provisioning**.
2. In the **Service Order States** pie chart, click the **Requested** or **Failed Deployment** segment.

The **Manage Service Orders** page shows only those service orders in the **Requested** state.

3. Select the service order you want to validate and save.
4. Open the **Actions** menu and click **Validate Service Order**.

The **Schedule Service Request Validation** window appears.

5. 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.

6. Click on the **Job ID** in the **Job Management** window to view details about the service validation.
7. Use the Jobs workspace to monitor the outcome of the validation. See *Viewing Scheduled Jobs* in the *Junos Space Network Application Platform User Guide* for details about the Jobs workspace.

RELATED DOCUMENTATION

[Deploying a Service Order | 631](#)

[Viewing Services | 832](#)

[Service Order States and Service States Overview | 576](#)

[Modifying a Point-to-Point Ethernet Service | 871](#)

[Modifying a Point-to-Multipoint Ethernet Service | 855](#)

[Modifying a Multipoint-to-Multipoint Ethernet Service | 844](#)

[Creating a Service Order Based on a Service Definition with a Template | 756.](#)

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 an E-Line Service Definition” on page 188](#).

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 586](#).

3. Deploy the point-to-point service order.

- a. In the Manage Service Orders inventory page, select the point-to-point service order you created in Step 2.
- b. Right-click the point-to-point service order and select **Deploy Service Order**. The Schedule Service Order Deployment window appears.
- c. Select the **Deploy now** option button and click **Ok**.

The service order is deployed.

4. In the Manage Services inventory page, right-click the point-to-point service that you created and select **Service > 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. 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 586](#).

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. In the Manage Service Orders inventory page, select the point-to-point service order you created in Step 6.
 - b. Right-click the point-to-point service order and select **Deploy Service Order**. The Schedule Service Order Deployment window appears.
 - c. Select the **Deploy now** option button and click **Ok**.

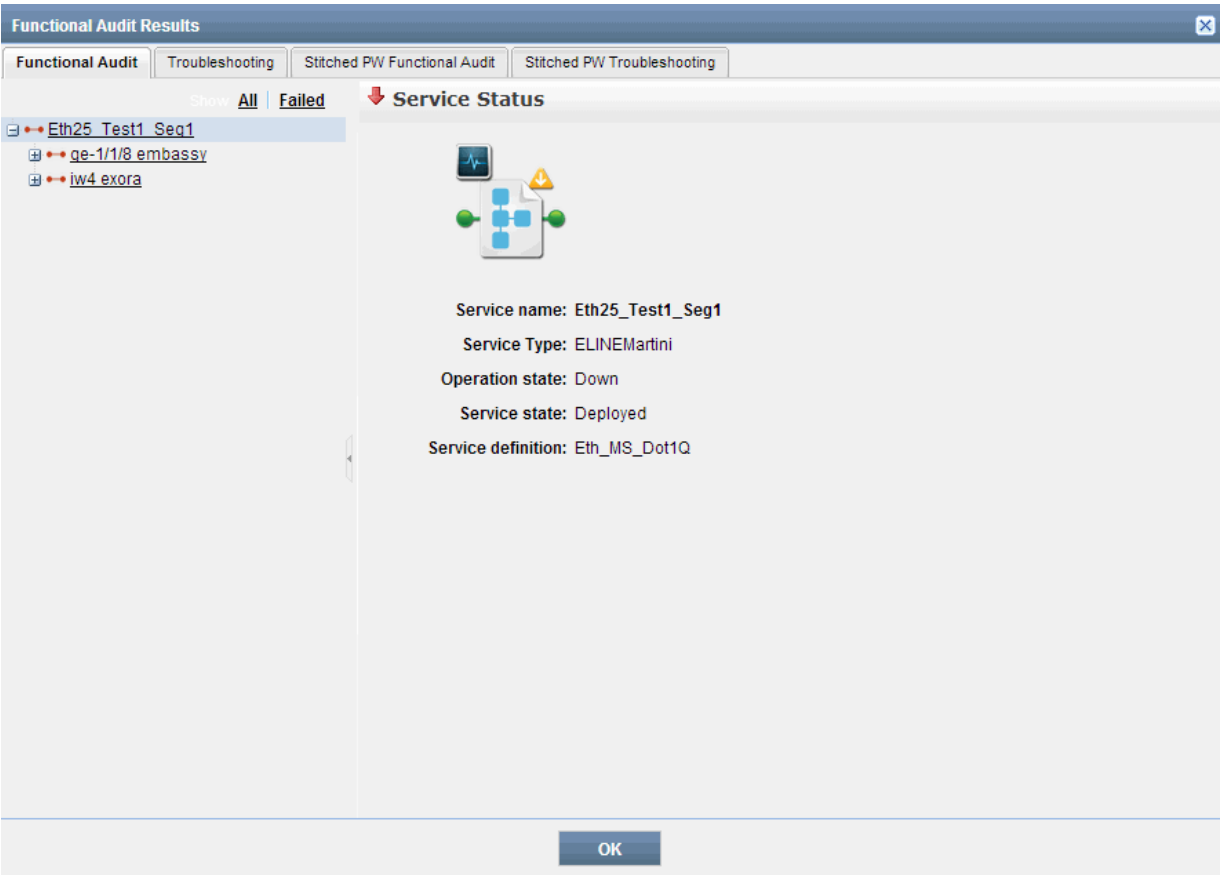
The service order is deployed.

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 | 578
- Creating a Point-to-Point Service Order | 586

Providing Broadband Network Gateway Service Support with Cross Provisioning Platform

IN THIS SECTION

- [Create Workflow for Broadband Network Gateway Services | 649](#)
- [Modify Workflow for Broadband Network Gateway Services | 651](#)
- [Viewing Broadband Network Gateway Services Details | 653](#)
- [Child-Endpoint Support for Broadband Network Gateway Services | 654](#)
- [API for Finding the Service Element ID | 654](#)

The following are the three kinds of broadband network gateway (BNG) services offered to residential subscribers:

- IPTV
- Broadband Remote Access Server (B-RAS)
- Wholesale

With Cross Provisioning Platform (CPP), you can provision, maintain, and troubleshoot BNG services. For example, you can add or remove BNG devices to or from the existing Layer 3 VPN services. You can add or remove underlying interfaces for any given BNG device. You can also troubleshoot subscriber issues by using the Report Management functionality through Juniper Networks devices.

NOTE: BNG service support is provided only for Juniper Networks devices. CPP multistaged service support is provided to all MX Series products of Juniper Networks and to third-party devices. A test service can be implemented only by using device configlets. The device configlets of third-party devices are not supported. Hence, you cannot create a test service for third-party devices through CPP.

Provisioning a BNG service involves multiple steps. For example, the following steps are involved in provisioning a B-RAS service in third-party devices:

- Create a prefix-list.
- Create a community.
- Create an export policy.

- Create an import policy.
- Create a virtual private routed network (VPRN) B-RAS service site.

Sending a validation or pretesting command may also be included in these steps to provision the service. If any one of the steps fails, you may manually intervene to correct the issue and resume from the failed step. This eliminates the need to repeat the previously completed successful steps. The GUI script controls the provisioning flow internally and shows the status of each step.

You can troubleshoot connectivity and networking issues for subscribers availing different BNG services. To troubleshoot, you can perform any one of the following tasks:

- You can issue remote procedure call (RPC) commands against the BNG devices to obtain information about active subscribers and to obtain a history of service utilization for a given BNG device that includes the number of current active subscribers and the peak subscriber count.
- You can execute operational scripts for all MX Series devices on a daily basis and generate graphs of the RPC commands.
- Subscribers can launch test commands from their devices at home to determine whether a physical connection exists from their homes to a BNG device. To enable subscribers to launch test commands, you need to create a test virtual routing and forwarding (VRF) on MX Series devices.

The CPP framework requires that information about the device and interface at every step to create a service order. The CPP multistage framework supports multiple devices at a time.

The BNG service type supports all three kinds of BNG services. In a multistaged workflow, all steps involved should include the creation of a new service order and the service endpoint common attribute.

This topic has the following sections:

Create Workflow for Broadband Network Gateway Services

The procedure to create a BNG service order is the same for Juniper Networks devices and third-party devices.

The create workflow for BNG services is as follows:

1. While creating a BNG service order, the GUI collects the data and sends **CreateRequest** with the Multistaged tag. The initial service order type must be ADD.

NOTE: You need to create a service definition with the BNG type and a service order based on this BNG service definition. The number of service orders you need to create is equal to the number of tasks you need to perform to troubleshoot the services.

The CPP returns the job information, polls the status of the job, and invokes the configuration script.

2. The configuration script verifies the value of the Multistaged tag.

- If you have specified the Multistaged tag as SINGLETON, the configuration script executes the specified single task.

If the single task is successful, the job status is updated. The service order status is changed to Completed, and the service status is changed to Deployed.

If the single task fails, the service order status is changed to Failed_Deployment. To fix the issue manually, you can modify or re-create the service order from the previously successful service order.

NOTE: The single-task BNG service must have an endpoint.

- If you have specified the Multistaged tag value as INIT, the configuration script executes all the specified tasks.

If the first task is successful, the job status is updated. The service order status is changed to Completed and the service status is changed to Deploying.

The configuration script again verifies the value of the Multistaged tag, and executes each task until the Multistaged tag value is LAST.

After the last task is successful, the job status is updated. The service order status is changed to Completed and the service status is changed to Deployed.

After you complete all the steps, the service modification options are enabled.

NOTE: If you close any page by mistake while performing a step, you can always go to the Service Orders landing page and perform the remaining steps by using the **Recreate Service Order** option. The **Recreate Service Order** option is available only in the previous successful service order. If the service is in the Deploying state, you cannot perform the following actions on the Services page:

- **Modify**
- **Configuration Audit**
- **View Service Configuration**

To poll a job, go to the following URL:

['/serviceui/reteasy/cpp-service-order/order-job-status/'+jobId](/serviceui/reteasy/cpp-service-order/order-job-status/'+jobId)

To delete a service order, go to the following URL:

['/serviceui/reteasy/cpp-service-order/'+serviceRequestId](/serviceui/reteasy/cpp-service-order/'+serviceRequestId)

To find the service element ID, go to the following URL:

['/serviceui/reteasy/cpp-service/selId](/serviceui/reteasy/cpp-service/selId)

The troubleshooting procedure, which involves the execution of operational scripts and CLI configlets, is applicable only to Juniper Networks devices. The configuration audit function is enabled only when the BNG service state is Deployed. The option to decommission is enabled only when the service state is Deploying or Deployed.

Modify Workflow for Broadband Network Gateway Services

The modify workflow for BNG services is as follows:

1. While modifying a BNG service order, the GUI collects the data and sends **CreateRequest** with the Multistaged tag.

The following tags are mandatory for modifying a BNG service:

- Service order type—The service order type must be MODIFY.
- Workflow type—The workflow type must be MODIFY.
- Record OP type—The record operation type must be MODIFY.
- Service Element ID—To identify the service element ID, you can call the findServiceEndpointId API.

The CPP returns job information, polls the status of the job, and invokes the configuration script.

2. The configuration script verifies the value of the Multistaged tag.

- If you have specified the Multistaged tag as SINGLETON, the configuration script executes the specified single task.

If modifying the single task is successful, the job status is updated. The service order status is changed to Completed and the service status is changed to Deployed.

If modifying the single task fails, the service order status is changed to Failed_Deployment. To fix the issue manually you can modify or re-create the service order from the previously successful service order.

NOTE: The single-task BNG service must have an endpoint.

- If you have specified the Multistaged tag value as INIT, the configuration script executes all specified tasks.

If modifying the first task is successful, the job status is updated. The service order status is changed to Completed and the service status is changed to Deploying.

The configuration script again verifies the value of the Multistaged tag and modifies each task until the Multistaged tag value is LAST.

After the last task is successful, the job status is updated. The service order status is changed to Completed and the service status is changed to Deployed.

After you complete all the steps, the service order status is changed to Completed.

Viewing Broadband Network Gateway Services Details

CPP Service Details

General

Service name: SO540328565
 Description:
 External Id: BNG_MultiStage
 Oss Customer Id:
 Administrative state : Deployed
 Service type: BNG
 Service definition: multistage

Device Name	Device IP	Port	Port Status	Parent Device	Role
PE3_re0	10.220.28.197	ge-1/0/3.111	Up		N_PE
PE4_re0	10.220.28.194	ge-1/0/3.111	Up		N_PE
exora	10.216.114.114	ge-0/1/2.1	Down	PE4_re0	L2E

Advanced Details For Device : PE3_re0

Interface | Igmp | Configuration | SO Audit

Attribute	Value
Description	L3VPN VRF 990 Interface
VLAN Type	dot1q
VLAN Id	111
Operation State	Up

Page 1 of 1 | Displaying 1 - 3 of 3 | Show 10 items

Ok Refresh

A BNG service is created only with common artifacts and no VPRN service is associated with a BNG service. Hence, the service details are not displayed in CPP. In this case, instead of service details, the following tabs are displayed, if available:

- General–Displays the service name, device name, artifact, and vendor type
- Configuration–Displays configuration details
- Artifact–Displays common artifact information from the Simple Object Access Protocol (SOAP) response
- Igmp–Displays information about group addresses and interfaces
- Interface–Displays dynamic profile-related information.
- MVPN–Displays neighbor ID and provider tunnel ID.
- AAA Info–Displays AAA-related information
- QoS Info–Displays QoS-related information

The Juniper Subscriber Service Details tab displays details of Dynamic Host Configuration Protocols server (DHCP) address pool, and RADIUS servers. In the case of IPTV, pool information and RADIUS are not displayed. In the case of B-RAS, DHCP server details are not displayed. All tabs of the Layer 3 VPN service are displayed in the case of the BNG service. The ALU Subscriber Service Details tab displays details of Dynamic Host Configuration Protocol (DHCP), Internet Group Management Protocol (IGMP), Physical Interface Module (PIM), and multicast virtual private network (MVPN).

Child-Endpoint Support for Broadband Network Gateway Services

For a BNG service, you can provision parent-child relationships between the endpoints. You can provision it as a single-task workflow or multitask workflow.

For a multitask workflow, you can select a parent endpoint in a task and then attach the child endpoint in the subsequent tasks.

API for Finding the Service Element ID

To modify or delete an endpoint, you must specify the service element ID and set the Record OP type tag as Modify or Delete.

The `findServiceEndpointId` API is used to find the service element ID. The GUI script validates the service element ID and identifies the end point that must be modified or deleted.

Following is the query to find the service element ID:

```
public String findServiceEndpointId(@QueryParam(serviceID) String serviceId, @QueryParam(deviceId) String deviceId, @QueryParam(port) String port, @QueryParam(outerEncap) String outerEncap)
```

This API returns the service element ID in string format with the following parameters:

- *serviceID*—ID of the service that is modified
- *deviceId*—Provider edge device ID
- *port*—Port of an interface
- *outerEncap*—Outer encapsulation VLAN value

RELATED DOCUMENTATION

| [Managing Reports for Broadband Network Gateway Services in Cross Provisioning Platform](#) | 1050

Deleting a Partial Configuration

A failed service order of type Provisioning can leave parts of the service configuration on the devices. To remove this partial configuration:

1. In the **Network Activate** task pane, select **Service Provisioning > Manage Service Orders**.
2. In the **Manage Service Orders** page, select the failed service order for which you want to delete the partial configuration.
3. Open the **Actions** menu and select **Delete Partial Configuration**.
4. In the confirmation screen, select **Delete**.

RELATED DOCUMENTATION

| [Viewing Service Orders | 620](#)

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 correct a service order in the invalid state, you must delete it and then recreate it; the Network Activate software does not support modifying the service order directly.

To delete a service order from the database:

1. In the Network Activate task pane, select **Service Provisioning > Manage Service Requests**.
2. In the **Manage Service Orders** page, select the service order you want to delete.
3. Open the **Actions** menu and select **Delete Service Order**.
A pop-up window appears requesting confirmation.
4. Click **Delete**.

The **Manage Service Orders** page reappears with the deleted service orders removed.

RELATED DOCUMENTATION

| [Creating a Point-to-Point Service Order | 586](#)

| [Creating a Multipoint-to-Multipoint VPLS Service Order | 660](#)

| [Creating a Point-to-Multipoint VPLS Service Order | 678](#)

Re-creating a Cross Provisioning Platform Service Order After a Failed Deployment

If a service order fails to deploy, you need not create a new service order. The Cross Provisioning Platform application allows you to re-create an existing service order whose order state is *Failed_Deployed* or *Invalid*.

To re-create a service order after a failed deployment:

1. From the Cross Provisioning Platform task pane, select **CPP > Service Orders**.

The Service Orders page is displayed.

2. Right-click a service order whose order state is *Failed_Deployed* or *Invalid* and select **Recreate Service Order**.

The output of the attached script is displayed.

NOTE: The **Recreate Service Order** option is available only if the **Order Type** column displays *ADD* or *MODIFY*.

If the **Order Type** column displays *ADD*, the output of the GUI script that you attached in the **Creation** field while creating a service definition is displayed.

If the **Order Type** column displays *MODIFY*, the output of the GUI script that you attached in the **Modification** field while creating a service definition is displayed.

NOTE: The **Recreate Service Order** option is available even after you decommission the corresponding service. If you have decommissioned a service, on the Service Orders page, the **Order Type** column displays *DELETE* and the order state is *Completed*. When you select the **Recreate Service Order** for such service orders, the output of the GUI script that you attached in the **Creation** field while creating a service definition is displayed.

3. (Optional) Before you click **Modify**, you can verify the modified parameters in the script output window by clicking **Verify**.

The Verify Service Order window is displayed. You can view the service order configuration details.

4. To modify the parameters in the script output window, click **Modify**.

The Job Details window appears. Click the **JOB ID** link to view the job status on the Job Management page.

If the job is successfully completed, the service order status changes to *Deployed*.

RELATED DOCUMENTATION

[Creating a Cross Provisioning Platform Service Order | 616](#)

[Viewing the Script Output on the Service Orders Inventory Page | 658](#)

Re-creating a Cross Provisioning Platform Service Order After a Successful Deployment

If you want to replicate a service order that is successfully deployed, you need not create a new service order. The Cross Provisioning Platform application allows you to re-create an existing service order whose order state is *Completed*.

To re-create a service order after a successful deployment:

1. From the Cross Provisioning Platform task pane, select **CPP > Service Orders**.

The Service Orders page is displayed.

2. Right-click a service order whose order state is *Completed* and select **Recreate Service Order**.

The output of the attached script is displayed.

NOTE: The **Recreate Service Order** option is available only if the **Order Type** column displays **ADD**.

If the **Order Type** column displays **ADD**, the output of the GUI script that you attached in the **Creation** field while creating a service definition is displayed.

3. (Optional) Before you click **Create**, you can verify the modified parameters in the script output window by clicking **Verify**.

The Verify Service Order window is displayed. You can view the service order configuration details.

4. To modify the parameters in the script output window, click **Create**.

The Job Details window appears. Click the **JOB ID** link to view the job status on the Job Management page.

If the job is successfully completed, the service order status changes to *Deployed*.

RELATED DOCUMENTATION

[Re-creating a Cross Provisioning Platform Service Order After a Failed Deployment](#) | 656

Viewing the Script Output on the Service Orders Inventory Page

In releases earlier than Cross Provisioning Platform Release 15.1R1, to view the output of the script that you attached while creating a service definition, you must deploy the service order.

With Cross Provisioning Platform Release 15.1R1, you can view the output of an attached script on the Service Orders inventory page, even before deploying the service order.

To view the output of a script on the Service Orders inventory page:

1. On the Cross Provisioning Platform task pane, select **CPP > Service Orders**.

The Service Orders page is displayed.

2. Right-click a service order and select **View Service Order Details**.

NOTE: If you select multiple service orders, the **View Service Order Details** option is unavailable.

The **View Service Order Details** option is available only if the **Order Type** column displays the following types: ADD, MODIFY, or RECOVER.

The output of the attached script is displayed. You cannot modify the parameters of the script because the output is displayed in the read-only format.

The following error message is displayed if the attached script does not include a method to call the View Service Order Details action:

Service order details view is not supported in GUI script.

RELATED DOCUMENTATION

[Adding Scripts Created for Cross Provisioning Platform | 775](#)

[Creating a Cross Provisioning Platform Service Definition | 305](#)

[Creating a Cross Provisioning Platform Service Order | 616](#)

Layer 2 VPLS Service Orders

IN THIS CHAPTER

- [Creating a Multipoint-to-Multipoint VPLS Service Order | 660](#)
- [Creating a Point-to-Multipoint VPLS Service Order | 678](#)
- [Creating a Service Order for VPLS Access into Layer 3 Networks | 698](#)
- [Creating a VPLS Service Order in Cross Provisioning Platform | 705](#)
- [Seamless MPLS Support in Junos Space Overview | 708](#)
- [Understanding VLAN Manipulation \(Normalization and VLAN Mapping\) on Ethernet Services | 710](#)

Creating a Multipoint-to-Multipoint VPLS Service Order

The Network Activate software 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 | 660](#)
2. [Entering General Settings Information | 661](#)
3. [Specifying QoS Settings | 662](#)
4. [Specifying OAM Settings | 663](#)
5. [Configuring Connectivity Settings | 663](#)
6. [Setting Attributes for All Endpoints | 665](#)
7. [Selecting N-PE Devices and Multihomed Groups | 671](#)
8. [Modifying Endpoint Settings | 672](#)
9. [Deploying the New Service | 677](#)

Selecting the Service Definition

To select a service definition on which to base the new service order:

1. In the Network Activate task pane, select **Service Provisioning > Manage Service Orders > Create 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. You can select the service definition based on the signaling type.

2. Select the service definition you want to base your service order on, then click **Next**.

The **Enter Order Information** window appears.

Entering General Settings Information

This part of the create multipoint Ethernet service order procedure sets general information about the service order in the **General Settings** box of the Enter Order Information window:

The screenshot shows the 'General Settings' window with the following fields and values:

- Service definition: MP_MP_BGP
- Name: [Empty text field]
- Customer: Please select ... [Dropdown menu]
- Comments: [Empty text area]
- Customer traffic type: Transport single vlan
- Signaling: BGP
- ☒ Allow access to L3 network

To enter general settings information:

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 1056](#).

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** is not selectable. Its value is set in the service definition.

The **Signaling** cannot be changed in the service order.

4. If QoS is enabled, continue with "Specifying QoS Settings" next. Otherwise, skip to "Setting Attributes for all Endpoints."

Specifying QoS Settings

If QoS is enabled on the service definition, type information in the QoS Settings box of the **Enter Order Information** window.

NOTE: QoS features appear in the Junos Space user interface only if you deploy the QoS Design application in Junos Space.

To specify QoS settings:

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 QoS Design software.

A QoS profile classifies traffic into defined service groups to provide the special treatment of traffic across the network service.

2. In the **CIR** field, select the committed information rate (CIR) from the list.

The CIR is the guaranteed rate and specifies the minimum bandwidth available if all sources are active at the same time. The value for CIR should be less than the value for PIR.

NOTE: For bursty traffic, the CIR represents the average rate of traffic per unit time, and the PIR represents the maximum amount of traffic that can be transmitted in a given interval.

3. In the **PIR** field, select the peak information rate (PIR) from the list. The PIR is the shaping rate.

NOTE: If the QoS profile that you selected in Step 1 is configured with a level-three scheduler and interface oversubscription is enabled, then PIR is not used.

4. Continue with "Setting Attributes for All Endpoints," next.

Specifying OAM Settings

To enable OAM on the service definition, type information in the OAM Settings of the General/Connectivity Settings panel.

1. In the **CFM Definition** 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.

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. Continue with configuring the connectivity settings.

Configuring Connectivity Settings

In this procedure, you specify the attributes that define the connectivity among remote sites across the service provider network and the service security. The following illustration is a sample **Connectivity** window.

The screenshot shows a window titled "Connectivity Settings". It contains the following elements:

- A checkbox for "Auto Discovery" which is currently unchecked.
- A checkbox for "Autopick VPLS ID" which is currently checked.
- A label "Revert time (sec):" followed by a text input field containing the value "5".
- A label "Switch Over Delay (sec):" followed by a text input field containing the value "0".

To configure connectivity settings for connectivity between sites across the network:

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. Click **Next**.

You can edit the **VPLS ID** field, if you have selected the **Select manually** option for the **VPLS ID** field in the service definition.

The **Auto Discovery** and **Autopick VPLS ID** fields appears dimmed in the **Connectivity Settings** dialog box. These fields are not editable in the service order.

Setting Attributes for All Endpoints

This part of the create multipoint Ethernet service order procedure sets the attributes that are usually common for all endpoints in the service.

NOTE: When the **Allow multihoming** check box is selected for the service definition on which the service order based, the **End Point Settings** box displays the **Allow multihoming on endpoints** check box to indicate that the service can include multihomed groups.

To set attributes common to most endpoints:

1. In the **Bandwidth** field, select a value from the drop-down 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.

2. 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.

3. If the signaling type is LDP and the if the auto discovery is enabled, the **Autopick VPN ID** appears dimmed. This field is not editable in the service order.

4. Specify the **VPLS ID** if the **Autopick VPLS ID** is disabled.

Range: 1 through 2147483647

5. Specify the **VPN ID** if the **Autopick VPN ID** is disabled.

Range: 1 through 65535

The **Auto-pick VLAN range constraint** field is displayed and validates the VLAN range specified in the service definition.

6. Specify the Logical If Settings.

NOTE: The Logical If Settings box is not available if you have selected the **Ethernet option** as port.

- 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.

- 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.

7. 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.

8. The **Physical IF encapsulation** and **Logical IF encapsulation** fields are not selectable. These values are set in the service definition.

In the **VLAN Tag to stack** field, type a value for the customer VLAN.

This field is present only for services that specify Normalize to Dot1q tags.

9. In the **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.

10. In the **Outer VLAN Tag to Stack** field, type a value to provide an outer VLAN tag that matches the Outer VLAN tag of at least one of the UNI endpoints.

11. In the **Inner VLAN Tag to Stack** field, type a value to provide a default inner VLAN tag for the UNI endpoints to provide a common inner VLAN tag for the routing instance.

This field is present only for services that specify Normalize to QinQ tags.

12. Click **Next**.

The **Select Endpoint PE Devices** window appears.

13. Continue with "Selecting N-PE Devices and Multihomed Groups."

Setting Attributes for Endpoints 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 **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 756](#).

This procedure sets the attributes listed in the **End Point Settings** box of the Enter Order Information window. 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.

NOTE: When the **Allow multihoming** check box is selected for the service definition on which the service order based, the **End Point Settings** box displays the **Allow multihoming on endpoints** check box to indicate that the service can include multihomed groups.

To set attributes common to most endpoints:

1. 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.
2. 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.
3. If the signaling type is LDP and the if the auto discovery is enabled, the **Autopick VPN ID** appears dimmed. This field is not editable in the service order.
4. Specify the **VPLS ID** if the **Autopick VPLS ID** is disabled.
Range: 1 through 2147483647
5. Specify the **VPN ID** if the **Autopick VPN ID** is disabled.
Range: 1 through 65535

6. To configure VLANs, choose from the following options depending on the VLAN transport type and Normalization that the service specifies:
 - If the service transports single VLANs and specifies Normalize to Dot1Q tags:
 - a. In the **Inner VLAN (for Q-in-Q)** field, type a VLAN ID to swap.
 - b. In the **VLAN Tag to stack** field, type a VLAN ID to push or swap at the relevant UNI endpoints.
 - If the service transports single VLANs and specifies Normalize to QinQ tags:
 - a. To manually assign an VLAN ID:
 - i. Clear the **Autopick VLAN ID** check box. The window expands to include the **VLAN ID** field.
This field is present in the service order only if the service definition allows it.
 - ii. In the **VLAN ID** field, type a value.
This field is configurable in the service order only if the service definition allows it.
 - b. In the **Inner VLAN (for Q-in-Q)** field, type a VLAN ID to swap.
 - c. In the **Outer VLAN Tag to stack** field, type a VLAN ID to push or swap at the relevant UNI endpoints.
 - d. In the **Inner VLAN Tag to stack** field, type a VLAN ID to push or swap at the relevant UNI endpoints.
 - If the service transports single VLANs and specifies Normalize to VLAN none:
 - In the **Inner VLAN (for Q-in-Q)** field, type a VLAN ID to swap.
 - If the service transports all traffic and specifies Normalize to VLAN all:
 - a. 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.
 - b. In the **VLAN Tag to stack** field, type a VLAN ID to push or swap at the relevant UNI endpoints.
 - If the service transports a range of VLANs and specifies Normalize to VLAN all:
 - a. 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.
 - b. In the **VLAN Tag to stack** field, type a VLAN ID to push or swap at the relevant UNI endpoints.

NOTE: A service that transports a range of VLANs and specifies Normalize to VLAN all allows only 802.1Q, and Q-in-Q interfaces for the UNI endpoints.

7. Click **Next**.

The **Select Endpoint PE Devices** window appears.

8. Continue with "Selecting N-PE Devices and Multihomed Groups," next.

Selecting N-PE Devices and Multihomed Groups

This part of the create multipoint Ethernet service order procedure selects the N-PE devices and, optionally, multihomed groups that hosts the service endpoints. The selection is made from the **Select Endpoint PE Devices** window.

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 756](#).

NOTE: If multihoming is enabled on the service definition on which the service order is based and you have configured and imported the connectivity file, you can select one or more multihomed groups that are configured in the multihomed groups connectivity file for the service endpoints.

NOTE: The **Select Endpoint PE Devices** 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 **Select Endpoint PE Devices** window, select the devices that you want to participate in the service. Use the multiple selection feature to select one or more devices.
2. Click **Next**.

The **Endpoint Settings** window appears.

3. Continue with "Modifying Endpoint Settings," next.

Modifying Endpoint Settings

This part of the create multipoint Ethernet service order procedure sets the attributes for each endpoint in the service. Selection is made using the **Endpoint Settings** window.

Endpoint Settings							
Add Endpoints							
Device	UNI Interface	Description	Autopick UNIT ID	UNIT ID	AutoPick VLAN ID	MTU (Bytes)	Action
Device: amx-1100-a (1 Interface) Add Label							
amx-1100-a	em1		true	0	<input checked="" type="checkbox"/>	1522	Delete UNI Interface
Device: amx-1100-b (1 Interface) Add Label							
amx-1100-b	em0		true	0	<input checked="" type="checkbox"/>	1522	Delete UNI Interface

This window shows one endpoint for each device that you selected from the **Select Endpoint PE Devices** window, as described in ["Selecting N-PE Devices and Multihomed Groups" on page 671](#).

The interface shown in the **UNI Interface** field is automatically selected by the Network Activate software, 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 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 Enter Order Information window, as described in [“Setting Attributes for All Endpoints” on page 665](#).

To modify the endpoint settings:

1. For a service with flexible VLAN tagging, set the interface type in the Ethernet Option column for each endpoint in the service.
2. To select a different UNI on a device, on the **Endpoint Settings** window, click the UNI name you want to change and choose another interface from the list.

Modified values are indicated by a small red triangle in the corner of the table cell.

3. To enter the description for an UNI interface, click the corresponding **Description** cell.
4. To change the bandwidth on an endpoint, click the bandwidth value for the endpoint and select another value from the list.
5. To change the committed information rate (CIR) on an endpoint, click the CIR value for the endpoint and select another value from the list. Make sure that the CIR value is less than the PIR value.
6. To change the peak information rate (PIR) on an endpoint, click the PIR value for the endpoint and select another value from the list. Make sure that the PIR value is greater than the CIR value.

Only QoS-enabled services specify CIR and PIR values.

Only QoS-enabled services specify CIR and PIR values.

7. The **AutoPick 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 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 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.

8. 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.
9. For Q-in-Q interface endpoints with customer VLAN ranges specified, you can also change the range limits for an endpoint.
10. For 802.1Q interface endpoints, you can change the customer VLAN ID.
11. To change the MTU for the UNI, click the value in the **MTU** field and type a new value.
12. To add a UNI on a selected device, select **Add UNI Interface** in the Action column, and then select the interface you want from the UNI interface list.
13. 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.
14. To delete a UNI from a device, in the Action column, click **Delete UNI Interface**.

If the deleted UNI is the only UNI selected from the device, then the device is deleted from the service configuration.
15. To specify the value of **Outgoing Label** for any device, click the **Add Label** link that is associated with that device. Specify the value in the **Outgoing Label Settings** window and click **OK** to save the value. All the devices act as hubs and no spoke devices are present.
16. To view the values of the **Incoming Label** and the **Outgoing Label** of any device, use the following method:
 - a. Select **Manage Service Orders > View Service Order Details**.
 - b. Click the **Label Details** link associated with any device.

17. To specify a different primary device for a multihomed group:

- a. To select a different primary device, in the **Endpoint Settings** box, click the Edit icon (indicated by a pencil).
- b. From the list of secondary devices, select the radio button for the secondary device that you want to specify as the primary device in the multihomed group.
- c. Click **Set As Primary**.
- d. Click **Create**.

The secondary device is configured as the primary device in the multihomed group.

18. 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.

To configure advanced settings for a device in the service order:

- a. Click **Advanced** in the Action column.

The **Advanced Setting** window displays the security and advanced settings that you can configure for a device.



The image shows a window titled "Advanced Setting: junos-mx240-space". Inside the window, there is a section titled "MAC Security Settings". This section contains the following configuration options:

- ☒ MAC learning
- Interface MAC limit:
- ☐ MAC statistics
- MAC table size:

At the bottom of the window, there are two buttons: "OK" and "Cancel".

- b. In the **MAC Security Settings** box, make selections for MAC learning and MAC statistics and type values for Interface MAC limit, MAC table size, and MAC table aging time.
- c. Enable or disable tunnel services by selecting or clearing the **disable-tunnel-service** check box.
- d. Enable or disable local switching by selecting or clearing the **disable-local-switching** check box.
- e. In the **Fast reroute priority** field, select the reroute priority for a VPLS routing instance.
- f. In the **Label block size** field, type the label block size for VPLS labels.

- g. 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)

- h. Click **OK** to save your Advanced Setting changes for the device.

19. To add an endpoint on a device not listed in the **Endpoint Settings** window:

- a. Click **Add Endpoints**.

The **Add Endpoint PE Devices** window displays the available N-PE devices that you did not assign when you first made your device selections from the **Select Endpoint PE Devices** window.

- b. Select additional devices, then click **Next**.

The **Endpoint Settings** window appears with the new devices added.

- c. Modify the endpoint settings for this device, as required.

20. If you have attached a service template in the service definition, the **Flexible Service Attributes** link appears. Click the link to modify the service template attributes. For more information about configuring the flexible Service Attributes, see [“Configuring Flexible Service Attributes to Modify Service Template Attributes” on page 938](#).

21. When you have finished modifying the endpoint settings, click **Create**.

The **Deployment Options** window appears.

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**.

For more information on topology, see [“Junos Space Network Topology Overview” on page 31](#)

22. Continue with "Deploying the New Service," next.

Deploying the New Service

This part of the create multipoint Ethernet service order procedure deploys the service.

To deploy the service from the **Deployment Options** window:

1. Perform one of the following actions:

- To save the request without deploying the service, select **Save only**, then click **OK**.

See [“Deploying a Service Order” on page 631](#) for information about how to deploy a saved service at a later time.

- 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. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details about the Jobs workspace.

RELATED DOCUMENTATION

Viewing Jobs in the Junos Space Network Application Platform User Guide

[Viewing Service Orders | 620](#)

[Service Attributes Overview | 152](#)

[Adding a New Customer | 1056](#)

[Deploying a Service Order | 631](#)

[Force-Deploying a Service | 632](#)

[Creating a Point-to-Multipoint VPLS Service Order | 678](#)

[Creating a Point-to-Point Service Order | 586](#)

[Understanding VLAN Manipulation \(Normalization and VLAN Mapping\) on Ethernet Services | 710](#)

[Creating a Service Order Based on a Service Definition with a Template | 756](#)

Creating a Point-to-Multipoint VPLS Service Order

IN THIS SECTION

- [Selecting the Service Definition | 679](#)
- [Entering General Settings Information | 679](#)
- [Configuring Connectivity Settings | 681](#)
- [Specifying QoS Settings | 683](#)
- [Specifying OAM Settings | 683](#)

- [Setting Attributes for All Endpoints | 684](#)
- [Setting Attributes for Endpoints on a Service | 684](#)
- [Setting Attributes for Endpoints on a Service with Flexible VLAN Tagging | 687](#)
- [Selecting N-PE Devices and Multihomed Groups | 690](#)
- [Selecting Hubs and Modifying Endpoint Settings | 690](#)
- [Deploying the New Service | 696](#)

The Network Activate software 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

To select a service definition on which to base the new service order:

1. In the Network Activate task pane, select **Service Provisioning > Manage Service Orders > Create VPLS Service Order**.

The **Create VPLS Service Order** window displays a filtered inventory view of only those published service definitions that are designed to work with multipoint Ethernet services. You can select the service definition based on the signaling type.

2. Select the point-to-multipoint service definition you want to base your service order on and then click **Next**.

The **Enter Order Information** window appears.

Entering General Settings Information

This part of the create point-to-multipoint Ethernet service order procedure sets general information about the service order in the **General Settings** box of the **Enter Order Information** window:

The screenshot shows a 'General Settings' form with the following fields and options:

- Service definition:** VPLS_LDP_PW_EXT
- Name:** VPLS_LDP_PW_EXT
- Customer:** Please select ... (dropdown menu)
- Comments:** (text area)
- Customer traffic type:** Transport single vlan
- Signaling:** LDP
 - ☒ Enable PW Extension
 - ☒ Enable PW Resiliency

To specify general settings information:

1. In the **Name** field, type a unique name for the point-to-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.

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 1056](#).

3. In the **Comments** field, type a description of the service. This description appears in information window about the request or service instance created from the request.

You cannot select the **Customer traffic type**. Its value is set in the service definition.

You cannot change the **Signaling** type 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.

4. If QoS is enabled, continue with "Specifying QoS Settings," next. Otherwise skip to "Setting Attributes for all Endpoints."

Configuring Connectivity Settings

In this procedure, you specify the attributes that define the connectivity among remote sites across the service provider network and the service security. The following illustration is a sample **Connectivity** window.

To configure connectivity settings for connectivity between sites across the network:

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. Continue with specifying the QoS settings.

You can edit the **VPLS ID** field, if you have selected the **Select manually** option for the **VPLS ID** field in the service definition.

The **Auto Discovery** and **Autopick VPLS ID** fields appears dimmed in **Connectivity Settings** dialog box. These fields are not editable in the service order.

Specifying QoS Settings

If QoS is enabled in the service definition, enter information in the QoS Settings box.

NOTE: QoS features appear in the Junos Space user interface only if you deploy the QoS Design application in Junos Space.

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 QoS Design software.

A QoS profile classifies traffic into defined service groups to provide the special treatment of traffic across the network service.

2. In the **CIR** field, select the committed information rate (CIR) from the list.

The CIR is the guaranteed rate and specifies the minimum bandwidth available if all sources are active at the same time. The value for CIR should be less than the value for PIR.

NOTE: For bursty traffic, the CIR represents the average rate of traffic per unit time, and the peak information rate (PIR) represents the maximum amount of traffic that can be transmitted in a given interval.

3. In the **PIR** field, select the peak information rate (PIR) from the list. The PIR is the shaping rate.

NOTE: If the QoS profile that you selected in Step 1 is configured with a level-three scheduler and interface oversubscription is enabled, then PIR is not used.

Specifying OAM Settings

To enable OAM on the service definition, enter information in the OAM Settings of the General/Connectivity Settings panel.

1. In the **CFM Definition** 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.

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. Continue with "Specifying Endpoint Information," next.

Setting Attributes for All Endpoints

This part of the create multipoint Ethernet service order procedure sets the attributes that are usually common for all endpoints in the service.

If a template was attached to the service definition on which the service order is based, the link to invoke the template editor appears on the **Endpoint Settings** page.

The values that you type varies, depending 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.

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 756](#).

Setting Attributes for Endpoints 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.

This procedure sets the attributes listed in the **End Point Settings** box of the **Enter Order Information** window. The attributes shown depend on the interface type and the signaling type. The following example shows the endpoints settings box for a point-to-multipoint service order with Q-in-Q interfaces, transporting a VLAN range.

End Point Settings

These settings from the selected Service Definition can be applied to all end points.

Bandwidth range: 10000Kbps - 100Mbps

Bandwidth: 10 Mbps

MTU (Bytes): 1522

MTU Factor: 10

Physical IF encapsulation: flexible-ethernet-services Logical IF encapsulation: vlan-vpls

Logical IF Settings

Auto-pick VLAN range constraint: 1-4094

☐ Autopick VLAN ID

VLAN ID: 2

☐ Autopick UNIT ID

UNIT ID: 30

NOTE: When the **Allow multihoming** check box is selected for the service definition on which the service order based, the **End Point Settings** box displays the **Allow multihoming on endpoints** check box to indicate that the service can include multihomed groups.

To set attributes common to most endpoints:

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. In the **VLAN Tag to stack** field, type a value for the customer VLAN.

This field is present only for services that specify Normalize to Dot1q tags.

7. In the **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.

8. In the **Outer VLAN Tag to Stack** field, type a value to provide an outer VLAN tag that matches the Outer VLAN tag of at least one of the UNI endpoints.

9. In the **Inner VLAN Tag to Stack** field, type a value to provide a default inner VLAN tag for the UNI endpoints to provide a common inner VLAN tag for the routing instance.

This field is present only for services that specify Normalize to QinQ tags.

10. The **LDP PW Extension Settings** field is available only if you have enabled the **Enable PW Extension** check box in the selected service definition.

The **Physical IF encapsulation** and **Logical IF encapsulation** fields are not selectable. These values are set in the service definition.

11. Specify the Logical If Settings:

NOTE: The Logical If Settings box is not available if you have selected the **Ethernet option** as Port.

- 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.

- 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.

12. Click **Next**.

The **Select Endpoint PE Devices** window appears.

13. Continue with "Selecting N-PE Devices and Multihomed Groups."

Setting Attributes for Endpoints 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.

This procedure sets the attributes listed in the **End Point Settings** box of the **Enter Order Information** window. 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 order that specifies a service with flexible VLAN tagging that is normalized to Dot1Q and transports a single VLAN.

NOTE: When the **Allow multihoming** check box is selected for the service definition on which the service order based, the **End Point Settings** box displays the **Allow multihoming on endpoints** check box to indicate that the service can include multihomed groups.

To set attributes common to most endpoints:

1. 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 can be configured in the service order only if the service definition allows it.
2. 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.
3. If the signaling type is LDP and the if the auto discovery is enabled, the **Autopick VPN ID** appears dimmed. This field is not editable in the service order,
4. Specify the **VPLS ID** if the **Autopick VPLS ID** is disabled.
Range: 1 through 2147483647
5. Specify the **VPN ID** if the **Autopick VPN ID** is enabled.
Range: 1 through 65535
6. The **LDP PW Extension Settings** is available only if you have enabled the **Enable PW Extension** check box in the selected service definition.
7. To configure VLANs, choose from the following options depending on the VLAN transport type and Normalization that the service specifies:
 - If the service transports single VLANs and traffic is Normalized to Dot1Q tag:
 - a. In the **Inner VLAN (for Q-in-Q)** field, type a VLAN ID to swap.
 - b. In the **VLAN Tag to stack** field, type a VLAN ID to push or swap at the relevant UNI endpoints.
 - If the service transports single VLANs and traffic is Normalized to QinQ tags:
 - a. To manually assign an VLAN ID:
 - i. Clear the **Autopick VLAN ID** check box. The window expands to include the **VLAN ID** field.

This field is present in the service order only if the service definition allows it.

- ii. In the **VLAN ID** field, type a value.

This field is configurable in the service order only if the service definition allows it.

- b. In the **Inner VLAN (for Q-in-Q)** field, type a VLAN ID to swap.
- c. In the **Outer VLAN Tag to stack** field, type a VLAN ID to push or swap at the relevant UNI endpoints.
- d. In the **Inner VLAN Tag to stack** field, type a VLAN ID to push or swap at the relevant UNI endpoints.
- If the service transports single VLANs and traffic is Normalized to VLAN none:
 - In the **Inner VLAN (for Q-in-Q)** field, type a VLAN ID to swap.
- If the service transports all traffic and specifies Normalize to VLAN all:
 - a. 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.
 - b. In the **VLAN Tag to stack** field, type a VLAN ID to push or swap at the relevant UNI endpoints.
- If the service transports a range of VLANs and specifies Normalized VLAN all:
 - a. 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.
 - b. In the **VLAN Tag to stack** field, type a VLAN ID to push or swap at the relevant UNI endpoints.

NOTE: A service that transports of a range of VLANs and specifies Normalized VLAN all allows only 802.1Q, and Q-in-Q interfaces for the UNI endpoints.

8. Click **Next**.

The **Select Endpoint PE Devices** window appears.

9. Continue with "Selecting N-PE Devices and Multihomed Groups," next.

Selecting N-PE Devices and Multihomed Groups

This part of the create point-to-multipoint Ethernet service order procedure selects the N-PE devices and, optionally, multihomed groups that hosts the service endpoints. The selection is made from the **Select Endpoint PE devices** window.

NOTE: If multihoming is enabled on the service definition on which the service order is based and you have configured and imported the connectivity file, you can select PE devices and multihomed groups that are specified in the multihomed groups connectivity file for the service endpoints.

NOTE: The **Select Endpoint PE devices** window 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.

To select endpoint N-PE devices and multihomed groups:

1. In the **Select Endpoint PE devices** window, select the devices and multihomed groups that you want to participate in the service. Use the multiple selection feature to select one or more devices.
 2. Click **Next**.
- The **Endpoint Settings** window appears.

Selecting Hubs and Modifying Endpoint Settings

This part of the create point-to-multipoint Ethernet service order procedure selects the devices that are service hubs and sets the attributes for each endpoint in the service. Selection is made using the **Endpoint Settings** window.

Endpoint Settings									
Add Endpoints									
Device	Ethernet Option	UNI Interface	Description	Autopick UNIT ID	UNIT ID	AutoPick VLAN ID	Inner VLAN ID	MTU (Bytes)	Action
<input checked="" type="checkbox"/> Hub	Device: amx-1100-a (1 Interface)		Add Label						Add UNI Interface
amx-1100-a	dot1q	ge-1/2/3		true	0	<input checked="" type="checkbox"/>	N/A	1522	Delete UNI Interface
<input type="checkbox"/> Hub	Device: amx-1100-b (1 Interface)	Neighbor Hub	Add Label						Add UNI Interface
amx-1100-b	qinq	em0		true	0	<input checked="" type="checkbox"/>	0	1522	Delete UNI Interface

This window shows one endpoint for each device that you selected from the **Select Endpoint PE devices** window, as described in [“Selecting N-PE Devices and Multihomed Groups” on page 690](#).

The interface shown in the **UNI Interface** field is automatically selected by the Network Activate software, 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.

- For port-to-port services, the displayed values are for Bandwidth and MTU.
- For 802.1Q UNIs, the displayed attributes are for 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.

The values shown are initially the values you set earlier on the **Enter Order Information** window, as described in [“Setting Attributes for Endpoints on a Service” on page 684](#).

To modify the endpoint settings:

1. For a service with flexible VLAN tagging, set the interface type in the Ethernet Option column for each endpoint in the service.
2. To select a hub, choose the device you want to serve as a hub and, above the device name, select **Hub**. The **Neighbor Hub** link is not applicable for hub devices.
To provide a higher level of availability, you can select multiple hubs.
3. To fill in the neighbor hub details for a spoke device, click the **Neighbor Hub** link. The **Neighbor Hub Setting** window is displayed.

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

Fill in the following information:

- **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.

4. To select a different UNI on a device, on the **Endpoint Settings** window, click the UNI name you want to change and choose another interface from the list.

Modified values are indicated by a small red triangle in the corner of the table cell.

5. To enter the description for an UNI interface, click the corresponding **Description** cell.

6. To change the bandwidth on an endpoint, click the bandwidth value for the endpoint and select another value from the list.

7. To change the committed information rate (CIR) on an endpoint, click the CIR value for the endpoint and select another value from the list. The value for CIR should be less than the value for PIR.

Only QoS-enabled services specify CIR and PIR values.

8. To change the peak information rate (PIR) on an endpoint, click the PIR value for the endpoint and select another value from the list. The value for PIR should be greater than the value for CIR.

Only QoS-enabled services specify CIR and PIR values.

9. The **AutoPick 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 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 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.

10. 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 a service 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.

11. For Q-in-Q interface endpoints with customer VLAN ranges specified, you can also change the range limits for an endpoint.

12. For 802.1Q interface endpoints, you can change the customer VLAN ID.

13. To change the MTU for the UNI, click the value in the MTU field and type a new value.

14. To add a UNI on a selected device, select **Add UNI Interface** in the **Action** column, and then select the interface you want from the UNI interface list.

You can add only one UNI interface for the point-to-point spoke device. If more than one UNI interface exists for a spoke device, you cannot select the **Enable P2P-Spoke** check box in the **Neighbor Hub** link.

15. If the interface you selected in the previous step is already configured (duplicate) you must either type a different value in the service **VLAN ID** field manually, or select the **Autopick VLAN ID** check box.

16. To delete a UNI from a device, in the **Action** column, click **Delete UNI Interface**.

If the deleted UNI is the only UNI selected from the device, then the device is deleted from the service configuration.

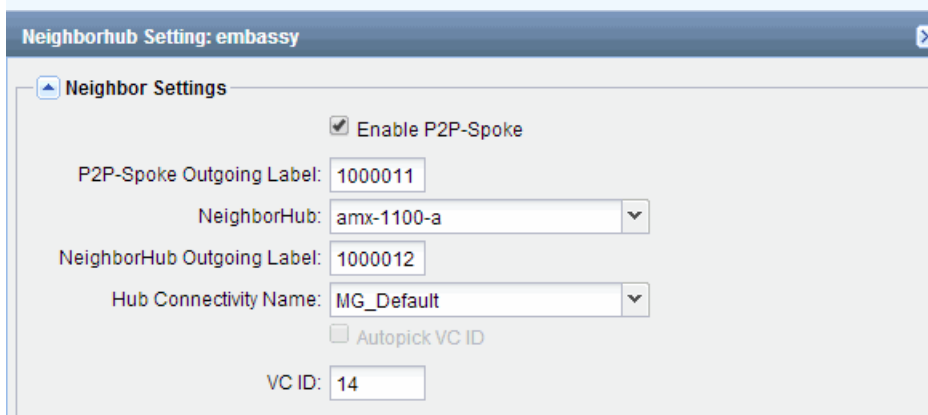
If a hub device is neighbor of a point-to-point spoke device, you cannot delete the device. To delete such device, you must delete the point-to-point spoke device, or change the point-to-point spoke to VPLS spoke.

17. To enter the value of **Outgoing Label** for any device, click the **Add Label** link that is associated with that device. You can enter the value in the **Outgoing Label Settings** window and click **OK** to save the value. Select the hub and spoke devices in the **Endpoint Settings** window.

18. To view the values of the **Incoming Label**, **Outgoing Label** and the **Neighboring Device** of any device, use the following method:

- a. Select **Manage Service Orders > View Service Order Details**
- b. Click the **Label Details** link associated with any device.

NOTE: When the signaling type is BGP and the service type is Point-to-Multipoint Ethernet VPLS, the **Label Details** link is not available under the **Endpoint Settings** link when you create or modify a service order. In the **Endpoint Settings** window, you need to select the devices that are going to act as hub because some devices act as hub and some act as spoke when the service type is **Point-to-Multipoint**. Now click the **Neighbor Hub** link that is associated with the devices acting as spokes. The **Neighborhub Setting** window that appears for the selected spoke device allows you to enter the details of the outgoing label values of **P2P-Spoke** and **neighbor hub**. The window displays details about the **Neighborhub** device, the **Backup Neighborhub** device, **Hub Connectivity Name** and **VC ID**. To specify and view these details, you need to select the **Enable P2P-Spoke** checkbox. If the **Enable P2P-Spoke** checkbox is not selected, you cannot specify any of these values.



Neighborhub Setting: embassy

Neighbor Settings

☒ Enable P2P-Spoke

P2P-Spoke Outgoing Label: 1000011

NeighborHub: amx-1100-a

NeighborHub Outgoing Label: 1000012

Hub Connectivity Name: MG_Default

☐ Autopick VC ID

VC ID: 14

19. To specify a different primary device for a multihomed group in the service:

- a. From the list of secondary devices, select a secondary device that you want to specify as the primary device in the multihomed group.
- b. Click **Set As Primary**.
- c. Click **Create**.

The secondary device is configured as the primary device in the multihomed group.

20. For spoke devices, in the **Neighbor Hub** select the hub device.

21. 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.

NOTE: The **Advanced** link is not available for a point-to-point spoke.

To change settings on an endpoint that has editable advanced settings:

- a. Click **Advanced** in the **Action** column.

The **Advanced Setting** window displays the security and advanced settings that you can configure for a device.



The screenshot shows a window titled "Advanced Setting: junos-mx240-space". Inside, there is a section titled "MAC Security Settings" with a minus icon to its left. This section contains the following settings:

- ☒ MAC learning
- Interface MAC limit:
- ☐ MAC statistics
- MAC table size:

At the bottom of the window are two buttons: "OK" and "Cancel".

See ["Service Attributes Overview" on page 152](#) for complete information about MAC security settings and advanced settings.

- b. In the **MAC Security Settings** box, make selections for MAC learning and MAC statistics and type values for Interface MAC limit, MAC table size, and MAC table aging time.
- c. Enable or disable tunnel services by selecting or clearing the **disable-tunnel-service** check box.
- d. Enable or disable local switching by selecting or clearing the **disable-local-switching** check box.

- e. In the **Fast reroute priority** field, specify the reroute priority for a VPLS routing instance.
- f. In the **Label block size** field, specify the label block size for VPLS labels.
- g. 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)
- h. Click **OK** to save your changes in the **Advanced** window.

22. To add an endpoint on a device not listed in the Endpoint Settings window:

- a. Click **Add Endpoints**.

The **Add Endpoint PE Devices** window displays the available N-PE devices that you did not assign when you first made your device selections from the **Select Endpoint PE devices** window.

- b. Select additional devices, then click **Next**.

The **Endpoint Settings** window appears with the new devices added.

- c. Modify the endpoint settings for this device, as required.

23. If you have attached a service template in the service definition, the **Flexible Service Attributes** link appears. Click the link to modify the service template attributes. For more information about configuring the flexible service attributes, see [“Configuring Flexible Service Attributes to Modify Service Template Attributes” on page 938](#).

24. When you have finished modifying the endpoint settings, click **Create**.

The **Deployment Options** window appears.

The service order that you have created is graphically represented in the network topology. In the network topology, to view the service order that you have created, select **Platform > Network Monitoring > Topology > Service > NA service order name**.

For more information on network topology, see [“Junos Space Network Topology Overview” on page 31](#).

25. Continue with "Deploying the New Service," next.

Deploying the New Service

This part of the create multipoint Ethernet service order procedure deploys the service.

To deploy the service from the **Deployment Options** window:

1. Perform one of the following actions:

- To validate and save the request without deploying the service, select the **Validate** check box, select **Save only**, then click **OK**.

See [“Deploying a Service Order” on page 631](#) for information about how to deploy a saved service at a later time.

- To save the request without validating the service, clear the **Validate** check box, select **Save only**, then click **OK**.

See [“Deploying a Service Order” on page 631](#) for information about how to deploy a saved service at a later time.

- 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.

2. Monitor the status of the deployment using the **Jobs** workspace.

The service order is now complete.

The **Manage Service Orders** page shows the service order you just added. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details about the Jobs workspace.

RELATED DOCUMENTATION

Viewing Jobs in the *Junos Space Network Application Platform User Guide*

[Viewing Service Orders | 620](#)

[Service Attributes Overview | 152](#)

[Adding a New Customer | 1056](#)

[Deploying a Service Order | 631](#)

[Force-Deploying a Service | 632](#)

[Creating a Multipoint-to-Multipoint VPLS Service Order | 660](#)

[Creating a Point-to-Point Service Order | 586](#)

[Understanding VLAN Manipulation \(Normalization and VLAN Mapping\) on Ethernet Services | 710](#)

[Creating a Service Order Based on a Service Definition with a Template | 756](#)

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. In the **Network Activate** task pane, select **Service Provisioning > Manage Service Orders > Create 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.

Service Provisioning > Manage Service Orders > Create VPLS Service Order

State	Name	Service Type	Signaling	Created By
→ Published	ELAN-BGP-QinQ-AllVLAN	VPLS (MultiPoint-MultiPoint)	BGP	super
→ Published	ELAN-BGP-Dot1Q-SingleVLAN	VPLS (MultiPoint-MultiPoint)	BGP	super
→ Published	ELAN-BGP-PortBased-10-100M	VPLS (MultiPoint-MultiPoint)	BGP	super
→ Published	ELAN-BGP-QinQ-Range-Normalized-VLAN	VPLS (MultiPoint-MultiPoint)	BGP	super
→ Published	ELAN-BGP-QinQ-AllVLAN-Normalized-All	VPLS (MultiPoint-MultiPoint)	BGP	super
→ Published	ELAN-BGP-QinQ-AllVLAN-Normalized-None	VPLS (MultiPoint-MultiPoint)	BGP	super
→ Published	ELAN-BGP-Dot1q-Normalized-VLAN-None	VPLS (MultiPoint-MultiPoint)	BGP	super
→ Published	ELAN-Hub-Spoke-QinQ-AllVLAN-Normalized-All	VPLS (Point-MultiPoint)	BGP	super
→ Published	ELAN-Hub-Spoke-QinQ-AllVLAN	VPLS (Point-MultiPoint)	BGP	super

Page 1 of 1 | Displaying 1 - 14 of 15 | Show 30 items

Next Cancel

2. Select the service definition you want to base your service order on, then click **Next**.

The **Enter Order Information** window appears.

General Settings

Service Provisioning > Manage Service Orders > Create VPLS Service Order

Enter Order Information

General Settings

Service definition: ELAN-BGP-QinQ-Range-Normalized-VLAN

Name:

Customer:

Please select ...

Comments:

Customer traffic type: Transport vlan range

Signaling: BGP

Connectivity Settings

☒ Autopick Route Target

End Point Settings

These settings from the selected Service Definition can be applied to all end points.

Bandwidth range: 10000Kbps - 100Mbps

Next

Cancel

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 1056.</p>

Field	Action
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>

1. Continue with the **End Point Settings** panel.

End Point Settings

Service Provisioning > Manage Service Orders > **Create VPLS Service Order**

Enter Order Information

End Point Settings

These settings from the selected Service Definition can be applied to all end points.

Bandwidth range: 10000Kbps - 100Mbps

Bandwidth : 10 Mbps

MTU (Bytes): 1522

Auto-pick VLAN range constraint: 1-4094

☒ Autopick VLAN ID

Customer VLAN Range Start:

Customer VLAN Range End:

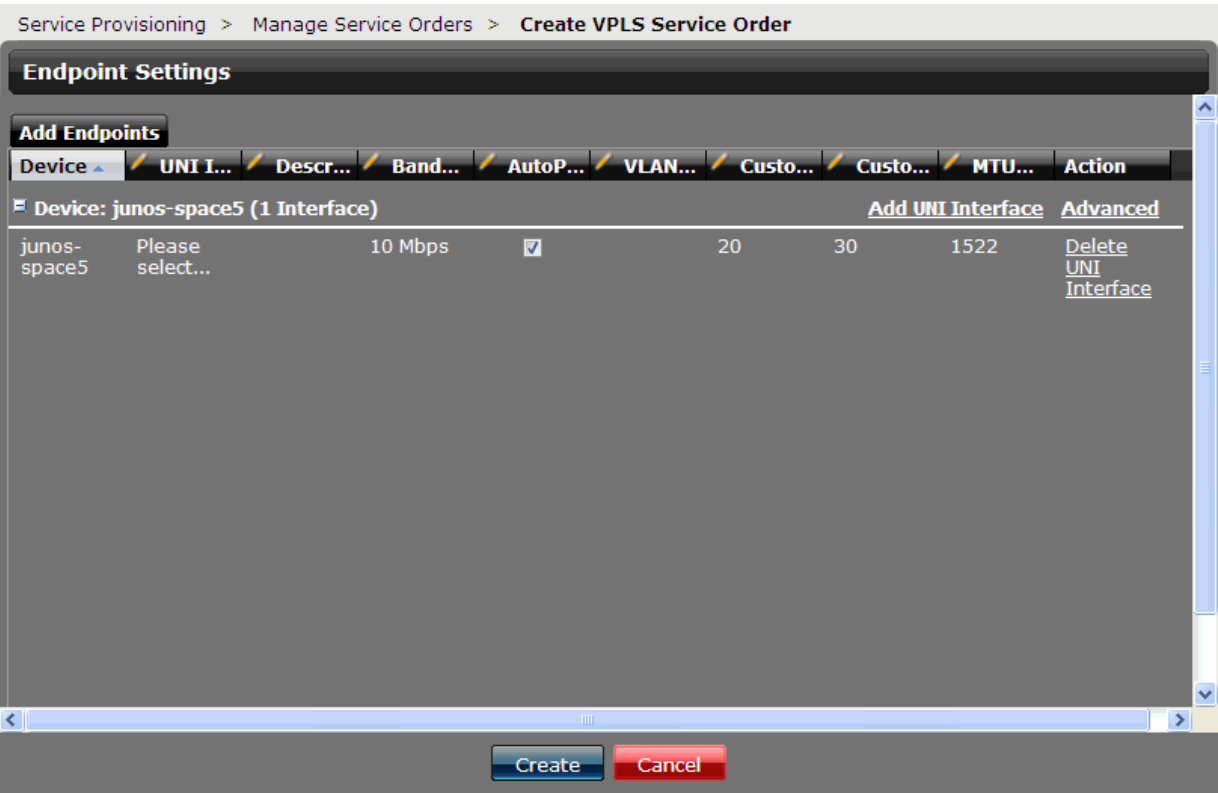
Physical IF encapsulation: flexible-ethernet-services Logical I

OAM Settings

Next Cancel

Field	Action
Apply to all	Check this box if you want these settings applied to all end points for this VPLS service order.
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.

1. Click **Next** to display the device list where you will select the end point devices.



2. Select the devices you will use for this Layer 3 access.
3. 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 **Endpoint Settings** panel.

Service Provisioning > Manage Service Orders > **Create VPLS Service Order**

Endpoint Settings

Add Endpoints

Device	UNI I...	Descr...	Band...	AutoP...	VLAN...	Custo...	Custo...	MTU...	Action
Device: junos-mx480-space (1 Interface)									
junos-mx480-space	Please select...		10 Mbps	<input checked="" type="checkbox"/>	20	30		1522	Delete UNI Interface
Device: junos-mx80-1-space (1 Interface)									
junos-mx80-1-space	Please select...		10 Mbps	<input checked="" type="checkbox"/>	20	30		1522	Delete UNI Interface
Device: junos-space5 (1 Interface)									
junos-space5	Please select...		10 Mbps	<input checked="" type="checkbox"/>	20	30		1522	Delete UNI Interface

4. Select the IRB interface and click **Create**. You will be prompted to deploy the service with the standard **Deploy Service** panel.

Verify the Service Order Results

After you have created the VPLS service order, return to the **Manage Service** screen.

1. Select the service you just deployed and right-click to display the action menu.
2. Select **View Service Configuration Change** to display the service configuration.



RELATED DOCUMENTATION

[Creating a Service Definition for VPLS Access into Layer 3 Networks](#) | 369

[Performing a Functional Audit](#) | 1064

Creating a VPLS Service Order in Cross Provisioning Platform

Cross Provisioning Platform is an extension of the Network Activate application within Junos Space, which provides a single pane of interaction to deploy services across vendor network devices. This topic discusses how to create and deploy a VPLS service order across the devices of Juniper Networks involved in Cross Provisioning Platform.

You need to create VPLS service definition before you can create VPLS service order. Refer to [“Creating a VPLS Service Definition in Cross Provisioning Platform” on page 311](#) for information about how to create a VPLS service definition.

To create a VPLS service order:

1. In the **Cross Provisioning Platform** task pane, select **CPP > Service Orders**.

The **Service Orders** page that appears displays a list of the existing service orders.

2. Click the **Create Service Order** icon above the tool grid.

The **Create CPP Service Order** page that appears contains the **General** section.

3. In the **General Settings** section, perform the following steps:

- a. In the **Select Service Definition** section, select a service definition based on the unique ID, name or type.

NOTE: The value in the **ID** field is associated with a service definition. This identifier can be used when you are searching for a particular service definition while creating a device configlet order. You can search the service definition by its name, type or unique ID. You can modify the ID only during the migration of old service definition IDs.

CPP > Service Orders > Create CPP Service Order

Create CPP Service Order

General Settings

Select Service Definition

ID	Name	Type
	VPLS_SD	VPLS
	P2P_SD	PW-LDP
5678	Test_SD_123	PW-LDP
1234	Test_123_P2P	PW-LDP
4321	Test_123_VPLS	VPLS

Page 1 of 1 | Displaying 1 - 5 of 5 | Show 30 items

Description:

Next Cancel

- b. In the **Order description** field, type 3 through 256 alphanumeric characters to describe the service order.
4. Click **Create**.

The VPLS service order page appears.

NOTE: The name of the page depends according to the details of the service definition.

5. In the VPLS service order page, enter the **General**, **Jumbo**, **Site B selector**, **Site A - Customer Facing Port**, and **Site B - Customer Facing Port** details.

The screenshot shows the 'Create CES-CCI Service' interface with the following sections:

- General:**
 - Name: SO387489310
 - External ID: (empty)
- Service Options:**
 - VPLS ID: 1
- Step1: Select Site** (Vendor: Juniper):

Site Name	Loopback	Vendor
10.216.128.1	192.168.1.10	Juniper
10.216.128.10	192.168.1.10	Juniper
10.216.128.100	192.168.1.10	Juniper
- Step2: Select Site Interface**:

Site Name	Port	Encapsulation	Speed	Status
10.216.128.10	ge-0/0/2	none	1000	up
10.216.128.10	ge-0/0/3	flexible-ethernet-services	1000	up
- Step3: Enter Staged Interface Details**:

Site Name	Port	VLAN ID	Validate VLAN	Speed	Action
Site Name: 10.216.128.10 (2 Items)					
10.216.128.10	ge-0/0/2		✓	1000	✗
10.216.128.10	ge-0/0/3		✓	1000	✗

Buttons at the bottom: Create, Clear, Create More, Cancel.

NOTE: The fields that appear on the **Endpoint Settings** page are determined by the information that you provide while creating the VPLS service definition that you attach with this service order.

6. Enter the **Site name**, **Port**, **Service speed**, **Outer encapsulation**, and **Inner encapsulation** details in the customer-facing port section of site A and site B.
7. Enter the details of **Site name**, **UNI port**, **Uplink port**, and **UNI encapsulation** in the customer-facing port section of site A and site B if the **L2 Extension** check box is selected for both the sections.

RELATED DOCUMENTATION

| [Creating a VPLS Service Definition in Cross Provisioning Platform](#) | 311

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.

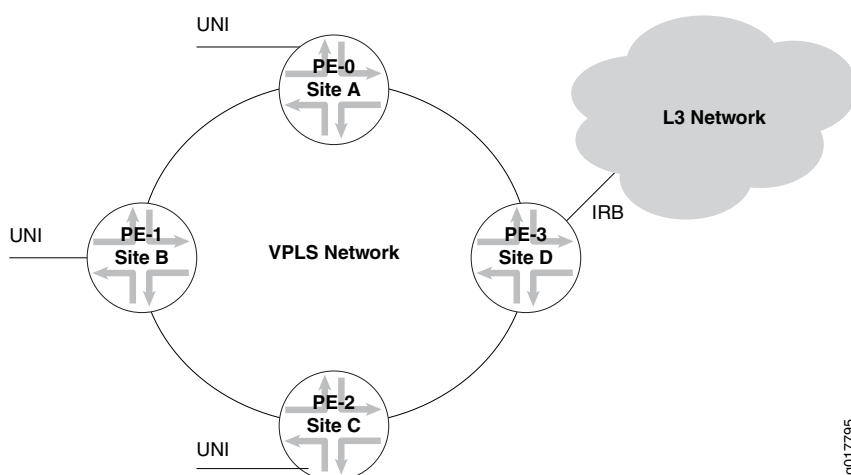
Using MPLS pseudowires makes it possible to encapsulate Layer 2 packets and extend Layer 2 services into Layer 3 networks. Junos Space supports the trend toward accomplishing Seamless MPLS with these two features:

- 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

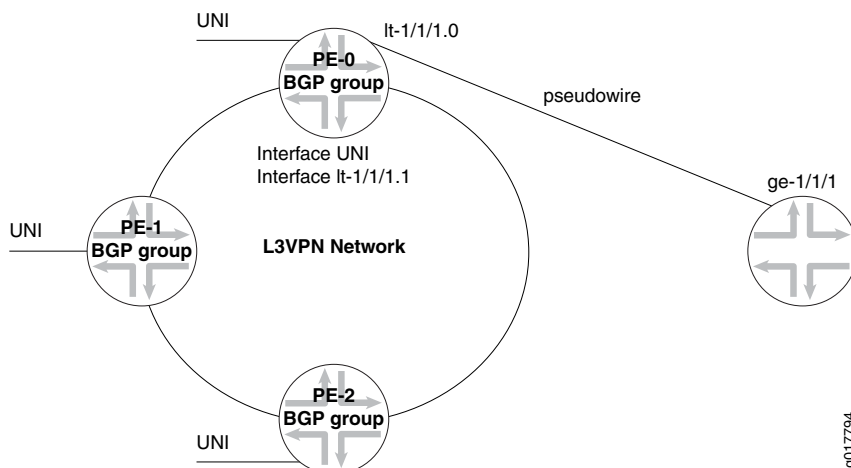
declare it as routing-interface rather than regular VPLS interface (which acts like the interface on a specific VPLS Site). This feature requires a normalized VLAN (vlan-id=xxx which is the same as the unit name on which the inet4 address is specified)



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 | 369](#)

[Creating a Service Order for VPLS Access into Layer 3 Networks | 698](#)

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 Network Activate software 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 Network Activate software 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 31 on page 712](#).
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 32 on page 713](#).

[Table 31 on page 712](#) and [Table 32 on page 713](#) 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 Network Activate, 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 31: 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
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 32: 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
    }
  }
}

```

```

##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

[Service Attributes Overview | 152](#)

[Creating a Point-to-Multipoint VPLS Service Order | 678](#)

[Creating a Multipoint-to-Multipoint VPLS Service Order | 660](#)

Layer 3 VPN Service Orders

IN THIS CHAPTER

- [Stitching a Pseudowire to an L3VPN Service | 715](#)
- [Creating a Full Mesh Layer 3 VPN Ethernet Service Order | 718](#)
- [Creating a Hub-and-Spoke Layer 3 VPN Service Order | 733](#)
- [Creating a Multicast VPN Service Order | 748](#)
- [Selecting a Published L3VPN Service Definition for a Service Order | 753](#)
- [Entering Layer 3 VPN Order Information | 753](#)
- [Selecting Endpoint PE Devices | 755](#)
- [Creating a Service Order Based on a Service Definition with a Template | 756](#)
- [Deploying a Layer 3 VPN Service Order | 759](#)
- [Creating a Cross Provisioning Platform Layer 3 VPN Service Order | 760](#)
- [Creating a Layer 3 VPN Service Order in Cross Provisioning Platform for Third-Party Devices | 765](#)

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 tab, 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 an E-Line Service Definition” on page 188](#).

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 376](#). 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 386](#).

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 718](#). For information about creating a hub-and-spoke service order, see [“Creating a Hub-and-Spoke Layer 3 VPN Service Order” on page 733](#).

4. In the Manage Services inventory page, right-click a Layer 3 VPN service that you created and select **Service > Extend PW Service**.

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

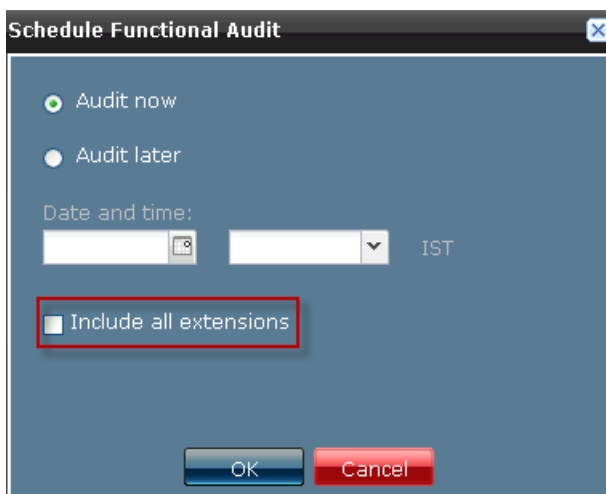
NOTE: This field is prepopulated for a stitched end of the point-to-point service.

- **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 586](#).

The Layer 3 VPN Service Details window now displays the **PW Extension** details.

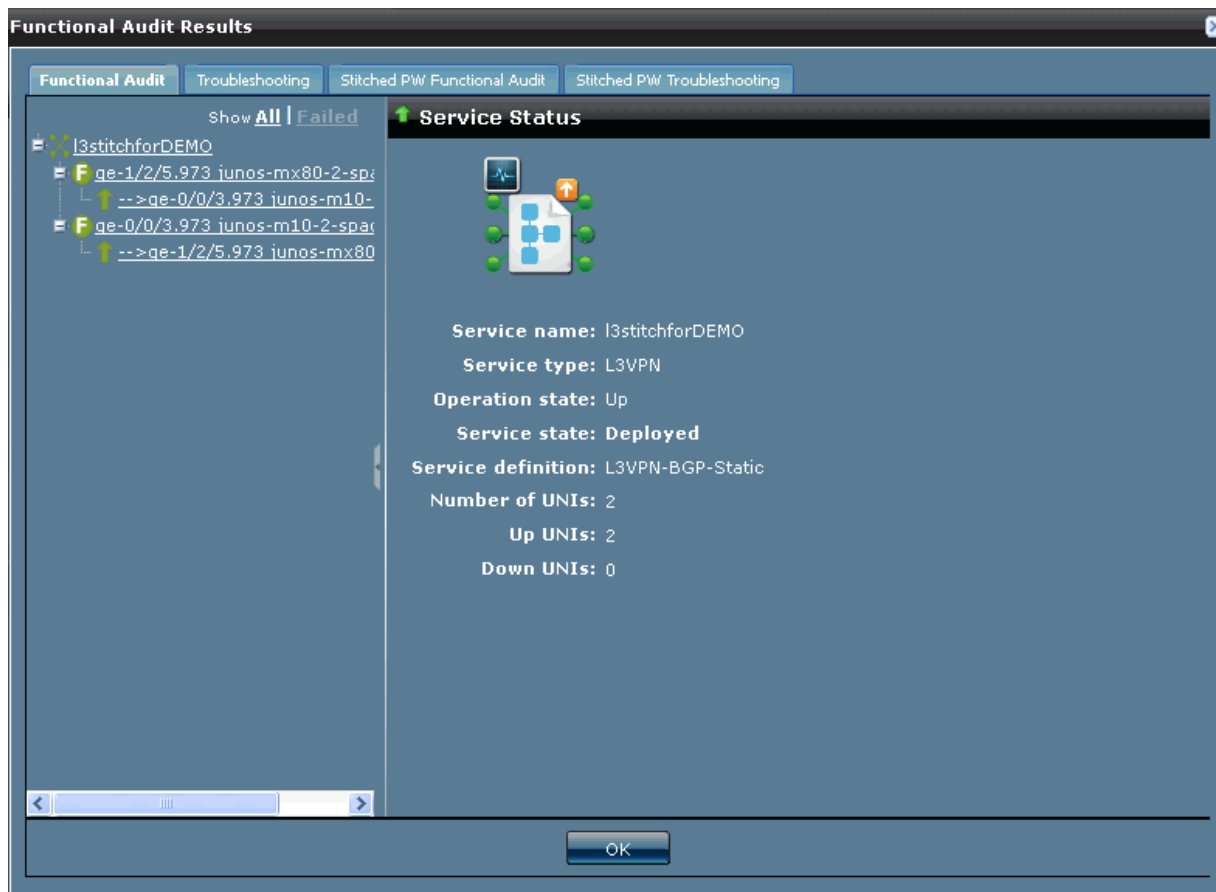
When you perform a functional audit for a Layer 3 VPN service with pseudowire termination, by default the functional audit is applicable only to the Layer 3 VPN service. To perform a functional audit for the pseudowires, select the **Include all extensions** check box in the Schedule Functional Audit 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 | 578](#)

[Creating a Point-to-Point Service Order | 586](#)

Creating a Full Mesh Layer 3 VPN Ethernet Service Order

You can use the Network Activate software to implement Layer 3 VPN Ethernet services.

To create a Layer 3 VPN full mesh Ethernet service order, complete the following tasks in order:

1. [Selecting the Service Definition | 719](#)
2. [Configuring Order Information | 719](#)
3. [Selecting N-PE Devices | 725](#)
4. [Setting Attributes for UNI Endpoints | 726](#)

5. [Adding, Deleting, and Modifying Endpoints | 731](#)
6. [Deploying the New Service | 732](#)

Selecting the Service Definition

To select a service definition on which to base the new service order:

1. Select **Service Provisioning > Manage Service Orders > Create L3 VPN Service Order**.

The **Select Service Definition** page appears and shows a filtered inventory view of only those published service definitions designed to work with Layer 3 VPN full mesh Ethernet services.

2. Select the service definition on which you want to base your service order, and then click **Next**.

The **Enter Order Information** window appears.

Configuring Order Information

IN THIS SECTION

- [Specifying General Settings | 719](#)
- [Specifying QoS Settings | 720](#)
- [Specifying VPN Settings and PE-CE Settings Information | 721](#)

You can configure general settings, VPN settings that can be applied to all end points, and routing protocol settings for provider edge (PE) and customer edge (CE) devices.

Specifying General Settings

You configure general information about the service order in the General Settings section of the Enter Order Information window.

If a service template is attached to the service definition, a link to that template is provided 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 756](#).

You must add the customer to the database before proceeding. See [“Adding a New Customer” on page 1056](#).

Enter Order Information

General Settings

Service definition: L3vpn_FLX_QOS_BGP_FM

Name:

Customer: ▼

Comments:

☐ Enable MVPN

☐ Enable MC LAG

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, periods, hyphens, 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.

4. Select the **Enable MVPN** check box to enable multicast virtual private network (MVPN).
5. Select the **Enable MC LAG** check box to enable the multichassis link aggregation group. If you select this check box, the **Enable MVPN** check box is disabled.

For more information about multichassis link aggregation groups (MC-LAGs), see [“Multichassis Link Aggregation Group Overview” on page 168](#).

Specifying QoS Settings

If you have selected the Enable QoS check box in the selected service definition, you must configure QoS settings.

To configure QoS settings:

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 QoS Design software.

A QoS profile classifies traffic into defined service groups to provide special treatment of traffic across the network service.

2. In the **CIR** field, select the committed information rate (CIR) from the list.

The CIR is the guaranteed rate, which specifies the minimum bandwidth available if all sources are active at the same time. Make sure that the CIR value is less than the PIR value.

NOTE: For bursty traffic, the CIR represents the average rate of traffic per unit time and the PIR represents the maximum amount of traffic that can be transmitted in a given interval.

3. In the **PIR** field, select the peak information rate (PIR) from the list. The PIR is the shaping rate.

NOTE: If the QoS profile that you selected in Step 1 is configured with a level-three scheduler and interface oversubscription is enabled, then PIR is not used.

Specifying VPN Settings and PE-CE Settings Information

You configure VPN attributes that are usually common for all 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.

VPN Settings

These settings from the selected Service Definition can be applied to all end points.

☐ Autopick UNID ID

UNIT ID:

☐ Autopick VLAN ID

VLAN ID:

☐ Autopick Route Target

Route Target:

☐ Autopick Route Distinguisher

Route distinguisher:

☒ Autopick Interface IP Address

☒ VRF Table label

☒ Export Direct Routes

PE-CE Settings

Routing protocol: OSPF/Static Route

OSPF domain ID:

To set attributes common to most endpoints on a service:

1. 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.

2. Specify the **MTU Factor** or **Burst Period**, based on the **Calculate Burst Size** you have selected in the service definition.

NOTE: You cannot edit these fields if you have not selected the **Editable in Service Order** check box in the service definition.

3. Select the bandwidth from the **Bandwidth** list. The **Bandwidth Range** and **Bandwidth** fields appear only if you have cleared the **Enable QoS** check box in the selected service definition:

NOTE: You cannot edit these fields if you have not selected the **Editable in Service Order** check box in the service definition.

4.

NOTE: The fields specified in the Logical IF Settings section are based on the **Ethernet option** type. The Logical IF Settings section is not available if you have selected the **Ethernet option** as *Port*.

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.

5. 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.

6. Specify whether the **Autopick Route target** can be selected automatically or manually.

- To assign the **Route Target** automatically, select the **Autopick Route target** check box.
- To assign the **Route Target**, clear the **Autopick 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 **Autopick 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.

7. Specify whether the **Autopick VLAN ID** can be selected automatically or manually.

- 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.

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.

8. 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.

9. Specify whether a service provider can create static routes on the service.

- To allow the service provisioner to create static routes on the service, select the **Static Route** check box.
- To prevent the service provisioner from creating static routes on the service, clear the **Static Route** check box.

10. If **BGP routing protocol** is specified in the service definition, specify whether the service provider can override the AS number.

- To allow the service provisioner to override the AS number, select the **AS override** check box.
- To prevent the service provisioner from overriding the AS number, clear the **AS override** check box.

If **OSPF routing protocol** is specified in the service definition, in the **OSPF domain ID** field, specify any valid IPv4 address.

11. Click **Next**.

The **Select Endpoint PE Devices** window appears.

Selecting N-PE Devices

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 **Select Endpoint PE Devices** window 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.

3 Items Selected				
<input type="checkbox"/> Name ▲	Role	Additional Role	Management Address	Loopback Address
<input type="checkbox"/> embassy	N_PE	N/A	10.216.114.109	50.1.2.4
<input checked="" type="checkbox"/> junos-m10-1-space	N_PE	N/A	10.216.114.102	30.1.2.4
<input type="checkbox"/> junos-m10-2-space	N_PE	N/A	10.216.114.103	30.1.2.2
<input checked="" type="checkbox"/> junos-mx480-space	N_PE	N/A	10.216.114.100	30.1.2.6
<input type="checkbox"/> junos-mx80-1-space	N_PE	N/A	10.216.114.104	30.1.2.5
<input checked="" type="checkbox"/> junos-mx80-2-space	N_PE	N/A	10.216.114.105	30.1.2.3
<input type="checkbox"/> junos-space2	N_PE	CSR	10.216.114.120	30.1.2.8
<input type="checkbox"/> kochin	N_PE	N/A	10.216.114.110	50.1.2.1

To select endpoint N-PE devices:

1. In the **Select Endpoint PE** devices window, select the devices that you want to participate in the service. You can select more than one device.
2. Click **Next**.

The **Endpoint Settings** window appears.

Setting Attributes for UNI Endpoints

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 756](#).

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 Network Activate software, 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.

Endpoint Settings
Add Endpoints; Add/Delete UNI Interfaces and set values here.

Add Endpoints

Device	UNI Interface	Action
Device: bhuj (1 Item)		
bhuj	ge-0/2/2	
Device: buxar (1 Item)		
buxar	xe-0/3/1	
Device: cuttack (1 Item)		
cuttack	ge-0/1/3	

Device: bhuj Save Add More

☐ Stitching point:
☐ Set loopback:
 Ethernet option:
 UNI interface:
 UNI Description:

Logical IF Settings

☒ Autopick UNIT ID:
☒ Autopick VLAN ID:

☒ Autopick interface IP:
 IP pool type:
 IP address pool:
 IP block size:

Routing Protocol Settings

Routing protocol:
 OSPF area ID:
 OSPF version:

Qos Settings

CIR:
 PIR:
 Mtu:

If you have selected the **Enable MC- LAG** check box in the General Settings section, the **Stitching point** check box is available for each endpoint. If you select this check box, all the parameters of that endpoint are disabled.

To configure or change the endpoint settings:

1. Make sure the **Stitching point** check box is not selected.
2. To add the loopback interface for a Layer 3 VPN service, select the **Set 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.

3. 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).

- **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.

See [“Creating a Service Template” on page 116](#)

When you create a service order based on a service definition with which a service template is associated, the Add Endpoints window includes a link labeled **Flexible Service Attributes**. If you click the link, the you can specify **Outer** and Inner **vlan-tags** in the **Flexible Service Attributes** window.

The screenshot shows the 'Flexible Service Attributes' configuration window. The left pane, titled 'Flexible Configuration', contains a tree view with two items: 'Flexi_Temp' and 'Config Page 1'. The right pane, titled 'Config Page 1', shows the 'vlan-tags' configuration. Under 'vlan-tags', there are two fields: 'Outer' with the value '100' and 'Inner choices' with the value '101'. At the bottom of the window are 'OK' and 'Cancel' buttons.

4. To select a different UNI on a device, click the UNI name you want to change and choose another interface from the list.

NOTE: If you have selected the **Enable MC-LAG** check box in the General Settings window, the **UNI interface** field displays integrated routing and bridging (IRB) interfaces along with the other interfaces.

5. In the **UNI interface**, if you select the integrated routing and bridging (IRB) interface the **MC LAG Interface** field is displayed. Select an interface for MC LAG.

6. In the **UNI Description**, provide a 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

7. Specifying the Logical IF Settings:

NOTE: The fields specified in the Logical IF Settings section are based on the **Ethernet option** type. The Logical IF Settings section is not available if you have selected the **Ethernet option** as *Port*.

- If you have selected the **Ethernet option** as *Dot1Q*, or, *QinQ*, or *Flexible UNI*, 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: 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 **Ethernet option** 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 **Ethernet option** as *QinQ*, select the **Customer VLAN Type**.

If the **Customer VLAN type** is *Transport all traffic*, select **Outer Tag Protocol ID**.

If the **Customer VLAN type** is *Transport single vlan*, select **Customer VLAN**, **Inner Tag Protocol ID**, and **Outer Tag Protocol ID**.

NOTE: You can optionally specify **Inner Tag Protocol ID** and **Outer Tag Protocol ID**.

8. Clear or select 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**, select the **Autopick interface IP** check box.

If you have selected the **Enable MC- LAG** check box in the General Settings window, 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.

9. Clear the **Autopick VLAN ID** check box to specify **VLAN ID**.

10. Select **Routing protocol type**.

- If **Routing protocol type** is **BGP**, specify the following information:
 - **Neighbor IP address**

NOTE: You need to clear the **Autopick neighbor IP** check box to specify **Neighbor IP address**.

- **Peer AS**
- If **Routing protocol type** is **OSPF**, specify the following information:

- **OSPF area ID**—Specify any valid IPv4 address.

NOTE: The IPv4 address that you use must be valid addresses. Refer to <http://www.iana.org/assignments/ipv4-address-space> for the list of restricted IPv4 addresses.

- **OSPF version**—Select the OSPF version from the list.

11. If you have attached a service template to the service definition, the **Flexible Service Attributes** link appears. Click the link to modify the service template attributes. For more information about configuring flexible service attributes, see “[Configuring Flexible Service Attributes to Modify Service Template Attributes](#)” on page 938.

12. If you have selected the **Enable QoS** check box in the service definition, specify the following fields:

- CIR
- PIR
- MTU(Bytes)
- QoS Profile

If you have cleared the **Enable QoS** check box in the service definition, specify the following fields:

- Bandwidth
- Default MTU

For more information about these fields, see “[Creating a Full Mesh Layer 3 VPN Service Definition](#)” on page 376.

13. When you have finished configuring the endpoint settings, click **Create**.

The Deployment Options window appears.

Adding, Deleting, and Modifying Endpoints

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 UNI Interface** icon in the Actions column, and then select the interface you want from the UNI interface list.
2. 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 select the **Autopick VLAN ID** check box.

To delete a UNI interface from a selected device:

- In the Actions column, click the **Delete UNI Interface** icon in the Actions column.

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.

UNI Settings appears on the right side of the window.

2. Modify the **UNI Settings** fields in the right pane.
3. Either apply the attributes you already specified or modify the attributes for other UNI endpoints:
 - To apply the attributes to the UNI interface, select **Save**.
 - To save your changes and modify attributes for other UNI endpoints on the service, select **Add More**.
4. When you have finished modifying the endpoint settings, click **Create**.

The **Deployment Options** window appears.

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**.

For more information on topology, see the [“Junos Space Network Topology Overview” on page 31](#).

Deploying the New Service

To deploy the service:

1. From the **Deployment Options** window, perform one of these actions:
 - To save the request without deploying the service, select **Save only** and then click **OK**.
See [“Deploying a Service Order” on page 631](#) for information about how to deploy a saved service at a later time.
 - 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**.

The **Job ID** dialog box appears.

2. Click the **Job ID** link to monitor the status of the service deployment.

The **Deployment Service** job appears on the **Platform > Jobs > Job Management** inventory page.

3. To view the Deploy Service Order username, user IP address, task, timestamp, description, and job ID, select **Platform > Audit Logs > Audit Log** inventory page to view the Deploy Service Order username, user IP address, task, timestamp, description, and job ID.

The service order is now complete.

The **Manage Service Orders** inventory view shows the service order you just added. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details about the Jobs workspace.

RELATED DOCUMENTATION

Viewing Jobs in the *Junos Space Network Application Platform User Guide*

[Viewing Service Orders | 620](#)

[Service Attributes Overview | 152](#)

[Adding a New Customer | 1056](#)

[Deploying a Service Order | 631](#)

[Force-Deploying a Service | 632](#)

[Creating a Service Order Based on a Service Definition with a Template | 756](#)

Creating a Hub-and-Spoke Layer 3 VPN Service Order

The Network Activate Service can configure and deploy Layer 3 VPN hub-and-spoke service orders. Creating a service order involves the following tasks:

1. [Selecting the Service Definition | 734](#)
2. [Entering Order Information | 734](#)
3. [Selecting Endpoint PE Devices | 740](#)
4. [Configuring Endpoint Settings | 740](#)
5. [Setting Attributes for UNI Endpoints | 741](#)
6. [Adding, Deleting and Modifying Endpoints | 746](#)
7. [Deploying the New Service | 746](#)

Selecting the Service Definition

To select a service definition on which to base the new service order:

1. Select **Service Provisioning > Manage Service Orders > Create L3 VPN Service Order**.

The **Select Service Definition** page appears and shows a filtered inventory view of only those published service definitions designed to work with Layer 3 VPN hub-and-spoke Ethernet services.

2. Select the service definition you want to base your service order on, and then click **Next**.

You must select only those published service definitions configured to work with Layer 3 VPN hub-and-spoke services. See [“Selecting a Published L3VPN Service Definition for a Service Order” on page 753](#).

The **Enter Order Information** screen appears.

Entering Order Information

IN THIS SECTION

- [Entering General Settings Information | 734](#)
- [Specifying QoS Settings | 735](#)
- [Entering VPN Settings and PE-CE Settings Information | 736](#)

This part of the create a Layer 3 VPN hub-and-spoke service order procedure sets general settings, VPN settings that can be applied to all end points, and routing protocol settings for the PE and CE devices.

You must enter the service order general settings, VPN settings, and PE-CE settings on the Enter Order Information page. See [“Entering Layer 3 VPN Order Information” on page 753](#).

Entering General Settings Information

This part of the create Layer 3 VPN hub-and-spoke Ethernet service order procedure sets general information about the service order in the General Settings box of the Enter Order Information screen.

Enter Order Information

General Settings

Service definition: L3VPNTCCHECKSD6

Name: L3VPN_HubandSpoke_SO

Customer: customer_06

Comments:

Enter the following information:

1. In the **Name** field, enter a unique name for the hub-and-spoke service.

The service order name can consist of only letters, numbers, periods, hyphens, 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.

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 1056](#).

3. In the **Comments** field, enter a description of the service. 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.

Specifying QoS Settings

If you have selected the **Enable QoS** check box in the selected service definition, you must configure QoS settings.

To configure QoS settings:

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 QoS Design software.

A QoS profile classifies traffic into defined service groups to provide special treatment of traffic across the network service.

2. In the **CIR** field, select the committed information rate (CIR) from the list.

The CIR is the guaranteed rate, which specifies the minimum bandwidth available if all sources are active at the same time. Make sure that the CIR value is less than the PIR value.

NOTE: For bursty traffic, the CIR represents the average rate of traffic per unit time and the PIR represents the maximum amount of traffic that can be transmitted in a given interval.

3. In the **PIR** field, select the peak information rate (PIR) from the list. The PIR is the shaping rate.

NOTE: If the QoS profile that you selected in Step 1 is configured with a level-three scheduler and interface oversubscription is enabled, then PIR is not used.

Entering VPN Settings and PE-CE Settings Information

This part of the create Layer 3 VPN full mesh Ethernet service order procedure sets VPN attributes that are usually common for all endpoints in the service. The values that you enter will 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.

VPN Settings

These settings from the selected Service Definition can be applied to all end points.

☐ Autopick UNID ID
UNIT ID: 13456

☐ Autopick VLAN ID
VLAN ID: 246

☐ Autopick Hub Route Target
☐ Autopick Spoke Route Target
Hub Route Target: 25:345
Spoke Route Target: 25:1024

☐ Autopick Hub Route Distinguisher
☐ Autopick Spoke Route Distinguisher
Hub Route distinguisher: 135.15.78.56:78
Spoke Route distinguisher: 25.15.78.56:45

☒ Autopick Interface IP Address
☒ VRF Table label
☒ Export Direct Routes

PE-CE Settings

Routing protocol: OSPF/Static Route
OSPF domain ID: 135.15.78.96

To set attributes common to most endpoints on a service:

1. 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.

2. Specify the **MTU Factor** or **Burst Period**, based on the **Calculate Burst Size** you have selected in the service definition.

NOTE: You cannot edit these fields if you have not selected the **Editable in Service Order** check box in the service definition.

3. Select the bandwidth from the **Bandwidth** list. The **Bandwidth Range** and **Bandwidth** fields appear only if you have cleared the **Enable QoS** check box in the selected service definition:

NOTE: You cannot edit these fields if you have not selected the **Editable in Service Order** check box in the service definition.

4.

NOTE: The fields specified in the Logical IF Settings box are based on the **Ethernet option** type. The Logical IF Settings box is not available if you have selected the **Ethernet option** as *Port*.

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.

5. Clear the **Autopick VLAN ID** check box if you want the **VLAN ID** chosen automatically by the Network Activate software. Select the check box to have the ID assigned manually.

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 VLAN ID:

1. Clear the **Autopick VLAN ID** check box. The screen expands to include the **VLAN ID** field.
 2. In the **VLAN ID** field, enter a value.
6. 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.

7.

8. Select the **Autopick Hub Route Distinguisher** and the **Autopick Spoke Route Distinguisher** check boxes if you want the Route distinguisher chosen automatically by the Network Activate software.

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.

9. 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 service order.

10. In the **PE-CE Settings** box, select the **Static Route** check box if you want to allow a service provisioner to create static routes on the service. Clear the **Static Route** check box to prevent a service provisioner from creating static routes on the service.

11. If **BGP routing protocol** is specified in the service definition, select the **AS override** check box 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.

If **OSPF routing protocol** is specified in the service definition, in the **OSPF domain ID** field, specify any valid IPV4 address in W.X.Y.Z "dot" notation.

12. Click **Next**.

The **Select Endpoint PE Devices** screen appears.

Selecting Endpoint PE Devices

You must select the endpoint PE devices that you want to participate in the service. See [“Selecting Endpoint PE Devices” on page 755](#).

Configuring Endpoint Settings

This part of the create multipoint Ethernet service order procedure selects the N-PE devices that will host the service endpoints. The selection is made from the **Select Endpoint PE Devices** screen.

NOTE: The **Select Endpoint PE Devices** screen 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 have L2VPN only will not appear.

3 Items Selected				
<input type="checkbox"/> Name ▲	Role	Additional Role	Management Address	Loopback Address
<input type="checkbox"/> embassy	N_PE	N/A	10.216.114.109	50.1.2.4
<input checked="" type="checkbox"/> junos-m10-1-space	N_PE	N/A	10.216.114.102	30.1.2.4
<input type="checkbox"/> junos-m10-2-space	N_PE	N/A	10.216.114.103	30.1.2.2
<input checked="" type="checkbox"/> junos-mx480-space	N_PE	N/A	10.216.114.100	30.1.2.6
<input type="checkbox"/> junos-mx80-1-space	N_PE	N/A	10.216.114.104	30.1.2.5
<input checked="" type="checkbox"/> junos-mx80-2-space	N_PE	N/A	10.216.114.105	30.1.2.3
<input type="checkbox"/> junos-space2	N_PE	CSR	10.216.114.120	30.1.2.8
<input type="checkbox"/> kochin	N_PE	N/A	10.216.114.110	50.1.2.1

To select endpoint N-PE devices: 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 756](#).

1. In the **Select Endpoint PE** devices screen, select the devices that you want to participate in the service. Use the multiple selection feature to select more than one device.

2. Click **Next**.

The **Endpoint Settings** screen appears.

Setting Attributes for UNI Endpoints

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 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 756](#).

This part of the create Ethernet service order procedure sets the attributes for each endpoint in the service. Selection is made using the Endpoint Settings screen.

The interface shown in the UNI Interface field is automatically selected by the Network Activate software, 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 screen shows the value for each UNI attribute.

The screenshot displays the 'Endpoint Settings' interface. On the left, a table lists endpoints under the 'Add Endpoints' section. The table has columns for 'Device', 'UNI Interface', 'Hub', and 'Action'. Two devices are listed: 'buxar' with UNI Interface 'xe-0/3/1' and 'cuttack' with UNI Interface 'ge-0/1/7'. Both have a red 'X' in the Hub column and a green '+' in the Action column.

The right panel shows the configuration for the selected device 'buxar'. It includes sections for 'Logical IF Settings' (Autopick UNIT ID, Autopick VLAN ID, Autopick interface IP, IP pool type, IP address pool, IP block size), 'Routing Protocol Settings' (Routing protocol, Autopick neighbor IP, Peer AS), and 'Qos Settings' (CIR, PIR, Mtu). The 'UNI interface' is set to 'xe-0/3/1'.

Device	UNI Interface	Hub	Action
Device: buxar (1 item)			
buxar	xe-0/3/1	X	+
Device: cuttack (1 item)			
cuttack	ge-0/1/7	X	+

Device: buxar

Stitching point: ☐
Set loopback: ☐
Ethernet option: Dot1Q
UNI interface: xe-0/3/1
UNI Description:
Hub: ☐

Logical IF Settings
Autopick UNIT ID: ☒
Autopick VLAN ID: ☒
Autopick interface IP: ☒
IP pool type: Global
IP address pool: 10.0.88.0/24
IP block size: 28

Routing Protocol Settings
Routing protocol: BGP
Autopick neighbor IP: ☒
Peer AS: 1

Qos Settings
CIR: 10000 Kbps
PIR: 10000 Kbps
Mtu: 1522

To configure or change the endpoint settings:

1. To add the loopback interface for a Layer 3 VPN service, select the **Set 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.

2. 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).

- **Flexible UNI**

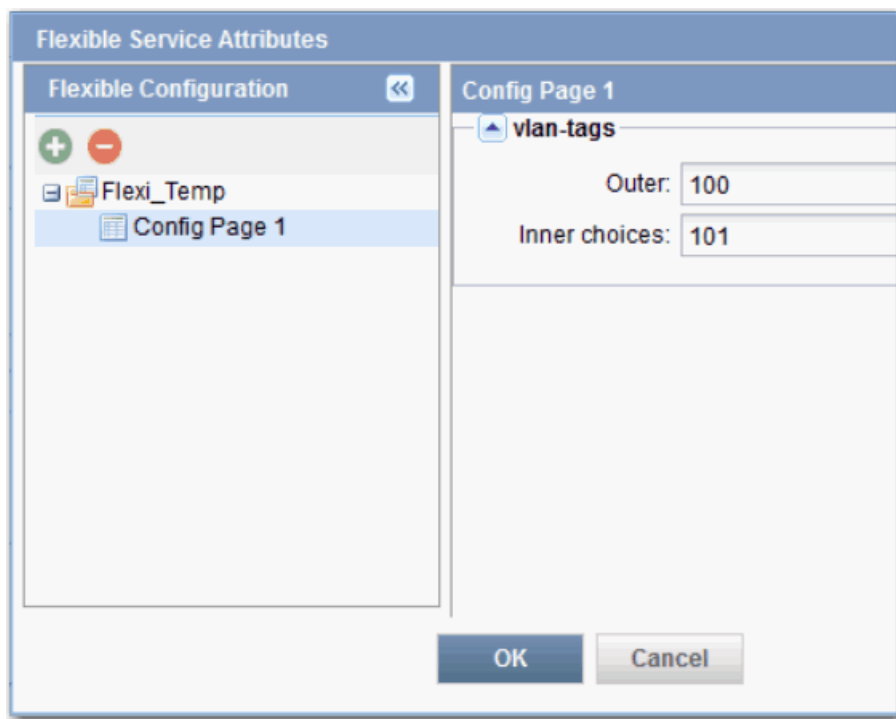
Specifying the **Flexible UNI** Ethernet option enables you to apply different values for the Unit ID and vlan-tags.

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.

See [“Creating a Service Template” on page 116](#)

When you create a service order based on a service definition with which a service template is associated, the Add Endpoints window includes a link labeled **Flexible Service Attributes**. If you click the link, the you can specify **Outer** and Inner **vlan-tags** in the **Flexible Service Attributes** window.



3. To select a different UNI on a device, click the **UNI interface** and choose another interface from the list.
4. 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

5. Specifying the Logical IF Settings:

NOTE: The fields specified in the Logical IF Settings box are based on the **Ethernet option** type. The Logical IF Settings box is not available if you have selected the **Ethernet option** as *Port*.

- If you have selected the **Ethernet option** as *Dot1Q*, or, *QinQ*, or *Flexible UNI*, 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: 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 **Ethernet option** 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 **Ethernet option** as *QinQ*, select the **Customer VLAN Type**.

If the **Customer VLAN type** is *Transport all traffic*, select the **Outer Tag Protocol ID**.

If the **Customer VLAN type** is *Transport single vlan*, select the **Customer VLAN**, **Inner Tag Protocol ID**, and **Outer Tag Protocol ID**.

NOTE: You can optionally specify **Inner Tag Protocol ID** and **Outer Tag Protocol ID**.

6. 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.

7. Select the **Routing protocol type**.

If the **Routing 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 **Routing protocol** type is **OSPF**, specify the following information:

- **OSPF area ID**--Specify any valid IPV4 address in W.X.Y.Z "dot" notation.

NOTE: The IPv4 address that you use must be valid addresses. Refer to <http://www.iana.org/assignments/ipv4-address-space> for the list of restricted IPv4 addresses.

- **OSPF version**--Select the OSPF version from the list.

8. If you have attached a service template in the service definition, the **Flexible Service Attributes** link appears. Click the link to modify the service template attributes. For more information about configuring the flexible service attributes, see "[Configuring Flexible Service Attributes to Modify Service Template Attributes](#)" on page 938.

9. If you have selected the **Enable QoS** check box in the service definition, specify the following fields:

- CIR
- PIR
- MTU(Bytes)
- QoS Profile

If you have cleared the **Enable QoS** check box in the service definition, specify the following fields:

- Bandwidth
- Default MTU

For more information about these fields, see "[Creating a Hub-and-Spoke \(One Interface\) Layer 3 VPN Service Definition](#)" on page 386.

10. When you have finished configuring the endpoint settings, click **Create**.

The Deployment Options window appears.

Adding, Deleting and Modifying Endpoints

You can add or delete UNI interfaces on the PE devices that participate in a service.

1. To add a UNI on a selected device, select the **Add UNI Interface** icon in the Actions column, and then select the interface you want from the UNI interface list.
2. If the interface you selected in the previous step is already configured (duplicate) you must either enter a different value in the VLAN ID field manually, or check the **Autopick VLAN ID** field.
3. To delete a UNI from a device, in the Actions column, click the **Delete UNI Interface** icon in the Actions column.

If the deleted UNI is the only UNI selected from the device, then the device is deleted from the service configuration.

4. To set or modify attributes for a UNI endpoint:
 - a. Select the row for the UNI endpoint that you want to modify.
A **UNI Settings** dialog box appears on the right side of the screen.
 - b. Modify the fields in right pane.
 - c. Select **Save** to apply the attributes to the UNI interface, or select **Add More** to save your changes and modify attributes for other UNI endpoints on the service.
5. When you have finished modifying the endpoint settings, click **Create**.

The **Deployment Options** window appears.

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**.

For more information on topology, see [“Junos Space Network Topology Overview” on page 31](#)

Deploying the New Service

This part of the create multipoint Ethernet service order procedure deploys the service.

To deploy the service, make selections from the **Deployment Options** window.

1. Perform one of these actions:

- To save the request without deploying the service, select **Save only** and then click **OK**.

See [“Deploying a Service Order” on page 631](#) for information about how to deploy a saved service at a later time.

- 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**.

The **Job ID** dialog box appears.

2. Click the **Job ID** link to monitor the status of the service deployment.

The **Deployment Service** job appears on the **Platform > Jobs > Job Management** inventory page.

3. You can also view the **Platform > Audit Logs > Audit Log** inventory page to view the Deploy Service Order username, user IP address, task, timestamp, description, and job ID.

The service order is now complete.

The **Manage Service Orders** inventory view shows the service order you just added. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details about the Jobs workspace.

Creating a Multicast VPN Service Order

This topic describes how to use the Network Activate application to create a Multicast VPN (MVPN) service order.

NOTE: Multicast VPN services are supported on LN2600, SRX 550/650, and MX devices only.

1. To select a service definition on which to base the new service order, in the Network Activate task pane, select **Service Provisioning > Manage Service Orders > Create L3VPN Service Order**.

Service Provisioning > Manage Service Orders > Create L3 VPN Service Order			
Actions ▾			
State	Name	Service Type	Created By
➔ Published	L3VPN-BGP-Static	L3 VPN (Full Mesh)	super
➔ Published	L3VPN-OSPF-Static	L3 VPN (Full Mesh)	super
➔ Published	L3VPN-OSPF-Static(Hub-Spoke-1-Interface)	L3 VPN (Hub-Spoke 1 Interface)	super
➔ Published	L3VPN-BGP-Static(Hub-Spoke-1-Interface)	L3 VPN (Hub-Spoke 1 Interface)	super
➔ Published	Multicat_test	L3 VPN (Full Mesh)	super

2. In the **Select Service Definition** window, select the service definition upon which you want to base your service order, then click **Next**.

Enter Order Information

General Settings

Service definition: Multicat_test

Name:

Customer:

Comments:

☒ MVPN

VPN Settings

These settings from the selected Service Definition can be applied to all end points.

☒ Autopick VLAN ID

☒ Autopick Route Target

☒ Autopick Route Distinguisher

☒ Autopick Interface IP Address

☒ VRF Table label

☒ Export Direct Routes

PE-CE Settings

Routing protocol: OSPF/Static Route

OSPF domain ID:

3. In the **Enter Order Information** window, enter 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.

Field	Description
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.

4. Click **Next**.

The screenshot shows a web interface for 'Service Provisioning > Manage Service Orders > Create L3 VPN Service Order'. It features a table with columns: Name, Role, Additional Role, Management Address, and Loopback Address. Two items, 'kochin' and 'jaipur', are selected. The interface also includes an 'Actions' dropdown and a search bar.

Name	Role	Additional Role	Management Address	Loopback Address
<input checked="" type="checkbox"/> kochin	N_PE	N/A	10.216.114.110	50.1.2.1
<input checked="" type="checkbox"/> jaipur	N_PE	N/A	10.216.114.112	50.1.2.2
<input type="checkbox"/> exora	N_PE	N/A	10.216.114.114	50.1.2.3
<input type="checkbox"/> embassy	N_PE	N/A	10.216.114.109	50.1.2.4

5. Select the device for which you want to implement the service order.

6. Click **Next**.

Endpoint Settings

Add Endpoints, Add/Delete UNI Interfaces and set values here.

Add Endpoints

Device	UNI Interface	Action
Device: fortius-f2100-b (1 Item)		MVPN Settings +
fortius-f2100-b	ge-1/2/1	✖
Device: junos-m10-1-space (1 Item)		MVPN Settings +
junos-m10-1-space		✖
Device: junos-mx240-space (1 Item)		MVPN Settings +
junos-mx240-space	lt-0/0/10	✖

Device: fortius-f2100-b

Save Add More

Stitching point: ☐

Set loopback: ☐

Ethernet option: VLAN

UNI interface: ge-1/2/1

UNI Description:

Autopick interface IP: ☒

IP pool type: Global

IP address pool: 10.0.88.0/24

IP block size: 28

Autopick VLAN ID: ☒

Routing Protocol Settings

Routing protocol: OSPF

OSPF area ID: 0.0.0.0

OSPF version: Ver 2

Create Cancel

7. In the **Endpoint Settings** window, enter information as described in the following table:

Field	Description
Add 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>
Ethernet option	<p>VLAN</p> <p>This field displays the value specified in the service definition upon which you are basing this service order.</p>

Field	Description
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	Global This field displays the value specified in the service definition upon which this service order is based.
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.
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.

8. Click **Create**.

RELATED DOCUMENTATION

[Creating a Full Mesh Layer 3 VPN Service Definition | 376](#)

[Multicast L3VPN Overview | 173](#)

[Creating a Multicast VPN Service Definition | 404](#)

Selecting a Published L3VPN Service Definition for a Service Order

To select a service definition on which to base the new service order:

1. In the **Network Activate** task pane, select **Service Provisioning > Manage Service Orders > Create L3 VPN Service Order**.

The **Select Service Definition** inventory page displays a view of only those published service definitions designed to work with Layer 3 VPN Ethernet services you need.

2. Select the service definition you want to base your service order on, then click **Next** to display the **Enter Order Information** window.

RELATED DOCUMENTATION

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 | 753](#)
2. [Entering VPN Settings Information | 754](#)
3. [Entering PE-CE Settings | 755](#)

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 1056](#).

You must specify the following general information about the service order in the General Settings box of the Enter Order Information 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 1056](#).

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 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. In the **VPN Settings** box, the **Apply to all** check box is selected by default. If the Apply to all option is selected, you enter the endpoint parameter values only once. If you clear the **Apply to all** check box and enter all the endpoint attributes individually later.
2. The **Autopick VLAN ID** option is automatically selected for Network Activate to automatically chose the VLAN ID. Deselect the check box if you want to manually assigned the VLAN ID.
The **VLAN ID** text box appears.
3. If you deselected the **Autopick VLAN ID** option, enter a value in the **VLAN ID** field.
4. The **Autopick Route Target** option is selected, and you cannot deselect it. Network Activate automatically selects the route target.
5. The **Autopick Route Distinguisher** option is selected, and you cannot deselect it.

6. The **Autopick Interface IP Address** option is selected, and you cannot deselect it. Network Activate automatically selects the interface IP address.
7. 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** box, 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.

1. Click **Next**.

The **Select Endpoint PE Devices** window appears.

Selecting Endpoint PE Devices

NOTE: The **Select Endpoint PE Devices** 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.

N-PE devices that are L2VPN-only will not appear.

To select endpoint N-PE devices:

1. In the **Select Endpoint PE Devices** inventory list, select the devices that you want to participate in the service. Use the multiple selection feature to select more than one device.
2. Click **Next** to display the **Endpoint Settings** page.

The

RELATED DOCUMENTATION

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 **Select Service Definition** page 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 586](#)
 - [Creating a Multipoint-to-Multipoint VPLS Service Order on page 660](#)
 - [Creating a Point-to-Multipoint VPLS Service Order on page 678](#)
 - [Creating a Full Mesh Layer 3 VPN Ethernet Service Order on page 718](#)
 - [Creating a Hub-and-Spoke Layer 3 VPN Service Order on page 733](#)
2. At the **Endpoint Settings** 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 586](#)).
3. Click **Flexible Service Attributes**.

The **Flexible Service Attributes** window opens. On the left, under **Flexible Configuration**, at the top level, are the names of the templates attached to the service definition. Each template contains at least one page, which appears below the name of the template. By default, such pages are called “Config Page 1.”

NOTE: We recommend you avoid using this default name: if multiple pages all share the same name, the template editor could save the page data wrongly.

Since template designers should group configuration options logically in pages, the designer can also name a page more usefully, for example, “UNI Description.”

4. (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.
5. 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.
6. For each page in each applicable template, make the appropriate changes in the field on the right.

7. (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.

8. 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

9. When you have finished configuring the current endpoint's group of flexible service attributes, click **OK**.

The Endpoint Settings page reappears.

10. (Optional) Repeat the preceding steps for other endpoints.

NOTE: Once a set of flexible service attributes has been deployed, it cannot be modified. However, you can modify that set of flexible service attributes to add a new endpoint if you modify the service (see, for example, ["Modifying a Point-to-Point Ethernet Service" on page 871](#) Find references to the other topics relevant to modifying under the rubric Related Documentation).

To verify your work:

1. Navigate to **Manage Services**, select the service you deployed, and select **View Service Configuration Change** either from the **Actions** drawer, or from the right mouse-click menu.

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

[Service Templates Overview | 113](#)

[Service Templates Workflow | 114](#)

[Creating a Service Template | 116](#)

[Specifying Service-Specific Values | 128](#)

[Modifying a Service Template | 127](#)

[Modifying a Multipoint-to-Multipoint Ethernet Service | 844](#)

[Modifying a Point-to-Multipoint Ethernet Service | 855](#)

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 **Deployment Options** window.

1. Perform one of these actions:

- To save the request without deploying the service, select **Save only** and then click **OK**.
See [“Deploying a Service Order” on page 631](#) for information about how to deploy a saved service at a later time.
- 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**.

The **Job ID** dialog box appears.

2. Click the **Job ID** link to monitor the status of the service deployment.

The **Deployment Service** job appears on the **Platform > Jobs > Job Management** inventory page.

3. You can also view the **Platform > Audit Logs > Audit Log** inventory page to view the Deploy Service Order username, user IP address, task, timestamp, description, and job ID.

RELATED DOCUMENTATION

[Creating a Full Mesh Layer 3 VPN Ethernet Service Order | 718](#)

[Creating a Hub-and-Spoke Layer 3 VPN Service Order | 733](#)

Creating a Cross Provisioning Platform Layer 3 VPN Service Order

The Cross Provisioning Platform(CPP) feature enables you to create an L3VPN service to operate across the platforms of different vendors.

Before creating the service, a service designer creates both a GUI script and a configuration script for the Juniper Networks device and for the device of the other vendor. The designer creates the GUI script using JavaScript and the Sencha Architecture tool to build the sequence of GUI windows to support the service creation procedure. The designer must also create a configuration script to define the configuration procedure.

To upload the GUI and configuration scripts, in the Network Activate task pane, select **Service Design > Manage Scripts**.

1. In the **Manage Scripts** window, click the **Add Script** icon (+) in the command bar.
2. In the **Add Script** window, type a name for the L3VPN script, select the **Vendor type**, and browse your local system for the **Configuration script** you want to add.
3. Click **Create**.

To create a CPP L3VPN service definition, in the Cross Provisioning Platform pane, select **CPP > Service Definitions**.

1. In the **CPP > Service Definitions** window, click the **Create CPP Service Definition** icon (+) in the command bar.

Create CPP Service Definition

General

Name: SD-L3VPN

ID: 10435

Type: L3VPN

Description:

Service Script Selections

Operation Type: Please Select

Select Scripts

Name	Vendor Type	Version
PD_BNG_Details_Script_JNPR	Juniper	1
PD_NPS_Details_Script_JNPR	Juniper	1
PD_VLAN-PATH_Details_Script_iPASO	Juniper	1
PD_Device_Details_Script_JNPR	Juniper	1
PD_P2P_LDP_Details_Script_ALU	Alcatel	1
PD_L3VPN_Details_Script_ALU	Alcatel	1
PD_BNG_Details_Script_ALU	Alcatel	1

Page 1 of 1

Displaying 1 - 47 of 47

Add Script

Selected Scripts

Name	Vendor Type	Operation Type	Action
PD_L3VPN_Details_Script_ALU	Alcatel	Modify	

Create

Cancel

2. In the **Create Service Definition** window, type a name for the service definition in the **Name** field.
3. In the **ID** field, type 1 through 2147483647 integers to identify the service definition by a unique value.

NOTE: The service definition ID is optional. If you do not provide any value in this field, the default value is -1. In the service definition selection grid, no value is displayed in the **ID** column. Each service definition is assigned a unique ID. If you give an existing ID value while creating a new service definition, exception occurs.

4. In the **Description** field, enter a description of the service definition to distinguish it from other service definitions.
5. In the **Type** field, select **L3VPN**.

6. Perform the following steps:

- In the **JUNOS Space Service Scripts** section:
 - a. From the **Select Junos Creation Script** column, select a Junos Space service script that was written for the creation of the service definition. The script that you selected is automatically populated in the corresponding **Creation** text field.
 - b. From the **Select Junos Modification Script** column, select a Junos Space service script that was written for the modification of the service definition. The script that you selected is automatically populated in the corresponding **Modification** text field.

NOTE: The Junos Space service scripts are mandatory to create a Layer 3 VPN service definition, whereas the SAM service scripts are optional.

- In the **SAM Service Scripts** section:
 - a. From the **Select SAM Creation Script** column, select a SAM service script that was written for the creation of the service definition. The script that you selected is automatically populated in the corresponding **Creation** text field.
 - b. From the **Select SAM Modification Script** column, select a SAM service script that was written for the modification of the service definition. The script that you selected is automatically populated in the corresponding **Modification** text field.

7. Click **Create**.

After the service definition is published, you can create the CPP L3VPN service order.

1. In the **Cross Provisioning Platform** task pane, select **CPP > Service Orders**.
2. In the **CPP Service Orders** window, click the **Create Service Order** icon (+) in the command bar.
3. In the **General Settings** section of **Create CPP Service Order**, select a service definition based on the unique ID, name or type.

NOTE: The value in the **ID** field is associated with a service definition. This identifier can be used when you are searching for a particular service definition while creating a device configlet order. You can search the service definition by its name, type or unique ID. You can modify the ID only during the migration of old service definition IDs.

4. In the **Description** field, enter a description of the service order to distinguish it from other service orders.

5. Click **Next**.

The **Create L3VPN Service** window appears, which the designer created specifically to support the configuration of the CPP L3VPN service order.

Create L3VPN Service

General

Name: SO13905766751

External ID: unique-new-service-name

Add Site

Site	Port	Action

Add Site/Interface Details

Site name: junos-m10-1-space

Port: ge-1/3/2

Vlan ID: 5

IP Address: /

View

Validate

Save

Create Clear Create More Cancel

6. Enter the endpoint information required to complete the service order.

NOTE: The CPP system automatically inserts a value in the **Name** field when you click **Next** in the preceding window.

In the **External ID** field, enter a unique text value to distinguish this service from all other services.

7. Click **Create**.

After you create a CPP L3VPN service order, you can view its details.

1. In the Network Activate task pane, select **CPP > Service Orders**.
2. In the **CPP Service Orders** window, double-click the listed service order for which you want to view the details.

The screenshot displays the 'CPP Service Details' window. The 'General' tab is active, showing the following information:

- Service name:** SO13909100463
- Description:**
- External Id:** AAAAA123
- Administrative state :** Deployed
- Service type:** L3VPN
- Service definition:** jun-jun-sd-l3

Below the General tab is a table listing devices:

Device Name	Device IP	Port	Int Status
jaipur	30.1.2.2	ge-0/0/3.829	↑ Up
junos-mx80-2...	30.1.2.3	ge-1/2/3.829	↑ Up

To the right of the device table is the 'Advanced Details For Device : jaipur' section. It has tabs for General, Protocols, Interface (selected), Firewall, Configuration, and SO Audit. The 'Interface' tab shows the following details:

Attribute	Value
Service name	SO13909100463
Description	L2E Manage Connected Devices -
Route distinguisher	69:1556889807
Import policy	SO13909100463_RP_MGMT_SPC
Export policy	SO13909100463_RP_MGMT_SPC

3. When you are finished viewing the service details, click **OK**.

RELATED DOCUMENTATION

[Adding Scripts Created for Cross Provisioning Platform | 775](#)

[Creating a Cross Provisioning Platform Service Definition | 305](#)

[Creating a Cross Provisioning Platform Service Order | 616](#)

Creating a Layer 3 VPN Service Order in Cross Provisioning Platform for Third-Party Devices

Cross Provisioning Platform is an extension of the Network Activate application within Junos Space, which provides a single pane of interaction to deploy services across vendor network devices. This topic discusses how Layer 3 VPN service order is created and deployed across third-party devices involved in Cross Provisioning Platform.

You need to create a Layer 3 VPN service definition before you create a Layer 3 VPN service order. Refer to [“Creating a Layer 3 VPN Service Definition in Cross Provisioning Platform for Third-Party Devices” on page 400](#) for information about how to create a Layer 3 VPN service definition.

To create a Layer 3 VPN service order:

1. From the **Cross Provisioning Platform** task pane, select **CPP > Service Orders**.

The **Service Orders** page that appears displays a list of the existing service orders.

2. Click the **Create CPP Service Order** icon above the tool grid.

The **Create CPP Service Order** page that appears contains the **General Settings** section.

3. In the **General Settings** section, perform the following steps:

- a. In the **Select Service Definition** section, select a service definition based on the unique ID, name or type.

NOTE: The value in the **ID** field is associated with a service definition. This identifier can be used when you are searching for a particular service definition while creating a device configlet order. You can search the service definition by its name, type or unique ID. You can modify the ID only during the migration of old service definition IDs.

CPP > Service Orders > Create CPP Service Order

Create CPP Service Order

General Settings

Select Service Definition

ID	Name	Type
	VPLS_SD	VPLS
	P2P_SD	PW-LDP
5678	Test_SD_123	PW-LDP
1234	Test_123_P2P	PW-LDP
4321	Test_123_VPLS	VPLS
7654	Test_SD_L3VPN	L3VPN
	L3VPN-SD	L3VPN

Page 1 of 1 | Displaying 1 - 7 of 7 | Show 30 items

Description:

Next Cancel

- b. In the **Order description** field, type 3 through 256 alphanumeric characters to describe the service order.

4. Click **Next**.

The **Create L3VPN Service** page that appears contains the **General** , **RD/RT**, **MVPN Settings**, **Step:1 Select Site**, **Step:2 Select Site Interface**, and **Step:3 Enter Staged Interface Details** sections.

Create L3VPN Service

General

Name: SO266585383

External ID:

Customer ID: [View](#)

RD/RT

Manual RT/RD ? : ☒

RD:

RT:

MVPN Settings

Enable MVPN: ☐

Step1: Select Site Vendor: **Juniper**

Site Name	Loopback	Vendor
buxar	30.1.37.1	Juniper
fortius-f2100-a	30.1.2.13	Juniper
fortius-f2100-b	30.1.2.14	Juniper
junos-mx240-space	30.1.2.1	Juniper
junos-mx80-2-space	30.1.2.3	Juniper

Page 1 of 1 | Displaying 1 - 5 of 5

Step2: Select Site Interface

Site Name	Port	Encapsulation	Speed	Status
-----------	------	---------------	-------	--------

Page 0 of 0 | No results

[Add to Staged Interfaces](#)

Step3: Enter Staged Interface Details

Site Name	Port	Ethernet Option	VLAN ID	Validate VLAN	IP Address	Subnet	Settings	Action
-----------	------	-----------------	---------	---------------	------------	--------	----------	--------

Page 0 of 0 | No results

[Create](#) [Clear](#) [Create More](#) [Cancel](#)

5. On the **Create L3VPN Service** page, perform the following steps:

- In the **General** section:

The **Name** field is filled by default with the name of the service order.

- In the **External ID** field, type 3 through 128 alphanumeric characters to specify the external ID.
- In the **Customer ID** section, click **View** to view and select a customer ID from the list of customer IDs.

- In the **RD/RT** section:

- Select the **Manual RT/RD** check box to enter the route target (RT) and route distinguisher (RD) values manually.
 - From the **RD** spin box, select any value.

b. From the **RT** spin box, select any value.

- In the **MVPN Settings** section:
 - Select the **Enable MVPN** check box to enable multicast VPN (MVPN) settings.
- In the **Step:1 Select Site** section:
 - Select any site from the list of available sites.

The site interfaces for the selected site automatically appear in the **Step:2 Select Site Interface** section.

- In the **Step:2 Select Site Interface** section:
 - Select one or more site interfaces from the list of available site interfaces.
- Click **Add to Staged Interfaces**.

The site interfaces that you selected are added to the staged interfaces and appear in the **Step:3 Enter Staged Interface Details** section.

- In the **Step:3 Enter Staged Interface Details** section, perform the following steps for all staged interfaces:

The **Site Name** and **Port** fields are automatically populated as soon as you add the site interfaces to the staged interfaces. Because the validation of VLAN is also done automatically, the **Validate VLAN** field is also filled.

- a. From the **Ethernet Option** spin box, select any Ethernet switching option.
- b. From the **VLAN ID** spin box, select any VLAN ID.
- c. Select the **IP Address** field to enter the corresponding IP address of the staged interface.
- d. Select the **Subnet** field to enter the subnet range.
- e. Select the **Settings** field to access the **Advanced Settings** page.

NOTE: The **Advanced Settings** page contains the routing protocol and L2 extension field sets that are UNI specific. If you select the **MVPN** check box, you can view and edit the MVPN settings. You can add or remove a UNI interface in the **Action** column. The option to delete the previously added sites is also offered in the **Action** column.

6. Click **Create**.

The **Job Details** dialog box that appears displays the job ID. You can click the **Job ID** link to view the job details.

NOTE: Click **Create More** to further modify the service order settings. The details that you provide on the **Create L3VPN Service** page determine which fields are displayed to help you further modify the service order settings.

RELATED DOCUMENTATION

| [Creating a Layer 3 VPN Service Definition in Cross Provisioning Platform for Third-Party Devices](#) | 400

21

CHAPTER

Service Types

[Managing Service Types in Cross Provisioning Platform | 771](#)

[Creating Service Types in Cross Provisioning Platform | 771](#)

[Modifying a Service Type in Cross Provisioning Platform | 772](#)

[Deleting a Service Type in Cross Provisioning Platform | 773](#)

Managing Service Types in Cross Provisioning Platform

The Service Types inventory page displays table of predefined and customized Cross Provisional Platform service types. The Service Types page displays information in a table categorized by service type name, whether the service type is predefined or customized, creation date, and troubleshooting context path. To view more detailed information about the service type double-click the service type.

You can perform the following actions on the Service Types inventory page:

- **Create Service Types**—See [“Creating Service Types in Cross Provisioning Platform” on page 771.](#)
- **Modify Service Types**—See [“Modifying a Service Type in Cross Provisioning Platform” on page 772.](#)
- **Delete Service Types**—See [“Deleting a Service Type in Cross Provisioning Platform” on page 773.](#)
- **Tag It**—See *Tagging an Object*.
- **View Tags**—See *Managing Tags*.
- **Untag It**—See *Untagging Objects*.

Creating Service Types in Cross Provisioning Platform

To create a service type:

1. In the **Cross Provisioning Platform** task pane, select **CPP > Service Types**.

The Service Type landing page appears.

2. Click the + button to create a service type.

The Create Service Type window appears.

3. Specify the information in the Create Service Type window using the following table as an aid:

Parameter	Description
Service Type	Enter a name for the service type.

Parameter	Description
Troubleshooting Context Path	Specify the context path for a script. Troubleshooting context path is an XPATH expression specific to service types to retrieve the service-related information. The context path is used while fetching service-related information from device configuration and while executing OP scripts.
Available Scripts	Based on the vendor type, select the scripts from the list.
Selected Scripts	Lists the script that you have selected from Available Scripts

4. Click **Create**.

The data that you have specified for a service type is stored in the database. This data is retrieved when you click an endpoint on the **View Service Details > Advance Details** tab.

Modifying a Service Type in Cross Provisioning Platform

To modify a service type:

1. Select **CPP > Service Types**.

The Service Types page appears.

2. On the Service Types page, select and right-click the service type that you want to modify.

NOTE: You can modify both predefined and customized service types.

3. Select **Modify Service Type**.

The Modify CPP Service Type page appears.

4. (Optional) You can modify the following fields in the **Modify CPP Service Type** dialog box:

- Troubleshooting Context Path

- Available Scripts
- Selected Scripts

5. Click **Modify**.

The selected service type is modified.

Deleting a Service Type in Cross Provisioning Platform

To delete a service type:

1. Select **CPP > Service Types**.

The Service Types page appears.

2. On the Service Types page, select and right-click the service type that you want to delete.

NOTE: You cannot delete a service type, if:

- The service type is a predefined service type.
- The service type is associated with a service definition.

3. Select **Delete Service Type**.

The Delete Service Type page appears.

4. Select the service type and click **Delete**.

The service type is removed from the database.

The **Manage Service Types** page appears, displaying the remaining service types.

22

CHAPTER

Scripts

[Adding Scripts Created for Cross Provisioning Platform | 775](#)

[Exporting Scripts Created for Cross Provisioning Platform | 776](#)

[Importing Scripts Created for Cross Provisioning Platform | 778](#)

[Modifying Scripts Created for Cross Provisioning Platform | 779](#)

[Viewing Scripts Created for Cross Provisioning Platform | 781](#)

[Predefined Scripts for Cross Provisioning Platform | 784](#)

[Viewing Script Version Support for Cross Provisioning Platform | 787](#)

[Debugging a Cross Provisioning Platform Script | 789](#)

Adding Scripts Created for Cross Provisioning Platform

Before you can create a Cross Provisioning Platform service definition, you must add scripts to the system that enable management of the Juniper Networks devices and the devices of another vendor.

To enable cross provisioning platform, you add three types of scripts:

- **GUI Script**—Provides the code that renders the Cross Provisioning Platform GUI window required for provisioning a Juniper Networks device.
- **Junos Configuration Script**—Provides the code that enables provisioning a particular Juniper Networks device.
- **Nokia or Canoga Configuration Script**—Provides the code that enables provisioning the device of another vendor.

To view the scripts that have been loaded into the system:

1. In the Cross Provisioning Platform task pane, select **CPP > Scripts**.
2. In the **Scripts** window, select the **Add Scripts** icon on the command bar (+).
3. In the **Add Script(s)** window, select a feature type and its corresponding vendor type from a list of features in the **Feature Type** drop-down list. These features require scripts in the cross provisioning platform.
4. In the **Add Script(s)** window, you can browse your local client file system for the scripts you want to be available to the Cross Provisioning Platform application. You can add scripts for Juniper Networks devices and for the devices of other vendors. If you select **Alcatel** or **Canoga** in the **Vendor type** field, the window displays fields for selecting both **Configuration script** and **GUI script**.

NOTE: If you want to do service interface migration, you need to upload both **Configuration script** and the **GUI script**.

If you select a third-party in the **Vendor type** field, the window displays a field for selecting a **Configuration script** only.

NOTE: If you access the server on which the Junos Space software is installed as a remote client, you must copy the scripts you intend to add to the CPP system to your local client file system. That is, when you click on **Browse** to select a script, which you want to add, Junos Space opens the local client file system, not the file system of the server on which Junos Space is installed.

5. Click **Create**.

The script is added to the CPP application.

RELATED DOCUMENTATION

[Importing Scripts Created for Cross Provisioning Platform | 778](#)

[Modifying Scripts Created for Cross Provisioning Platform | 779](#)

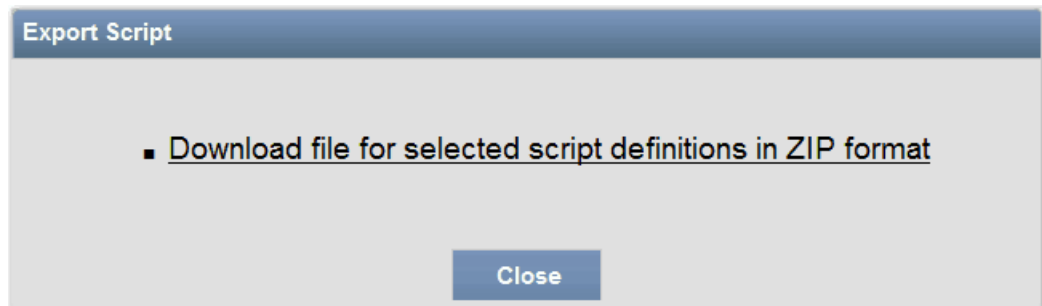
[Exporting Scripts Created for Cross Provisioning Platform | 776](#)

[Viewing Scripts Created for Cross Provisioning Platform | 781](#)

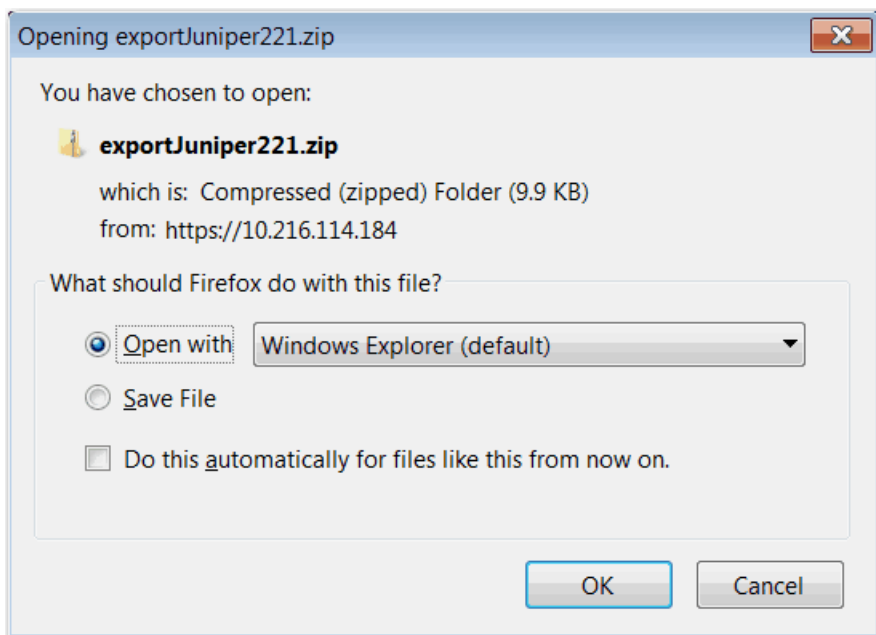
Exporting Scripts Created for Cross Provisioning Platform

To export scripts created for cross provisioning platform:

1. In the Cross Provisioning Platform task pane, select **CPP > Scripts**.
2. In the **Scripts** inventory page, select the script that you want to export and click the **Export Script** icon in the command bar.



3. In the **Export Script** window, click the link that enables you to bundle scripts into a ZIP file for exporting to a local file system.



4. In the **Open exportscript_name.zip** window, browse to the location in the local file system to which you want to export the script bundle.
5. Click **OK**.

RELATED DOCUMENTATION

[Importing Scripts Created for Cross Provisioning Platform | 778](#)

[Modifying Scripts Created for Cross Provisioning Platform | 779](#)

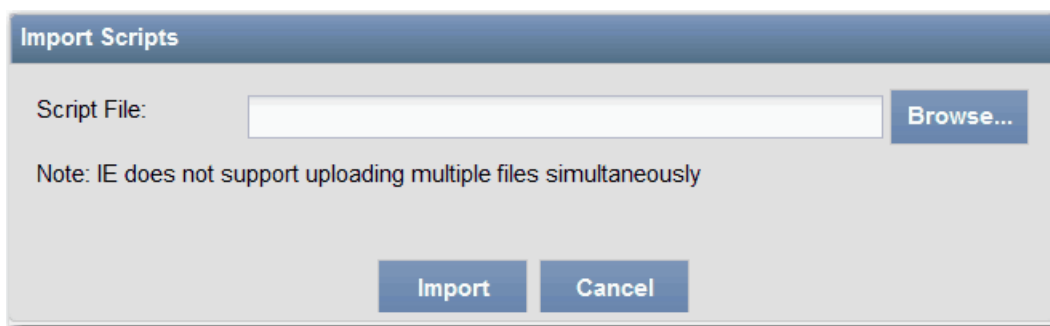
[Adding Scripts Created for Cross Provisioning Platform | 775](#)

[Viewing Scripts Created for Cross Provisioning Platform | 781](#)

Importing Scripts Created for Cross Provisioning Platform

To import scripts created for cross provisioning platform:

1. In the Cross Provisioning Platform task pane, select **CPP > Scripts**.
2. In the **Scripts** inventory page, click the **Import Script** icon in the command bar.



3. In the **Import Scripts** window, browse the local file system to locate the script you want to import into the CPP system.
4. Click **Import**.

The imported script is displayed in the **Manage Scripts** window.

NOTE: The IE browser enables importing only a single script at time.

RELATED DOCUMENTATION

[Exporting Scripts Created for Cross Provisioning Platform | 776](#)

[Modifying Scripts Created for Cross Provisioning Platform | 779](#)

[Adding Scripts Created for Cross Provisioning Platform | 775](#)

[Viewing Scripts Created for Cross Provisioning Platform | 781](#)

Modifying Scripts Created for Cross Provisioning Platform

The Cross Provisioning Platform application allows you to modify an existing script.

To modify an existing configuration or GUI script:

1. In the Cross Provisioning Platform task pane, select **CPP > Scripts**.

The **Scripts** inventory page appears.

2. Select a script from the list of displayed scripts and click the **Modify Script** icon in the command bar.

The Modify Script window appears.

CPP > Scripts > Modify Script

Modify Script(s)

Name: Script221-Junos-ADD

Description:

Version: 7

Vendor Type: Junos Space

Configuration Script | GUI Script

Configuration script:

```
<?xml version='1.0' ?>
<!--
*****
221-NGCE-EI-BURSTABLE JNPR XSLT    > Support: Jag Channa & Eric Novinscak
> Company: Juniper Networks
> Contact: jchanna@juniper.net & enovinscak@juniper.net
> Version: 0.2
> Revision Date: 2013-10-25
*****
-->

<xsl:stylesheet version="2.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
xmlns:ns2="http://provisioning.jmp.juniper.net/servicerequest/dto"
xmlns:ResourceMap="java:net.juniper.jmp.provisioning.scriptUtil.ResourceMap"
xmlns:ServiceActivationUtils="java:net.juniper.jmp.provisioning.scriptUtil.ServiceActivationUtils"
exclude-result-prefixes="http://provisioning.jmp.juniper.net/servicerequest/dto"
>
```

Note: Changes made to the script contents will be saved as a new version

3. In the **Modify Script** window, modify the script by performing one of the following tasks:
 - Browse the local file system to upload the script that you have modified in your local file system.
 - Modify the script directly in the text area.

The fields in the Modify Script window are described in [Table 33 on page 780](#).

Table 33: Fields in the Modify Script Window

Field	Description
Name	The Name field displays the name of the selected script.
Description	If you have entered a description while creating a script, the Description field displays the description of the selected script.
Version	<p>The Version list displays the latest version number of the script. You can select the preferred version from the list. For more information about the script version, see “Viewing Script Version Support for Cross Provisioning Platform” on page 787.</p> <p>NOTE: By default, the latest version of the script is populated in the text area.</p>
Vendor Type	<p>The Vendor Type field displays the name of the vendor.</p> <ul style="list-style-type: none"> • Junos Space • Alcatel SAM
Configuration Script	<p>On clicking the Configuration Script tab, you can browse and upload the configuration script from your local file system. After uploading the configuration script from your local file system, the newly uploaded script is displayed in the text area.</p> <p>If you prefer to make changes to the existing configuration script, the Cross Provisioning Platform application provides you with the option to modify the configuration script directly in the text area.</p>
GUI Script	<p>On clicking the GUI Script tab, you can browse and upload the GUI script from your local file system. After uploading the GUI script from your local file system, the newly uploaded script is displayed in the text area.</p> <p>If you prefer to make changes to the existing configuration script, the Cross Provisioning Platform application provides you with the option to modify the configuration script directly in the text area.</p> <p>NOTE: If the vendor type is <i>Alcatel SAM</i>, the GUI Script tab is not displayed.</p>
Save	To save the changes, click Save .
Preview	To preview the changes, click Preview . You can preview the GUI script output before creating a service.
Cancel	To discard the changes, click Cancel .

4. Click **Save**.

The system modifies the script and updates the version number.

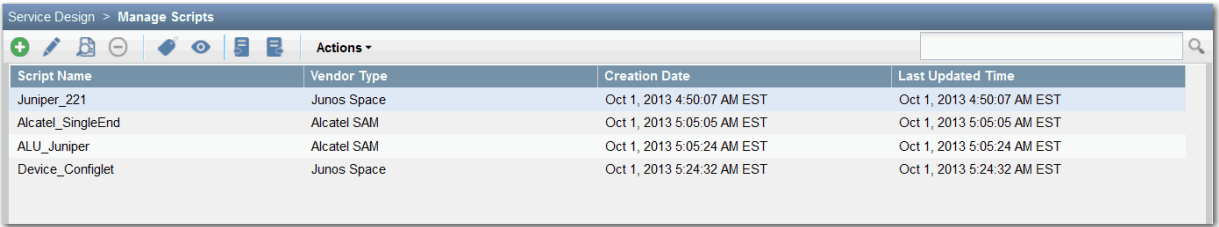
RELATED DOCUMENTATION

Importing Scripts Created for Cross Provisioning Platform 778
Exporting Scripts Created for Cross Provisioning Platform 776
Adding Scripts Created for Cross Provisioning Platform 775
Viewing Scripts Created for Cross Provisioning Platform 781
Debugging a Cross Provisioning Platform Script 789

Viewing Scripts Created for Cross Provisioning Platform

To view the details of the scripts added to the system to enabled cross provisioning platform:

1. In the Cross Provisioning Platform task pane, select **CPP > Scripts**.



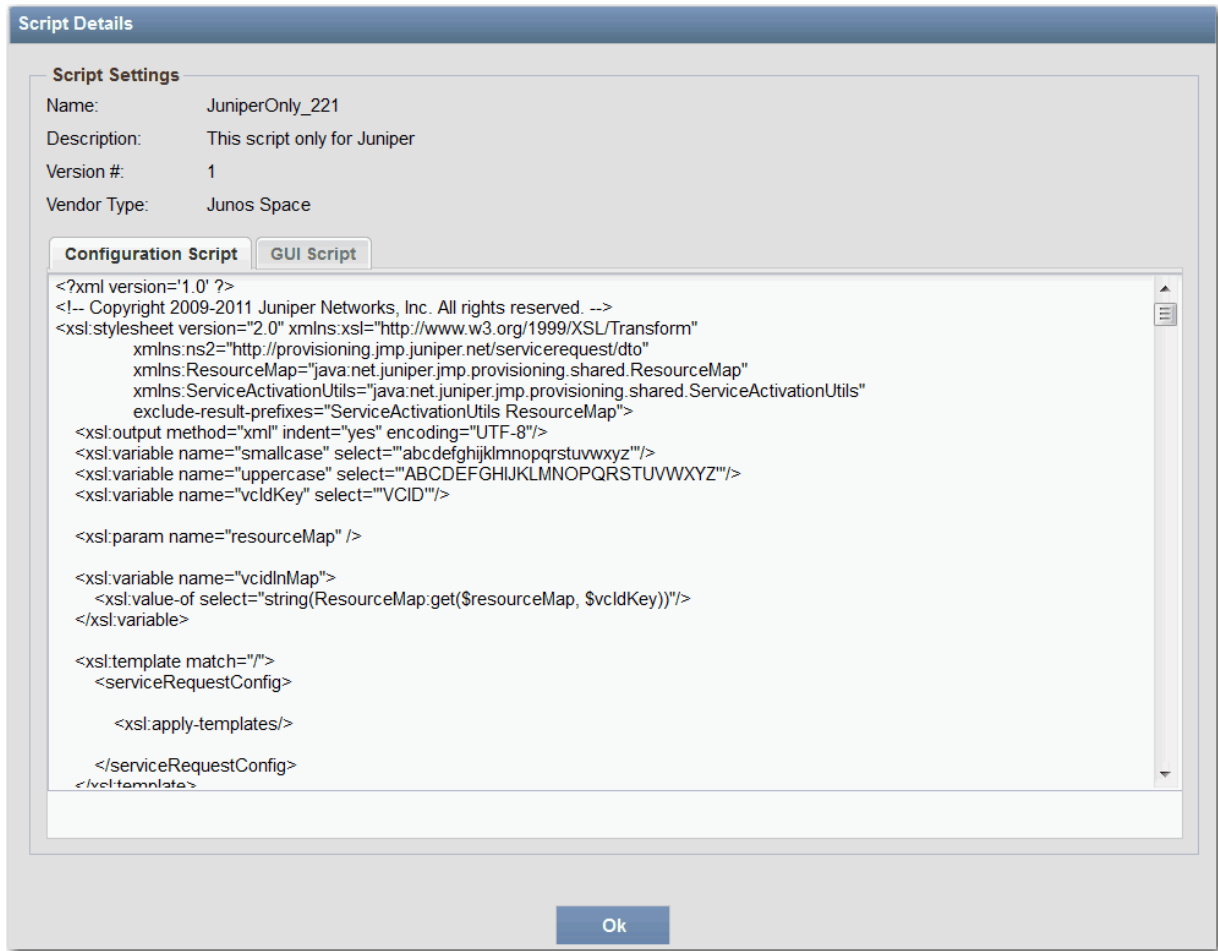
Script Name	Vendor Type	Creation Date	Last Updated Time
Juniper_221	Junos Space	Oct 1, 2013 4:50:07 AM EST	Oct 1, 2013 4:50:07 AM EST
Alcatel_SingleEnd	Alcatel SAM	Oct 1, 2013 5:05:05 AM EST	Oct 1, 2013 5:05:05 AM EST
ALU_Juniper	Alcatel SAM	Oct 1, 2013 5:05:24 AM EST	Oct 1, 2013 5:05:24 AM EST
Device_Configlet	Junos Space	Oct 1, 2013 5:24:32 AM EST	Oct 1, 2013 5:24:32 AM EST

2. In the **Scripts** inventory page, double-click the script for which you want to view its details.

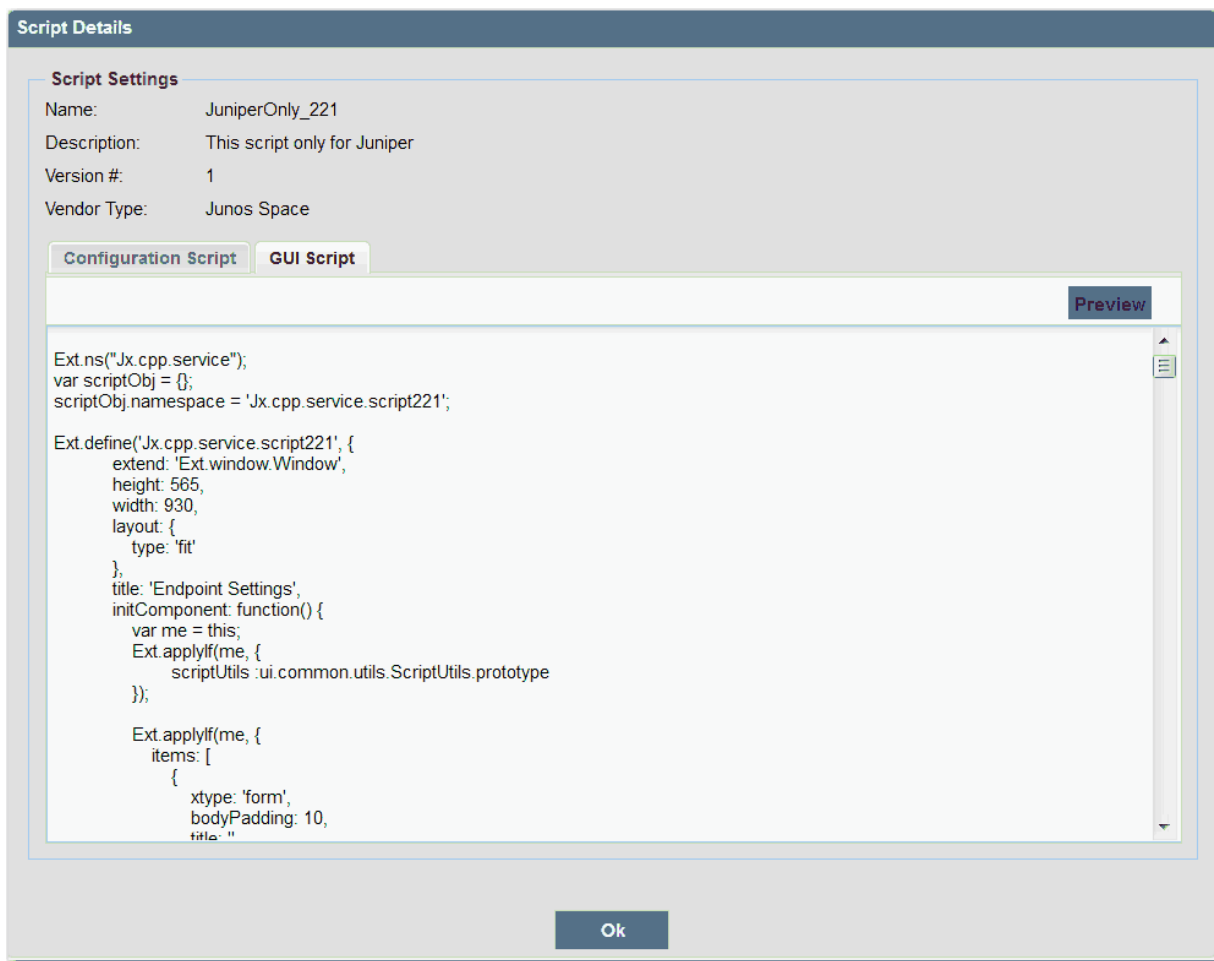
The **Script Details** window displays a **Configuration Script** tab and a **GUI Script** tab.

The **Configuration Script** tab displays the script for the particular Juniper Networks device.

NOTE: If you select a script that was created for managing the device of another vendor, the **Script Details** window displays the **Configuration Script** tab only.



3. Click the **GUI Script** tab to display the code that generates the GUI window for configuring the associated Juniper Networks device.



4. Click **Preview** to display the **Endpoint Settings** window that is generated by the GUI script.

RELATED DOCUMENTATION

Importing Scripts Created for Cross Provisioning Platform 778
Modifying Scripts Created for Cross Provisioning Platform 779
Exporting Scripts Created for Cross Provisioning Platform 776
Adding Scripts Created for Cross Provisioning Platform 775

Predefined Scripts for Cross Provisioning Platform

IN THIS SECTION

- [Predefined Service Scripts | 785](#)
- [Predefined Feature Scripts | 786](#)
- [Predefined Troubleshooting Scripts | 787](#)

Cross Provisioning Platform provides predefined scripts that a service provisioner can use while creating a service. There are two types of scripts:

- GUI Script

In the Junos Space CPP context, the GUI script generates the user interface for interacting with the Cross Provisioning Platform service. The GUI defines the parameters for which a user specifies values. The GUI can define hidden fields and values that are passed to the server. The GUI also guides a user to enter valid values for the parameters to define a service order. In addition, the GUI script can provide some client-side validation.

- Flex scripts or Configuration scripts

The Juniper Networks XSLT Flex script derives input variables from the ServiceRequest.xml document, which is created from data a user inputs into the Junos Space CPP GUI, and generates JUNOS XML configuration that is passed to the intended Juniper Networks device. An XSLT Flex script for a Juniper device has two major components:

- Derivations Logic—In this section, input variables are extracted and additional parameters are derived.
- Configuration Logic—In this section, parameters derived from the derivation logic are used to construct the XML configuration that activates the service on a Juniper Networks device.

The Cross Provisioning Platform application provides predefined scripts based on the service type, feature type, and for troubleshooting. The following sections list these predefined scripts:

Predefined Service Scripts

Table 34 on page 785 describes the predefined scripts based on the service type.

Table 34: List of Predefined Scripts Based on Service Type

Service Type	Vendor	Configuration Script		GUI Script
		Script to CREATE Service	Script to Modify Service	
LDP-based Point-to-Point service	Juniper Networks	PD_P2P_LDP_Create_Script_JNPR	PD_P2P_LDP_Modify_Script_JNPR	PD_P2P_LDP_Modify_Script_JNPR
LDP-based Point-to-Point service	Alcatel-Lucent	PD_P2P_LDP_Create_Script_ALU	PD_P2P_LDP_Modify_Script_ALU	PD_P2P_LDP_Modify_Script_ALU

Table 34: List of Predefined Scripts Based on Service Type (continued)

Service Type	Vendor	Configuration Script		GUI Script
		Script to CREATE Service	Script to Modify Service	
BGP-based Point-to-Point service	Juniper Networks	PD_P2P_BGP_Create_Script_JNPR	PD_P2P_BGP_Modify_Script_JNPR	PD_P2P_BGP_Modify_Script_JNPR
L3VPN service	Juniper Networks	PD_L3VPN_Create_Script_JNPR	PD_L3VPN_Modify_Script_JNPR	PD_L3VPN_Modify_Script_JNPR
L3VPN service	Alcatel-Lucent	PD_L3VPN_Create_Script_ALU	PD_L3VPN_Modify_Script_ALU	PD_L3VPN_Modify_Script_ALU
VPLS service	Juniper Networks	PD_VPLS_Create_Script_JNPR	PD_VPLS_Modify_Script_JNPR	PD_VPLS_Modify_Script_JNPR
Device Configlet service	Juniper Networks	PD_Device_Turn_Up_Create_Script_JNPR	PD_Device_Turn_Up_Modify_Script_JNPR	PD_Device_Turn_Up_Modify_Script_JNPR

Predefined Feature Scripts

Table 35 on page 786 describes the predefined scripts based on the feature type.

Table 35: List of Predefined Scripts Based on Feature Type

Feature Type	Vendor	Configuration Script	GUI Script
Bulk Service Modify Interface Migration	Juniper Networks	PD_Bulk_Service_Modify_Script_JNPR	PD_Bulk_Service_Modify_Script_JNPR
Bulk Device Modify	Juniper Networks	PD_Bulk_Device_Modify_Script_JNPR	PD_Bulk_Device_Modify_Script_JNPR
Interface Migration	Juniper Networks	PD_Interface_Migration_Script_JNPR	PD_Interface_Migration_Script_JNPR
Interface Migration	Alcatel-Lucent	PD_Interface_Migration_Script_ALU	PD_Interface_Migration_Script_JNPR

Predefined Troubleshooting Scripts

Table 36 on page 787 describes the troubleshooting scripts.

Table 36: List of Predefined Scripts Based for Troubleshooting

Service Type	Troubleshooting Script
LDP-based Point-to-Point service	P2PLDPPredefinedScript
BGP-based Point-to-Point service	P2PBGPPredefinedScript
L3VPN service	L3VPNPredefinedScript
VPLS service	VPLSPredefinedScript

RELATED DOCUMENTATION

[Adding Scripts Created for Cross Provisioning Platform | 775](#)

[Exporting Scripts Created for Cross Provisioning Platform | 776](#)

[Importing Scripts Created for Cross Provisioning Platform | 778](#)

[Modifying Scripts Created for Cross Provisioning Platform | 779](#)

[Viewing Scripts Created for Cross Provisioning Platform | 781](#)

Viewing Script Version Support for Cross Provisioning Platform

The script version support in Cross Provisioning Platform enables you to view the older versions of the script and set the preferred version to active while creating the service order.

To view script version support for Cross Provisioning Platform:

1. From the **Cross Provisioning Platform** task pane, select **CPP > Scripts**.

The page that appears displays a list of the existing scripts.

2. Double-click any script from the list of the existing scripts.

The **Script Details** page that appears provides information on the script that you selected. You can also click the **View Script** icon above the tool grid to view the **Script Details** page.

3. From the **Version#** drop-down list, select the preferred version.

CPP > Scripts > View Script

Script Details

Script Settings

Name: ALU_Modify_L3VPN

Description:

Version #: 12 Set as default

Vendor Type: Alcatel SAM

Configuration Script

```
<?xml version="1.0"?>
<!--
*****
9999-NGCE-EI-BURSTABLE ALU XSLT TRANSFORMATION SCRIPT
*****
-->
<xsl:stylesheet version="2.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
xmlns:ns2="http://provisioning.jmp.juniper.net/servicerequest/dto" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ServiceActivationUtils="java:net.juniper.jmp.provisioning.scriptUtil.ServiceActivationUtils"
xmlns:OSSClient="java:net.juniper.jmp.external.oss.sam.inventory.SAMOSSMediator" exclude-result-
prefixes="ServiceActivationUtils OSSClient xsl xs">
  <xsl:output method="xml" version="1.0" encoding="UTF-8" indent="yes" omit-xml-declaration="yes"/>
  <xsl:template match="/">
    <!-- TOP-LEVEL DERIVATIONS - BEGIN -->
    <xsl:variable name="client" select="OSSClientnew()"/>
    <xsl:variable name="serviceDefinitionName" select="/ns2:ServiceRequest/Policy/Name"/>
    <xsl:variable name="serviceOrderName" select="/ns2:ServiceRequest/Name"/>
    <xsl:variable name="serviceOrderDescription" select="/ns2:ServiceRequest/Description"/>
    <xsl:variable name="serviceOrderExtRef" select="/ns2:ServiceRequest/ExtRef"/>
    <xsl:variable name="userId" select="/ns2:ServiceRequest/Createdby"/>
    <xsl:variable name="customerName" select="/ns2:ServiceRequest/Customer"/>
    <xsl:variable name="subscriberPointer">
      <xsl:choose>
        <xsl:when test="not($customerName) and $customerName != "">
```

Ok

4. Click **Set as default** to set the selected version as default.

A confirmation dialog box that appears asks you to confirm the selection.

5. Click **OK**.

A dialog box that appears confirms the selection of the new version of the script.

NOTE: If a service definition has already been created with a particular version, the script contents of the service order will point to the same version.

On the **Script Details** page, you can see a list of script versions on the drop-down list, from which you can select a version to view its contents and set it as the active version. Internally, a new version is created, pointing to the selected older version and the same version contents are effective while creating the Cross Provisioning Platform service order.

For example, if you change the version number from 3 to 2 and set it as the active version, a new version number 4 is created internally, pointing to the contents of version 2 and making this the active version.

After you set the script version, you are redirected to the landing page of **Scripts**.

RELATED DOCUMENTATION

[Viewing Scripts Created for Cross Provisioning Platform | 781](#)

[Creating a Cross Provisioning Platform Service Definition | 305](#)

Debugging a Cross Provisioning Platform Script

IN THIS SECTION

- [Modifying a Cross Provisioning Platform Script | 790](#)
- [Previewing a Cross Provisioning Platform Script | 790](#)
- [Verifying a Cross Provisioning Platform Script | 791](#)

In releases prior to Cross Provisioning Platform Release 14.3R1, you can identify script-related issues only after you create a service. You cannot preview the XML configuration that is being pushed to the device.

With Cross Provisioning Platform Release 14.3R1, you can debug both the configuration script and the GUI script while you are still creating a service. This enables you to identify and rectify all script-related issues before you create a service. You can debug both Juniper Networks and Nokia scripts.

You can debug a Cross Provisioning Platform script by performing the following tasks:

Modifying a Cross Provisioning Platform Script

In releases prior to Cross Provisioning Platform Release 14.3R1, you need to upload the modified script from your local file system. In Cross Provisioning Platform Release 14.3R1, you can modify the script directly in the text area included in the Modify Script window. By default, the latest version of the script is populated in the text area.

To modify a Cross Provisioning Platform script, perform one of the following tasks:

- Browse the local file system to upload the script that you have modified in your local file system.

The uploaded script is displayed in the text area, included in the Modify Script window.

- Modify the script directly in the text area.

NOTE: In the text area in the Modify Script window, you can also modify the script that you have uploaded from your local file system. For more information about modifying an existing script, see [“Modifying Scripts Created for Cross Provisioning Platform” on page 779](#).

Use the **Preview** option in the Modify Script window to preview the script output. In the script output, use the **Verify** option to verify the script output.

Previewing a Cross Provisioning Platform Script

With Cross Provisioning Platform Release 14.3R1, you can preview the script output before you create a service.

To preview the output of a GUI script, perform one of the following tasks:

- On the **Scripts** inventory page, right-click a script and select **Preview**.
- In the Modify Script window, click the **Preview** option.

Verifying a Cross Provisioning Platform Script

Verify the script output to identify and troubleshoot issues, if any. The Cross Provisioning Platform application provides you with the option to specify real-time data while you preview the script output.

To verify the Cross Provisioning Platform script output:

1. In the Modify Script window, click the **Preview** option.

You can preview the script output.

2. In the script output window, specify real-time data.
3. Click **Verify**.

NOTE: For the **Verify** option to appear in the script output window and to generate the required XML output, you must append the GUI script with the newly created script utility function, `scriptUtils.verifyForm(this,data)`.

Following is the code snippet to add the **Verify** option:

```
{
  xtype: 'button',
  handler: function(button, event) {
    var data = this.getDataJSON();
    this.scriptUtils.verifyForm(this,data)
  },
  scope: this,
  text: 'Verify'
}
```

All necessary information required for debugging the Cross Provisioning Platform script is displayed in a new window.

RELATED DOCUMENTATION

[Importing Scripts Created for Cross Provisioning Platform | 778](#)

[Exporting Scripts Created for Cross Provisioning Platform | 776](#)

[Adding Scripts Created for Cross Provisioning Platform | 775](#)

[Viewing Scripts Created for Cross Provisioning Platform | 781](#)

23

CHAPTER

Device Configlet Services

[Creating and Deploying a Device Configlet Order for Cross Provisioning Platform | 793](#)

[Administering a Device Configlet Service Order for Cross Provisioning Platform | 795](#)

[Administering a Device Configlet Service for Cross Provisioning Platform | 797](#)

[Decommissioning Bulk Device Configlet Services in Cross Provisioning Platform | 799](#)

[Modifying a Device Configlet Service in Cross Provisioning Platform | 801](#)

[Deleting Bulk Device Configlet Orders in Cross Provisioning Platform | 802](#)

Creating and Deploying a Device Configlet Order for Cross Provisioning Platform

To create a device configlet for Cross Provisioning Platform:

1. In the **Cross Provisioning Platform** task pane, select **CPP** > **Device Configlets Order**.
2. In the **Device Configlets Order** window, click the **Create CPP Device Configlet** icon (+).

SPACE User su

Applications << CPP > Device Configlet Orders > Create Device Configlet Order

Cross Provisioning Platform

Dashboard

Devices

CPP

Third-Party Devices

Device Configlet Orders

Device Configlet Services

Service Definitions

Service Orders

Services

Interface Migration

Report Management

Scripts

Log Collection

Service Provisioning

Service Design

Prestage Devices

Prestage Services

Jobs

Create CPP Device Configlet Order

General Settings

Select Service Definition

ID	Name
	migration
5555	Device_Sample_SD

Page 1 of 1 | Displaying 1 - 2 of 2 | Show 30 items

Order description:

Next Cancel

3. In the **Create CPP Device Configlet Order**, select the **Service definition** using the unique identifier **ID** associated with each service definition or name of the service definition.

NOTE: The value in the **ID** field is associated with a service definition. This identifier can be used when you are searching for a particular service definition while creating a device configlet order. You can search the service definition by its name, type or unique ID. You can modify the ID only during the migration of old service definition IDs.

4. In the **Order description** field, type a description for the service configlet.
5. Click **Next**.

6. Fill in the fields in the **Create Device Configlet Order** window as described in the following table.

Field	Description
Name	Type a name for the configlet
Device	Browse to locate the device upon which you want the configlet to operate.
Host Name	Type the hostname of the device upon which you want the configlet to operate.
Primary Loopback IP	Type the loopback address of the device.
Device Role	Select the role that you want the device to serve in the network: <ul style="list-style-type: none"> • L2E • Edge • Trunk
Region	Select the region where the device is located.
Uplink Interface 1	Select an interface connected to the upstream provider-edge device.
Uplink Interface 2	Select an interface connected to the upstream provider-edge device.

Field	Description
L2E UNI Interface	This field is displayed if you selected L2E as the Device Role . Select the L2E UNI interface.
L2E UNI Inner VLAN Id	This field is displayed if you selected L2E as the Device Role . Specify the inner VLAN ID of the L2E UNI interface.
L2E UNI Outer VLAN Id	This field is displayed if you selected L2E as the Device Role . Specify the outer VLAN ID of the L2E UNI interface.

7. Click **Create**.

The device configlet order is deployed, and you can view the device configlet order in the Device Configlet Orders inventory page.

If you want to create and deploy more orders, click **Create More**.

RELATED DOCUMENTATION

[Cross Provisioning Platform Overview | 33](#)

[Administering a Device Configlet Service Order for Cross Provisioning Platform | 795](#)

Administering a Device Configlet Service Order for Cross Provisioning Platform

To administer a device configlet service order for cross provisioning platform:

1. In the Cross Provisioning Platform task pane, select **CPP > Device Configlet Orders**.

2. In the Device Configlet Orders inventory page, display or delete a device configlet order, as indicated in the following table.

Action	Procedure
View Order Configuration	<p>To view the configuration of a device configlet order, do one of the following:</p> <ul style="list-style-type: none"> • Select and right-click a device configlet order, and then select View Order Configuration. • Select a device configlet order and then click the View CPP Device Configlet icon.
Delete Device Configlet	<p>To delete a device configlet order:</p> <ol style="list-style-type: none"> 1. Select and right-click a device configlet order. 2. Select Delete Device Configlet.
View Device Configlet Order Details	<p>To view the output of an attached script:</p> <ol style="list-style-type: none"> 1. Select and right-click a device configlet order. <p>NOTE: If you select multiple device configlet orders, the View Device Configlet Order Details field is unavailable.</p> 2. Select View Device Configlet Order Details. <p>The output of the attached script is displayed.</p> <p>NOTE: The View Device Configlet Order Details field is available, only if the Order Type is <i>ADD</i> or <i>MODIFY</i>.</p> <p>You cannot modify the parameters of the script as the output is displayed in Read Only format.</p> <p>The following error message is thrown if the attached script does not include any method to implicate the action:</p> <p><i>Service order details view is not supported in GUI script.</i></p>

RELATED DOCUMENTATION

Creating and Deploying a Device Configlet Order for Cross Provisioning Platform | 793

Administering a Device Configlet Service for Cross Provisioning Platform

Use the Device Configlet Services page to view or decommission a device configlet service, perform a configuration audit on a device configlet service, or view service configuration changes.

To administer a device configlet service for Cross Provisioning Platform:

1. In the Cross Provisioning Platform task pane, select **CPP > Device Configlet Services**.
2. In the Devices Configlet Services inventory page, you can perform any of the actions as indicated in the following table:

Action	Procedure
Viewing the Device Configlet Service details	<p>To view the device configlet service details:</p> <ol style="list-style-type: none"> 1. Select a device configlet service. 2. Click the View CPP Device Configlet icon. <p>The CPP Device Configlet Service Details window appears. You can view the service details, configurations, and service order audit status on the Service Details, Configuration, and SO Audit tabs respectively.</p>
Decommissioning a Device Configlet Service	<p>To decommission a device configlet service:</p> <ol style="list-style-type: none"> 1. Select a device configlet service. 2. Right-click the device configlet service, and select Service > Decommission Device Configlet. 3. Do one of the following: <ul style="list-style-type: none"> • 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. • To deploy the service at a later time, select Decommission later, select a date and time, then click OK.

Action	Procedure
Performing a Configuration Audit	<p>To perform a configuration audit on a device configlet service:</p> <ol style="list-style-type: none"> 1. Select a device configlet service. 2. Right-click the device configlet service, and select Audit > Perform Configuration Audit. 3. In the Schedule Configuration Audit window, do one of the following: <ul style="list-style-type: none"> • To audit the service configuration immediately, select Audit Now, then click OK. An Audit Information window appears, providing a link to details about the audit in the Job Management workspace, and an OK button. • To audit the service configuration at a later time, select Audit Later, enter a date and time, then click OK.
Viewing the Service Configuration Changes	<p>To view the service configuration changes:</p> <ol style="list-style-type: none"> 1. Select a device configlet service. 2. Right-click the device configlet service, and select Audit > Service Configuration Changes. <p>The Service Configuration window displays the list of devices and its configuration.</p>

RELATED DOCUMENTATION

| [Creating and Deploying a Device Configlet Order for Cross Provisioning Platform](#) | 793

Decommissioning Bulk Device Configlet Services in Cross Provisioning Platform

Use the **Device Configlet Services** page to decommission multiple device configlet services of Cross Provisioning Platform in bulk. You can select the number of services that a single page displays, by selecting one of the following values from the **Show items** drop-down list at the bottom of the page:

- 10
- 20
- 40
- 60
- 80
- 100
- 200

To decommission device configlet services in bulk:

1. From the **Cross Provisioning Platform** task pane, select **CPP > Device Configlet Services**.
The **Device Configlet Services** page that appears displays a list of existing services.
2. Select the check boxes against the device configlet services that you want to decommission.
3. Either right-click and select **Service > Decommission** or click the **Decommission** icon on the grid tool bar. You can also decommission a service by selecting **Actions > Service > Decommission**.

The **Schedule Decommission** page appears where the selected services are listed. You can schedule the decommissioning to happen immediately or later at a scheduled time.

NOTE: You cannot decommission a service that has been modified on the **Services** page unless the value of the **Order State** field of the corresponding service is **Completed**. You can decommission only 25 services at a time. If the count exceeds 25, the following error message appears:

Service decommissioning cannot be scheduled if the selected services count is greater than 25.

SPACE

User **super** logged in Domain: Gl...

Applications

Cross Provisioning Platform

CPP > Device Configlet Services

2 Items Selected

Name	State	Service Type	Definition
SO380545104	Deployed	Device	jnpr_intrfacmigration_halan
SO379742487	Deployed	Device	jnpr_intrfacmigration_halan
SO376984279	Deployed	Device	Interfacemigration_sd
SO376955259	Deployed	Device	Interfacemigration_sd
SO376...	Service	Device	Interfacemigration_sd
SO376...	Audit	Device	Interfacemigration_sd

Actions

- Service
- Audit
- View Results
- View Service Order(s)
- Delete Private Tags
- Tag It
- UnTag It
- View Tags
- Clear All Selections

Decommission

4. Select the **Decommission now** option button to decommission the services immediately. You can also decommission the selected services later by selecting the **Decommission later** option button and setting the preferred date and time.
5. Click **OK** to decommission the selected device configlet services.

The **Job Details** dialog box appears with a list of job IDs.

NOTE: For every device configlet service that is selected to be decommissioned, a unique job ID is assigned. You can view the details of each job on the **Job Management** page by clicking the corresponding job ID.

For every device configlet service that is decommissioned, a message is logged on the Audit Log page. To view the **Audit Log** page, select **Network Management Platform > Audit Logs > Audit Log**.

RELATED DOCUMENTATION

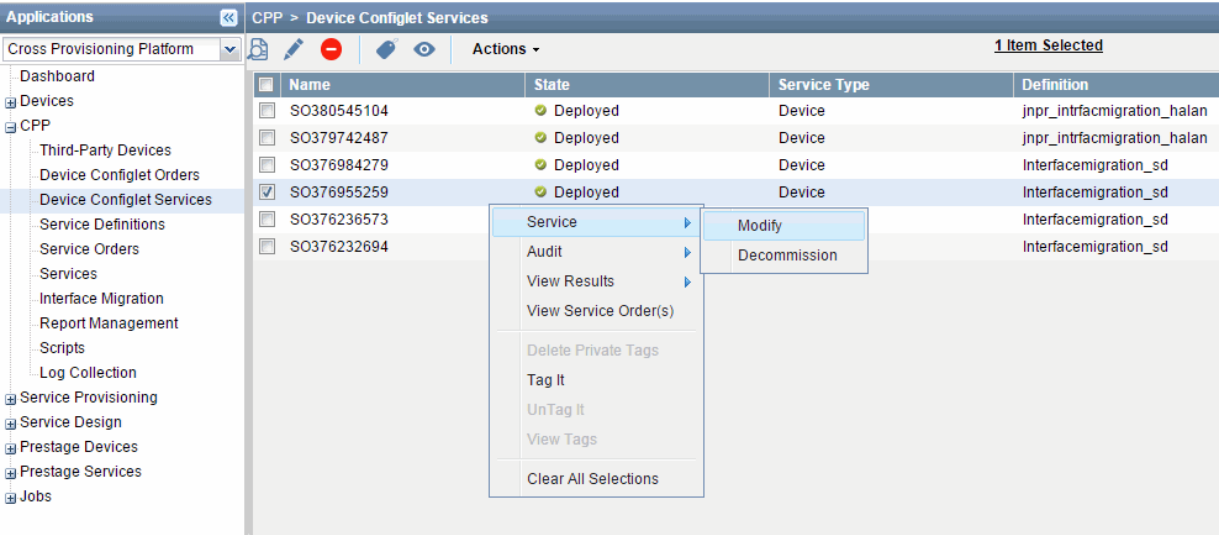
[Decommissioning a Service](#) | 834

Modifying a Device Configlet Service in Cross Provisioning Platform

Use the **Device Configlet Services** landing page to modify a device configlet service in Cross Provisioning Platform. You can modify a device configlet service only if a modification script is attached to the device configlet service.

To modify a device configlet service:

1. From the **Cross Provisioning Platform** task pane, select **CPP > Device Configlet Services**.
The **Device Configlet Services** page that appears displays a list of existing device configlet services.
2. Select and right-click a device configlet service that you want to modify.
3. Either right-click a device configlet service and select **Service > Modify** or select a service and click the **Modify** icon on the grid tool bar. You can also modify a service by selecting the service and then selecting **Actions > Modify**.



The **Modify Service** page appears.

NOTE: The **Modify Service** page details vary according to the type of the selected device configlet service.

4. Modify the device configlet service details and click **Modify**.

The **Job Details** dialog box appears along with a job ID link.

5. Click the **Job ID** link to view the job details.

The **Job Management** page that appears contains a list of the jobs, along with the status of the jobs.

RELATED DOCUMENTATION

[Modifying Bulk Services and Devices in Cross Provisioning Platform | 816](#)

Deleting Bulk Device Configlet Orders in Cross Provisioning Platform

Use the **Device Configlet Orders** landing page to select and delete multiple device configlet orders in bulk. You can select the number of services that a single page displays, by selecting one of the following values from the **Show items** drop-down list at the bottom of the page:

- 10
- 20
- 40
- 60
- 80
- 100
- 200

To delete device configlet orders of Cross Provisioning Platform in bulk:

1. From the **Cross Provisioning Platform** task pane, select **CPP > Device Configlet Orders**.

The **Device Configlet Orders** page that appears displays a list of existing device configlet orders.

2. Select the check boxes against the device configlet orders that you want to delete.
3. Right-click any device configlet order and select **Delete Device Configlet** or click the **Delete Device Configlet** icon on the grid tool bar.

The **Delete Device Configlet** page appears asking you to confirm the selection of the device configlet orders to be deleted.

NOTE: When you select multiple device configlet orders, the **Delete Device Configlet** option is enabled only if the order state of the selected device configlet orders is either **Failed_Deployed**, **Requested** or **Invalid**.

When the order state is **Completed**, the following points hold true:

- You cannot delete a device configlet order if its order state is **Completed** and the related service is listed on the **Device Configlet Services** landing page.
- You cannot delete the first and the last device configlet order created for a service if their order state is **Completed** and the related service is listed on the **Device Configlet Services** landing page.
- The device configlet orders that are in the **Completed** state for a service can be deleted only if the related service is not listed on the **Device Configlet Services** landing page.

You can delete 25 device configlet orders at a time. If the count exceeds 25, the following error message appears:

Device configlet orders cannot be deleted if the selected device configlet order count is greater than 25.

The screenshot shows the SPACE application interface. The left sidebar contains a navigation menu with options like Dashboard, Devices, CPP, Third-Party Devices, Device Configlet Orders, Device Configlet Services, Service Definitions, Service Orders, Services, Interface Migration, Report Management, Scripts, Log Collection, Service Provisioning, Service Design, Prestage Devices, Prestage Services, and Jobs. The main content area displays a table titled 'CPP > Device Configlet Orders'. The table has columns for Name, Order State, Service Type, and Created Date. Two items are selected, and a context menu is open over them, showing options like 'View Pending Order Configuration', 'Delete Device Configlet', 'Cancel Order', 'Delete Private Tags', 'Tag It', 'UnTag It', 'View Tags', and 'Clear All Selections'.

Name	Order State	Service Type	Created Date
SO380545104	Completed	Device	Mar 17, 2015 4:12:08 PM IST
SO379742487	Completed	Device	Mar 16, 2015 5:54:28 PM IST
SO379737028	Failed_Deployed	Device	Mar 16, 2015 5:51:23 PM IST
SO377088245	Completed	Device	Mar 13, 2015 4:10:41 PM IST
SO376984279	Completed	Device	Mar 13, 2015 1:17:21 PM IST
SO376982000	Failed_Deployed	Device	Mar 13, 2015 1:15:22 PM IST
SO376955	Completed	Device	Mar 13, 2015 12:28:53 PM IST
SO376236	Completed	Device	Mar 12, 2015 4:31:24 PM IST
SO376232	Completed	Device	Mar 12, 2015 4:24:36 PM IST

4. Click **Delete** to delete the selected device configlet orders.

The selected device configlet orders are deleted and the landing grid is refreshed. For every device configlet order that is deleted, a message is logged on the **Audit Log** page. To view the Audit Log page, select **Network Management Platform > Audit Logs > Audit Log**.

RELATED DOCUMENTATION

[Deleting Bulk Service Orders in Cross Provisioning Platform](#) | 828

24

CHAPTER

Third-Party Devices

[Adding a Third-Party Device to the Cross Provisioning Platform System | 806](#)

[Viewing Third-Party Device Details for Cross Provisioning Platform | 807](#)

[Synchronizing Third-Party Devices with the OSS for Cross Provisioning Platform | 808](#)

[Confirming Communication with the Third-Party OSS Server for Cross Provisioning Platform | 810](#)

[Preconfiguring the Third-Party OSS Device for Cross Provisioning Platform | 811](#)

Adding a Third-Party Device to the Cross Provisioning Platform System

To add a third-party device to the cross provisioning platform system:

1. In the Cross Provisioning Platform task pane, select **CPP > Third-Party Devices**.
2. In the **Third-Party Devices** window, click the **Add Third-Party Device** icon (+).

The Add OSS Device appears.



3. In the **Add OSS Device** window, click the **Host Name** or **IP Address** button and then enter the hostname or IP address of the device.
4. In the **Vendor**, select the third-party vendor.
5. Click **Add**.

The Cross Provisioning Platform application discovers and displays the device that you have added. In the Third-Party landing page, you can view and filter devices based on the vendor type.

RELATED DOCUMENTATION

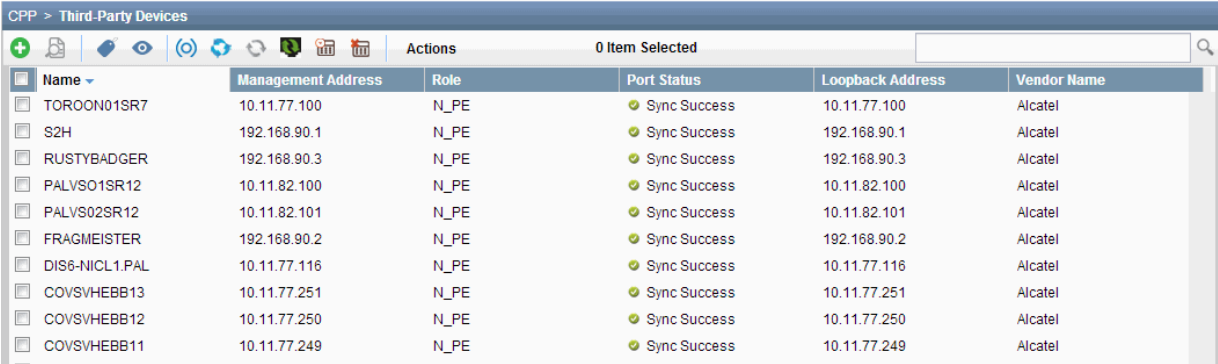
[Viewing Third-Party Device Details for Cross Provisioning Platform | 807](#)

[Synchronizing Third-Party Devices with the OSS for Cross Provisioning Platform | 808](#)

Viewing Third-Party Device Details for Cross Provisioning Platform

To view the details of a device added for cross provisioning platform:

1. In the Cross Provisioning Platform task pane, select **CPP > Third-Party Devices**.



Name	Management Address	Role	Port Status	Loopback Address	Vendor Name
TOROON01SR7	10.11.77.100	N_PE	Sync Success	10.11.77.100	Alcatel
S2H	192.168.90.1	N_PE	Sync Success	192.168.90.1	Alcatel
RUSTYBADGER	192.168.90.3	N_PE	Sync Success	192.168.90.3	Alcatel
PALVSO1SR12	10.11.82.100	N_PE	Sync Success	10.11.82.100	Alcatel
PALVSO2SR12	10.11.82.101	N_PE	Sync Success	10.11.82.101	Alcatel
FRAGMEISTER	192.168.90.2	N_PE	Sync Success	192.168.90.2	Alcatel
DIS6-NICL1.PAL	10.11.77.116	N_PE	Sync Success	10.11.77.116	Alcatel
COVSVHEBB13	10.11.77.251	N_PE	Sync Success	10.11.77.251	Alcatel
COVSVHEBB12	10.11.77.250	N_PE	Sync Success	10.11.77.250	Alcatel
COVSVHEBB11	10.11.77.249	N_PE	Sync Success	10.11.77.249	Alcatel

2. In the **Third-Party Device** window, select a device from the list and click the **View Device Details** icon in the command bar.



Device Details

Name: S2H
MPLS role: N_PE
Vendor: Alcatel
Loopback address: 192.168.90.1
Connection status: unknown
Service role: L2, L3

UNI Interfaces

Name	Status	Description	Admin Status	Duplex	Speed	Auto Negotia	Dot1Q	Q-in-Q	Port MTU	Lag Id	Is NNI Port	Mode
Port 2/1/13	Down	Arsalan - Shaw EAS Testing	Up	fullDuplex	0	true	0x8100	0x8100	1596	0	false	access
Port 2/1/15	Up	SAR-8 LAG-1	Up	fullDuplex	1000000	false	0x8100	0x88a8	1500	27	false	access
Port 1/1/16	Down	Jason - Aux IP Test	Up	fullDuplex	0	true	0x8100	0x8100	2000	0	false	access
Port 2/1/20	Down	WireIE NNI LAG	Up	fullDuplex	0	limited	0x8100	0x88a8	9212	15	false	access
Port 2/1/2	Up	to-RustyBad... 2/1/2	Up	fullDuplex	1000000	limited	0x8100	0x8100	9212	3	true	network

OK Resync

3. When you are done viewing the device details, click **OK**.

RELATED DOCUMENTATION

[Adding a Third-Party Device to the Cross Provisioning Platform System](#) | 806

Synchronizing Third-Party Devices with the OSS for Cross Provisioning Platform

The Cross Provisioning Platform (CPP) application enables you to synchronize newly added third-party devices added to the CPP system with the Operations Support System (OSS) of the third party.

You can set a synchronization job to run daily at a specified scheduled time (default 5:00 AM). The job synchronizes the following data with the CPP system:

- The job synchronizes newly added third-party devices.
- The job synchronizes ports newly added or deleted from existing devices.
- Third-party devices are deleted from the CPP system if the device is no longer associated with an active service that was created in CPP.

To set the time at which you want the synchronization job to run:

1. In the Network Management Platform task pane, select **Administration > Applications**.
2. In the **Applications** window, select **Network Activate**.
3. From the **Actions** menu, select **Modify Application Settings**.
4. In the **Modify Application Settings** window, select **OSSConfigParameters**.

OSSConfigParameters		
OSSConfigParameters		
Alcatel Primary Server IP:	<input type="text" value="10.216.114.28"/>	
Alcatel Primary Server Port:	<input type="text" value="28443"/>	
Backup Server IP:	<input type="text"/>	
Backup Server Port:	<input type="text"/>	
HTTP Connection TimeOut (Milliseconds):	<input type="text" value="25000"/>	[default]
Maximum API Requests:	<input type="text" value="5"/>	[default]
Number of devices for port sync request:	<input type="text" value="10"/>	[default]
OSS User Name:	<input type="text" value="SAM-CPP"/>	
OSS User Password:	<input type="password"/>	
Synchronize OSS Inventory daily at given time:	<input type="text" value="05:00 AM"/>	[default]
<input checked="" type="checkbox"/> Use HTTP protocol		
<input checked="" type="checkbox"/> Use primary server		

NOTE: The **HTTP Connection Timeout** parameter is measured in milliseconds.

- In the **Synchronize OSS Inventory daily at given time** field of the **OSSConfigParameters** panel, set the time at which you want the synchronization job to run.

NOTE: The time at which the synchronization job runs is associated with the location of the browser in which you are using the Junos Space software. That is, the synchronization job runs according to the browser time where the job is scheduled, not according to the time where the Junos Space server is located.

You can also manage synchronization operations from the Cross Provisioning Platform application. To synchronize devices:

- In the Cross Provisioning Platform task pane, select **CPP > Third-Party Devices**.

The Third-Party Devices window appears.

- Select a synchronize operation.

The Third-Party Devices window displays four icons in the command bar, which enable you to run the following synchronization operations:

- Synchronize all the devices with OSS—This operation discovers new devices and synchronizes old devices with OSS.
- Synchronize selected device with OSS—This operation synchronizes only the selected devices with the OSS.
- Schedule OSS synchronization job—This operation schedules daily synchronization.
- Cancel OSS synchronization job—This cancels the daily synchronization job.

3. In **Vendor**, select the vendor type.

4. Click **OK**.

RELATED DOCUMENTATION

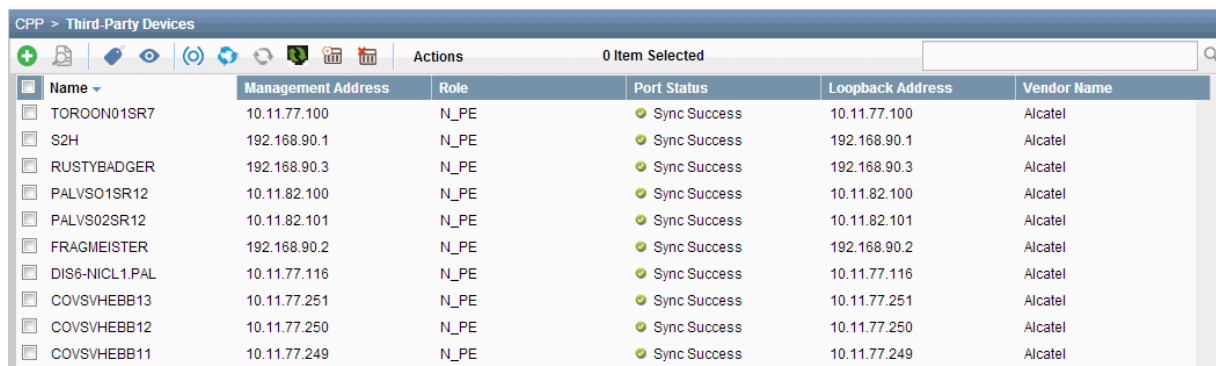
[Adding a Third-Party Device to the Cross Provisioning Platform System | 806](#)

[Viewing Third-Party Device Details for Cross Provisioning Platform | 807](#)

Confirming Communication with the Third-Party OSS Server for Cross Provisioning Platform

To confirm that the cross provisioning platform system can communicate with the OSS server:

1. In the Cross Provisioning Platform task pane, select **CPP > Third Party Devices**.



Name	Management Address	Role	Port Status	Loopback Address	Vendor Name
TOROON01SR7	10.11.77.100	N_PE	Sync Success	10.11.77.100	Alcatel
S2H	192.168.90.1	N_PE	Sync Success	192.168.90.1	Alcatel
RUSTYBADGER	192.168.90.3	N_PE	Sync Success	192.168.90.3	Alcatel
PALVS01SR12	10.11.82.100	N_PE	Sync Success	10.11.82.100	Alcatel
PALVS02SR12	10.11.82.101	N_PE	Sync Success	10.11.82.101	Alcatel
FRAGMEISTER	192.168.90.2	N_PE	Sync Success	192.168.90.2	Alcatel
DIS6-NICL1.PAL	10.11.77.116	N_PE	Sync Success	10.11.77.116	Alcatel
COVSVHEBB13	10.11.77.251	N_PE	Sync Success	10.11.77.251	Alcatel
COVSVHEBB12	10.11.77.250	N_PE	Sync Success	10.11.77.250	Alcatel
COVSVHEBB11	10.11.77.249	N_PE	Sync Success	10.11.77.249	Alcatel

2. In the **Third-Party Devices** window, click the **Ping OSS Server** icon in the command bar.

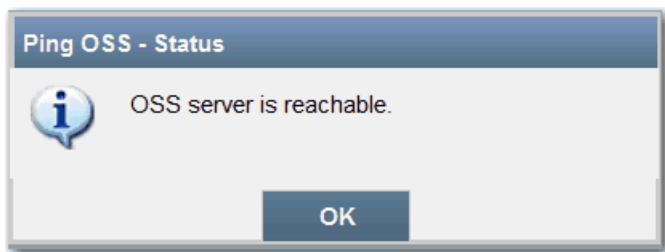
The Select Vendor window appears.

3. In the Select Vendor window, select the vendor type.

The primary address and the secondary address of the vendor is displayed.

4. Click **Ok**.

The **Ping OSS – Status** window indicates whether or not the CPP system has access to the OSS server.



NOTE: You must have configured the OSS server parameters in the application settings. For more information about configuring the OSS parameters, see [“Preconfiguring the Third-Party OSS Device for Cross Provisioning Platform”](#) on page 811.

RELATED DOCUMENTATION

[Synchronizing Third-Party Devices with the OSS for Cross Provisioning Platform | 808](#)

[Preconfiguring the Third-Party OSS Device for Cross Provisioning Platform | 811](#)

Preconfiguring the Third-Party OSS Device for Cross Provisioning Platform

To preconfigure the third-party OSS device:

1. In the Network Management Platform, select **Administration > Applications**.

The Applications window appears.

2. In the **Applications** window, select **Cross Provisioning Platform**.

3. From the **Actions** menu, select **Modify Application Settings**.

The Modify Application Settings window appears.

4. In the **Modify Application Settings** window, select **OSSConfigParameters**.

The OSSConfigParameters pane lists the OSS configuration parameters that you must configure for the following vendors:

- Alcatel OSS Configuration
- Canoga OSS Configuration

You can view or configure for the OSS parameters.

5. In the OSSConfigParameters pane, select **Alcatel OSS Configuration** or **Canoga OSS Configuration**.

The OSSConfigParameters pane lists a set of parameters that you can configure for Nokia or Canoga Perkins.

OSSConfigParameters

OSSConfigParameters

Alcatel Primary Server IP:

10.216.114.28

Alcatel Primary Server Port:

28443

Backup Server IP:

Backup Server Port:

HTTP Connection TimeOut (MilliSeconds):

25000

[default]

Maximum API Requests:

5

[default]

Number of devices for port sync request:

10

[default]

OSS User Name:

SAM-CPP

OSS User Password:

Synchronize OSS Inventory daily at given time:

05:00 AM

[default]

☒ Use HTTP protocol

☒ Use primary server

Modify

Cancel

6. Fill in the fields in the **OSSConfigParameters** panel for a specific vendor as described in the following table.

OSS Parameter	Description
Primary Server IP	IP address of the primary server.

OSS Parameter	Description
Primary Server Port	Port number of the primary server.
Backup Server IP	IP address of the backup server.
Backup Server Port:	Port number of the backup server.
HTTP Connection Timeout (milliseconds)	Duration of HTTP connection (in milliseconds) before the timeout elapses.
Maximum API Requests	Maximum number of simultaneous API requests permitted.
Number of Device for Port Sync Request	Fetches the port details for the number of devices that you have specified here.
OSS User Name	Username for accessing the OSS server.
OSS User Password	Hashed password for accessing the OSS server.
Synchronize OSS Inventory daily at given time	<p>Sets the daily time at which the CPP system synchronizes third-party devices, added or deleted from the CPP system, with the OSS server.</p> <p>NOTE: The time at which the synchronization job runs is associated with the location of the browser in which you are using the Junos Space software. That is, the synchronization job runs according to the browser time where the job is scheduled, not according to the time where the Junos Space server is located.</p>
Use HTTP Protocol	<p>If this check box is selected, the CPP system uses the HTTP protocol.</p> <p>The default protocol is HTTPS.</p>
Use primary server	If this check box is selected, the CPP system communicates with the primary OSS server. If the check box is not selected, the system interacts with the backup server.

- When you are done entering information in the **OSSConfigParameters** fields, click **Modify**.

If you want to modify the application settings of the Cross Provisioning Platform application, select **Administration > Applications > Cross Provisioning Platform** and select **Modify Application Settings** in the Network Management platform. You can uninstall the application by selecting **Cross Provisioning Platform > Uninstall Application**.

NOTE: The OSS configuration values are still retained and reflected in the corresponding fields even after you uninstall and reinstall the application.

RELATED DOCUMENTATION

[Synchronizing Third-Party Devices with the OSS for Cross Provisioning Platform | 808](#)

[Confirming Communication with the Third-Party OSS Server for Cross Provisioning Platform | 810](#)

25

CHAPTER

Bulk Services and Devices

Modifying Bulk Services and Devices in Cross Provisioning Platform | **816**

Administering Bulk Service Operations in Cross Provisioning Platform | **822**

Decommissioning Bulk Services in Cross Provisioning Platform | **826**

Deleting Bulk Service Orders in Cross Provisioning Platform | **828**

Modifying Bulk Services and Devices in Cross Provisioning Platform

IN THIS SECTION

- [Modifying Bulk Services in Cross Provisioning Platform | 816](#)
- [Modifying Bulk Devices in Cross Provisioning Platform | 819](#)

Cross Provisioning Platform is an extension of the Network Activate application within Junos Space, which provides a single pane of interaction to deploy services across vendor network devices. You can modify the device and the service configuration in bulk on the basis of the service definition. This feature is applicable only to Juniper Networks devices.

With this feature, you can modify all the services on the basis of a particular service definition or all the devices within a particular service definition. To modify services or devices in bulk, you need to create a configuration script in XSLT format and a GUI script in JS format.

NOTE: Bulk modification cannot be applied on services and devices simultaneously.

Make sure that you have the configuration and the GUI scripts present on the local machine.

To modify and deploy services and devices in bulk:

Modifying Bulk Services in Cross Provisioning Platform

To modify services in bulk based on a service definition:

1. In the **Cross Provisioning Platform** task pane, select **CPP > Scripts**.

The **Scripts** page that appears displays a list of the existing scripts.

2. Click the **Add Script** icon above the tool grid.

The **Add Script(s)** page that appears contains the **Script Settings** section.

3. In the **Script Settings** section, perform the following steps:

- In the **Name** field, type 3 through 128 alphanumeric characters to identify the script that you are creating.
- In the **Description** field, type 3 through 128 alphanumeric characters to further identify the script.
- Select **Junos Space** from the **Vendor Type** drop-down list, because this feature supports only Juniper Networks devices.

NOTE: The **GUI Script** field appears only when the **Vendor Type** is **Junos Space**. If the vendor type is third-party, the **GUI Script** field does not appear.

- In the **Configuration Script** field, click **Browse** to upload the configuration script from the local machine.
- In the **GUI Script** field, click **Browse** to upload the GUI script from the local machine.
- Click **Create** to add the uploaded scripts to the Cross Provisioning Platform application.

The **Status** dialog box that appears confirms the successful addition of scripts.

NOTE: The default value of the **Version** field is 1.

4. Click **OK**.

You are redirected to the **Scripts** page.

5. In the **Cross Provisioning Platform** task pane, select **CPP > Service Definitions > Create CPP Service Definition**.

The **Create Service Definition** page appears.

6. Perform the following steps in the **Create Service Definition** page:

- a. In the **Name** field, type 3 through 128 alphanumeric characters to identify the service definition that you are creating.
- b. In the **Description** field, type 3 through 128 alphanumeric characters to further identify the service definition.
- c. From the **Type** drop-down list, select the type of the service definition.
- d. In the **Creation** field of the **JUNOS Space Service Scripts** section, click **Browse** to upload the script.

NOTE: The **Modification** script for **JUNOS Space Service Scripts** is optional. You do not have to upload the **SAM Service Scripts** because this feature is applicable to Juniper Networks devices.

7. Click **Create**.

The **Service Definitions** page that appears displays a list of the existing service definitions along with the one that you created.

8. Right-click the service definition you created and click **Attach Scripts**.

The **Attach Scripts** page appears.

9. Perform the following steps:

- In the **Bulk service modify** field, click **Browse** and upload the bulk service modification script.
- In the **Bulk device modify** field, click **Browse** and upload the bulk device modification script.
- Click **Attach**.

A confirmation dialog box appears to confirm the successful attachment of the scripts.

10. Click **OK**.

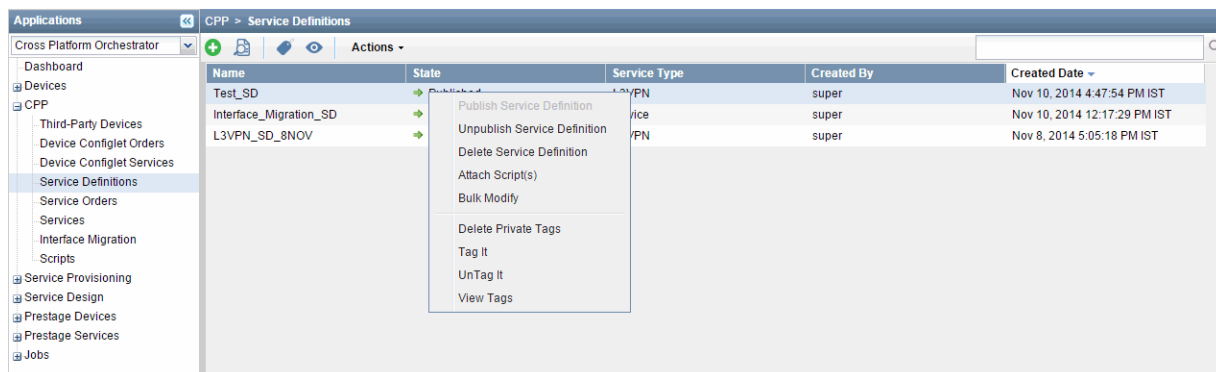
11. In the **Cross Provisioning Platform**, select **CPP > Service Definitions**.

The **Service Definitions** page that appears displays a list of the existing service definitions.

12. Right-click the service definition that you created and select **Bulk Modify**.

The **Bulk Modify** page appears.

NOTE: The **Service** option is selected by default in the **Apply to** section on the **Bulk Modify** page.



13. On the Bulk Modify page, select the services that you want to modify.

Cross Provisioning Platform provides you with an option to modify parameters before you deploy the services in bulk. Based on the script that you have attached, you have the following options:

- **Next**—This option is available only if **isGUIRequired** is set to True in the script you have attached.
- **Deploy**—This option is available only if **isGUIRequired** is set to False in the script you have attached.

14. Click **Next** to modify services in bulk.

The Bulk Service Modify page appears.

15. Modify the parameters.

NOTE: The script you have attached determines which parameters can be modified.

16. Click **Deploy**.

The **Job Details** dialog box that appears contains the Job ID. You can click the *Job ID* link to view the status of the modified services on the **Job Management** page.

Modifying Bulk Devices in Cross Provisioning Platform

To modify devices in bulk within a service definition:

1. In the **Cross Provisioning Platform** task pane, select **CPP > Scripts**.

The **Scripts** page that appears displays a list of the existing scripts.

2. Click the **Add Script** icon above the tool grid.

The **Add Script(s)** page that appears contains the **Script Settings** section.

3. In the **Script Settings** section, perform the following steps:

- In the **Name** field, type 3 through 128 alphanumeric characters to identify the script that you are creating.
- In the **Description** field, type 3 through 128 alphanumeric characters to further identify the script.
- Select **Junos Space** from the **Vendor Type** drop-down list, because this feature supports only Juniper Networks devices.

NOTE: The **GUI Script** field appears only when the **Vendor Type** is **Junos Space**. If the vendor type is third-party, the **GUI Script** field does not appear.

- In the **Configuration Script** field, click **Browse** to upload the configuration script from the local machine.
- In the **GUI Script** field, click **Browse** to upload the GUI script from the local machine.
- Click **Create** to add the uploaded scripts to the Cross Provisioning Platform application.

The **Status** dialog box that appears confirms the successful addition of scripts.

NOTE: The default value of the **Version** field is 1.

4. Click **OK**.

You are redirected to the **Scripts** page.

5. In the **Cross Provisioning Platform** task pane, select **CPP > Service Definitions > Create CPP Service Definition**.

The **Create Service Definition** page appears.

6. Perform the following steps in the **Create Service Definition** page:
 - a. In the **Name** field, type 3 through 128 alphanumeric characters to identify the service definition that you are creating.
 - b. In the **Description** field, type 3 through 128 alphanumeric characters to further identify the service definition.
 - c. From the **Type** drop-down list, select the type of the service definition.
 - d. In the **Creation** field of the **JUNOS Space Service Scripts** section, click **Browse** to upload the script.

NOTE: The **Modification** script for **JUNOS Space Service Scripts** is optional. You do not have to upload the **SAM Service Scripts** because this feature is applicable to Juniper Networks devices.

7. Click **Create**.

The **Service Definitions** page that appears displays a list of the existing service definitions along with the one that you created.

8. Right-click the service definition you created and click **Attach Scripts**.

The **Attach Scripts** page appears.

9. Perform the following steps:
 - a. In the **Bulk service modify** field, click **Browse** and upload the bulk service modification script.

- b. In the **Bulk device modify** field, click **Browse** and upload the bulk device modification script.
- c. Click **Attach**.

A confirmation dialog box appears to confirm the successful attachment of the scripts.

10. Click **OK**.

11. In the **Cross Provisioning Platform**, select **CPP > Service Definitions**.

The **Service Definitions** page that appears displays a list of the existing service definitions.

12. Right-click the service definition and select **Bulk Modify**.

The **Bulk Modify** page appears.

Device Name	Interface	Unit	Loopback	Service Type	Status
Service Name: SO175764310 (2 Items)					
trala	ge-2/0/6	206	192.70.0.53	FLEX	Pending
trala	ge-0/3/2	206	192.70.1.58	FLEX	Pending
Service Name: SO175766337 (2 Items)					
trala	ge-1/3/0	156	192.70.1.58	FLEX	Pending
trala	ge-2/0/9	156	192.70.0.53	FLEX	Pending
Service Name: SO175766002 (2 Items)					
trah	ge-1/1/1	178	192.70.0.51	FLEX	Pending
trala	ge-0/0/2	178	192.70.1.58	FLEX	Pending
Service Name: SO175766714 (2 Items)					
trala	ge-0/3/3	233	192.70.1.58	FLEX	Pending
trah	ge-1/1/4	233	192.70.0.51	FLEX	Pending

13. Select the **Device** option in the **Apply to** section to modify the devices in bulk.

14. Select the devices that you want to modify.

Cross Provisioning Platform provides you with an option to modify parameters before you deploy the devices in bulk. Based on the script that you have attached, you have the following options:

- **Next**—This option is available only if **isGUIRequired** is set to True in the script you have attached.
- **Deploy**—This option is available only if **isGUIRequired** is set to False in the script you have attached.

15. Click **Next** to modify devices in bulk.

The Bulk Device Modify page appears.

16. Modify the parameters.

NOTE: The script you have attached determines which parameters can be modified.

17. Click **Deploy**.

The **Job Details** dialog box that appears contains the Job ID. You can click the *Job ID* link to view the status of the modified services on the **Job Management** page.

RELATED DOCUMENTATION

[Adding Scripts Created for Cross Provisioning Platform | 775](#)

[Importing Scripts Created for Cross Provisioning Platform | 778](#)

Administering Bulk Service Operations in Cross Provisioning Platform

Use the Bulk Service Operations page to delete services in bulk, migrate service interfaces, or resynchronize services.

To administer bulk service operations in Cross Provisioning Platform:

1. On the Cross Provisioning Platform task pane, select **CPP > Bulk Service Operations**.

2. On the Bulk Service Operations inventory page, you can perform the following actions:

Action	Procedure
Service Deletion	<p>To delete the services in bulk:</p> <ol style="list-style-type: none"> 1. Select the Service Deletion option button. Service Type is displayed. 2. Select an option button from Service Type. <ul style="list-style-type: none"> ● PW-LDP—Select this option button if you want to delete LDP-based point-to-point services. ● PW-BGP—Select this option button if you want to delete BGP-based point-to-point services. <p>NOTE: Only LDP-based and BGP-based point-to-point services are supported. If PW-LDP or PW-BGP options are unavailable, you must verify the roles assigned to your user account. For information about roles, see “Creating a User-Specific Role to Prevent or Allow Certain Actions on a Service” on page 65.</p> 3. On the Step 1: Select Device grid, select a device. The corresponding interfaces are listed on the Step 2: Select Interface grid. 4. On the Step 2: Select Interface grid, select an interface. The corresponding services are listed on the Step 3: Select Service(s) grid. 5. On the Step 3: Select Service(s) grid, select the services. NOTE: The number of services is restricted to 20. 6. Click Decommission. The Schedule Decommission window appears. 7. Do one of the following: <ul style="list-style-type: none"> ● To decommission the service immediately, select Decommission now and click OK. <ol style="list-style-type: none"> a. In the Order Information window, click the job ID of the decommission job. The Job Management page that appears displays a filtered view of the job inventory, showing only the decommission job. b. Double-click the job. The Bulk Service Deletion Deployment window appears. You can view the list of service orders that are deleted. ● To decommission the service at a later time, select Decommission later, select a date and time, then click OK.

Action	Procedure
Interface Migration	<p>When an interface becomes faulty or needs to be migrated to a higher-capacity port, you must migrate all services deployed on a specific interface to the destination interface on the same device. The Cross Provisioning Platform application modifies the device configuration to migrate all the services. The Cross Provisioning Platform application deletes the source interface and adds the destination interface to the service.</p> <p>For information about migrating service interfaces, see “Migrating Service Interfaces in Cross Provisioning Platform” on page 61.</p>

Action	Procedure
Resync Services	<p>The Cross Provisioning Platform allows you to perform service resynchronization to validate and merge selected services with the current configuration of the devices or network. You can resynchronize the configuration changes made within the same device or different devices. The information about migrated devices is obtained from the latest configuration of a device using VCID and the IP address of the neighboring device.</p> <p>When you perform the Resync Services action, the service configurations in the Cross Provisioning Platform database are updated with the latest values. Following are the parameters that are updated in the Cross Provisioning Platform database:</p> <ul style="list-style-type: none"> • Device • Interface • VLAN ID <p>To perform service resynchronization:</p> <ol style="list-style-type: none"> 1. Select the Resync Service option button. The Service Type section is displayed. By default, PW_LDP is selected. NOTE: This feature is supported only on LDP-based point-to-point services, deployed on Juniper Networks and Nokia devices. If the LDP-based point-to-point service is configured for a Layer 2 Ethernet device, Layer 2 Ethernet configurations are not validated. 2. On the Step 1: Select Device grid, select Vendor and select the device from the list. The corresponding interfaces are listed on the Step 2: Select Interface grid. 3. On the Step 2: Select Interface grid, select an interface. The corresponding services are listed on the Step 3: Select Service(s) grid. 4. On the Step 3: Select Service(s) grid, select the services. 5. Click Resync. 6. In the Order Information window, click the job ID. The Job Management page that appears displays a filtered view of the job inventory, showing only the resynchronization job. 7. Double-click the job. The Bulk Deployment window appears. You can view the list of services that are updated.

RELATED DOCUMENTATION

[Migrating Service Interfaces in Cross Provisioning Platform | 61](#)

[Decommissioning a Service | 834](#)

Decommissioning Bulk Services in Cross Provisioning Platform

Use the **Services** page to decommission multiple services of Cross Provisioning Platform in bulk. You can select the number of services that a single page displays, by selecting one of the following values from the **Show items** drop-down list at the bottom of the page:

- 10
- 20
- 40
- 60
- 80
- 100
- 200

To decommission services in bulk:

1. From the **Cross Provisioning Platform** task pane, select **CPP > Services**.

The **Services** page that appears displays a list of existing services.

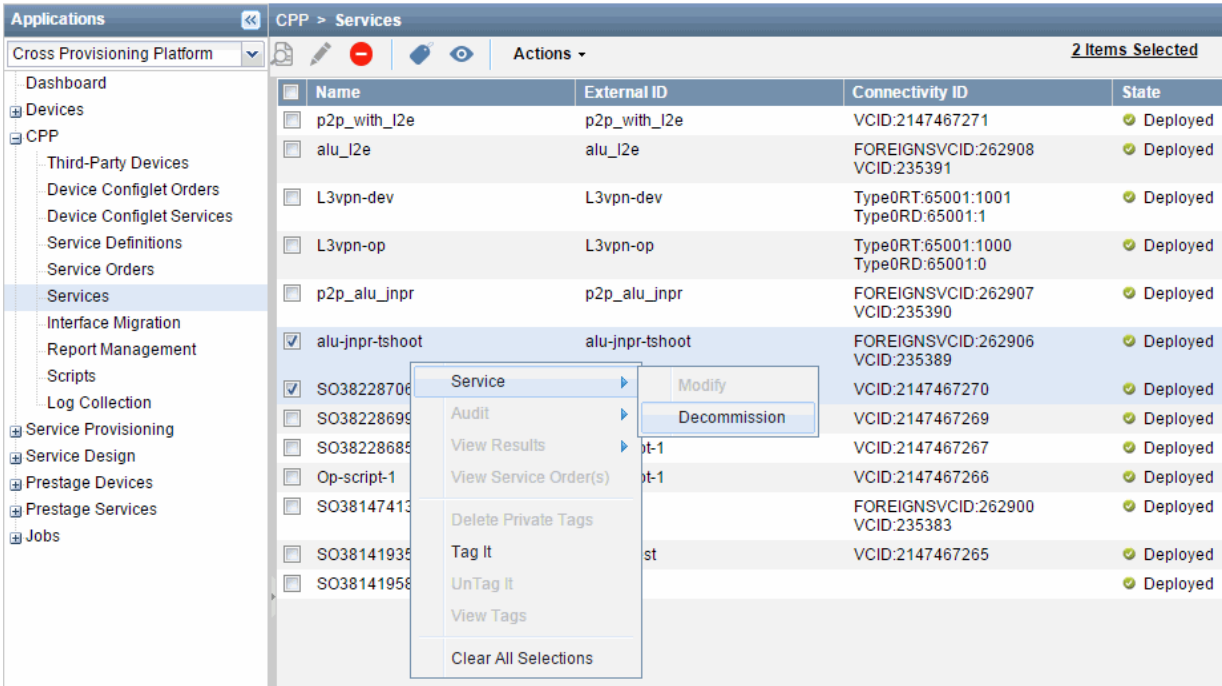
2. Select the check boxes against the services that you want to decommission.
3. Either right-click and select **Service > Decommission** or click the **Decommission** icon on the grid tool bar. You can also decommission a service by selecting **Actions > Service > Decommission**.

The **Schedule Decommission** page appears where the selected services are listed. You can schedule the decommissioning process to happen immediately or later.

NOTE: You cannot decommission a service that has been modified in the **Services** page unless the value of the **Order State** field of the corresponding service is **Completed**. You can decommission only 25 services at a time. If the count exceeds 25, the following error message appears:

Service decommissioning cannot be scheduled if the selected services count is greater than 25.

4. Select the **Decommission now** option button to decommission the services immediately. You can also decommission the selected services later by selecting the **Decommission later** option button and setting the preferred date and time.



5. Click **OK** to decommission the selected services.

The **Job Details** window appears with a list of job IDs.

NOTE: For every service that is selected to be decommissioned, a unique job ID is assigned. You can view the details of each job on the **Job Management** page by clicking the corresponding job ID.

For every service that is decommissioned, a message is logged on the Audit Log page. To view the Audit Log page, select **Network Management Platform > Audit Logs > Audit Log**.

RELATED DOCUMENTATION

[Decommissioning a Service](#) | 834

Deleting Bulk Service Orders in Cross Provisioning Platform

Use the **Service Orders** landing page to select and delete multiple device configlet orders in bulk. You can select the number of services that a single page displays, by selecting one of the following values from the **Show items** drop-down list at the bottom of the page:

- 10
- 20
- 40
- 60
- 80
- 100
- 200

To delete service orders of Cross Provisioning Platform in bulk:

1. From the **Cross Provisioning Platform** task pane, select **CPP > Service Orders**.

The **Service Orders** page that appears displays a list of existing service orders.

2. Select the check boxes against the service orders that you want to delete.

3. Right-click and select **Delete Service Order** or click the **Delete Service Order** icon on the grid tool bar.

The **Delete Service Orders** page appears asking you to confirm the selection of the service orders to be deleted.

NOTE: When you select multiple service orders, the **Delete Service Order** option is enabled only if the order state of the selected service orders is either **Failed_Deployed**, **Requested** or **Invalid**.

When the order state is **Completed**, the following points hold true:

- You cannot delete a service order if its order state is **Completed** and the related service is listed on the **Services** landing page.
- You cannot delete the first and the last service order created for a service if their order state is **Completed** and the related service is listed on the **Services** landing page.
- The service orders that are in the **Completed** state for a service can be deleted only if the related service is not listed on the **Services** landing page.

You can delete 25 service orders at a time. If the count exceeds 25, the following error message appears:

Service orders cannot be deleted if the selected service order count is greater than 25.

The screenshot shows the 'Service Orders' page in the Cross Provisioning Platform. A table lists various service orders with columns for Name, External ID, Order State, Order Type, and Service Type. A context menu is open over the row with Name 'SO380523' and External ID 'vpks_test', showing options like 'View Pending Order Configuration', 'Deploy Service Order', 'Delete Service Order', 'Recreate Service Order', 'Cancel Order', 'Delete Private Tags', 'Tag It', 'UnTag It', 'View Tags', and 'Clear All Selections'. The 'Delete Service Order' option is highlighted.

Name	External ID	Order State	Order Type	Service Type
SO379543352_1426670300820	A534	Failed_Deployed	MODIFY	PW-LDP
SO379742463_1426665661321	Local	Failed_Deployed	MODIFY	PW-LDP
p2p_error	p2p_error	Failed_Deployed	ADD	PW-LDP
SO380601172	dsfsdfsdf	Completed	ADD	L3VPN
SO380569459	kav_l3vn_test	Failed_Deployed	ADD	L3VPN
SO380567194	VPLS_ge138	Completed	ADD	VPLS
SO380545694	l3vpn_kav	Completed	ADD	L3VPN
l3vpn_2Decomm2015-03-17 10:45:27.443	l3vpn_2	Completed	DELETE	L3VPN
SO380543013	vpks_test	Failed_Deployed	ADD	VPLS
SO380523	vpks_test	Failed_Deployed	ADD	L3VPN
SO379754		Completed	MODIFY	PW-LDP
SO379754		Completed	ADD	PW-LDP
SO379752		Completed	ADD	PW-LDP
SO379748		Completed	MODIFY	PW-LDP
SO379748		Completed	ADD	PW-LDP
SO379719		Invalid	MODIFY	VPLS
SO379719 12:30:25.0		Completed	AUDIT	VPLS
SO379742		Completed	MODIFY	PW-LDP
SO379742		Completed	ADD	PW-LDP
SO379719 12:14:01.4		Completed	AUDIT	VPLS
SO379570116Decomm2015-03-16 12:00:11.763		Completed	DELETE	PW-LDP
SO379719168_audit_2015-03-16 11:57:01.564	test34	Completed	AUDIT	VPLS

4. Click **Delete** to delete the selected service orders.

The selected service orders are deleted and the landing grid is refreshed. For every service order that is deleted, a message is logged on the **Audit Log** page. To view the Audit Log page, select **Network Management Platform > Audit Logs > Audit Log**.

RELATED DOCUMENTATION

| [Deleting Bulk Device Configlet Orders in Cross Provisioning Platform](#) | 802

26

CHAPTER

Deployed Services

[Viewing Services | 832](#)

[Editing a Service Name | 834](#)

[Decommissioning a Service | 834](#)

[Modifying a Full Mesh Layer 3 VPN Ethernet Service | 837](#)

[Modifying a Multipoint-to-Multipoint Ethernet Service | 844](#)

[Modifying a Point-to-Multipoint Ethernet Service | 855](#)

[Modifying a Point-to-Point Ethernet Service | 871](#)

[Modifying a Service in Cross Provisioning Platform | 873](#)

[Understanding Service Validation | 875](#)

[Service Troubleshooting Overview | 875](#)

[Troubleshooting Services in Cross Provisioning Platform | 876](#)

Viewing Services

The following topic describes how to view services:

- [Viewing Services in a Table | 832](#)

Viewing Services in a Table

To view the services inventory in a table:

1. In the **Network Activate** task pane, select **Service Provisioning > Manage Services**.

The Manage Services page presents information on existing services in a table.

The **Manage Services** page provides the following information about each service:

- Name—Unique name assigned to the service.
- Customer—Name of the customer for which the service is provided.
- State:
 - Deployed—Service does not exist until it is deployed.
 - Failed Deploy—An attempt to modify the service failed.
- Status:
 - Up—Service passed functional audit.
 - Down—Service failed functional audit.
- Definition—Service definition on which the service is based.
- Activation Date—Date and time the service was activated.
- Last Modified Date—Date and time at which the service was last modified.

Service Provisioning > **Manage Services**

0 Actions ▾

Name	Customer	State	FA Status	Fault Status	PM Status
VPLS_SO_withST	October	✓ Deployed	Pending	Up	None
SO_ELine-BGP-Dot1q-SingleVLAN_bulk_2	October	✓ Deployed	Pending	None	None
SO_ELine-BGP-Dot1q-SingleVLAN_bulk_1	October	✓ Deployed	Pending	Down	None
LVPN_SO1	October	✓ Deployed	Pending	Up	None
VPLSSO_1	October	✓ Deployed	Down	Up	None
P2P_QinQ_ALL_V...	October	✓ Deployed	Down	None	None
cfm_p2p_test	October	✓ Deployed	Up	Up	None

Page 1 of 1 | Displaying 1 - 7 of 7 | Show 30 items

2. 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.
3. To view details of a specific service, double-click the table row that summarizes the service. For a point-to-point Ethernet service, a graphical illustration of the service appears. See [“Creating a Point-to-Point Service Order” on page 586](#) for information about interpreting this graphic and obtaining additional information.

For a VPLS service (point-to-multipoint or multipoint-to-multipoint), a table of service details appears. See [“Creating a Point-to-Multipoint VPLS Service Order” on page 678](#) and [“Creating a Multipoint-to-Multipoint VPLS Service Order” on page 660](#) for information about interpreting this graphic.

RELATED DOCUMENTATION

- [Understanding Service Validation | 875](#)
- [Decommissioning a Service | 834](#)
- [Modifying a Point-to-Point Ethernet Service | 871](#)
- [Modifying a Multipoint-to-Multipoint Ethernet Service | 844](#)
- [Modifying a Point-to-Multipoint Ethernet Service | 855](#)

[Viewing Service Orders | 620](#)[Deploying a Service Order | 631](#)

Editing a Service Name

You can edit the name of a deployed service. This is applicable only to LDP based pseudowires.

To rename a service:

1. Select **Network Activate > Service Provisioning > Manage Services**.
2. In the Manage Services inventory page, select the service you want to rename.
3. Open the Actions drawer and select **Service > Edit Name**. The **Edit Service Name** window appears.

NOTE: The **Edit Name** appears to be dimmed if the service selected is BGP based point-to-point service, or VPLS service or L3VPN service.

4. Type the new name in the **Enter New name** fields and click **Save**.

The service is renamed.

RELATED DOCUMENTATION

[Decommissioning a Service | 834](#)

[Modifying a Full Mesh Layer 3 VPN Ethernet Service | 837](#)

[Modifying a Multipoint-to-Multipoint Ethernet Service | 844](#)

[Modifying a Point-to-Multipoint Ethernet Service | 855](#)

[Modifying a Point-to-Point Ethernet Service | 871](#)

Decommissioning a Service

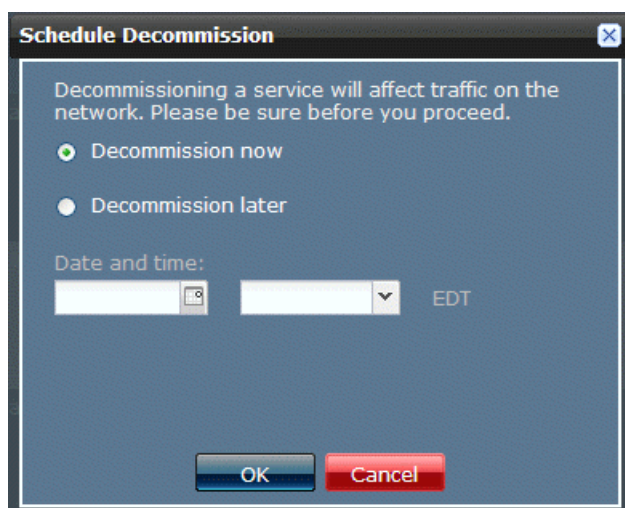
You can decommission a service that a customer no longer needs.

You cannot decommission a service if a service order requesting action on that service is in the Requested, Scheduled, In Progress, or Invalid state.

To decommission a service:

1. In the **Network Activate** task pane, select **Service Provisioning > Manage Services**.
2. In the **Manage Services** page, select the service you want to decommission.
3. Open the **Actions** menu and click **Decommission Service**.

The **Schedule Decommission** window appears.



4. 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.

- To deploy the service at a later time, select **Decommission later**, select a date and time to perform the operation, then click **OK**.

NOTE: The following error message is displayed if you decommission a service that has more number of devices or endpoints than the specified limit:

Decommission of service cannot be performed due to more number of devices or endpoints. Please modify the service and remove few devices or endpoints before decommissioning the whole service. (Maximum of 100 devices or 250 endpoints are only allowed)

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 Network Activate row and select **Modify Applications Settings**. The Modify Network Activate 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 Jobs in the Junos Space Network Application Platform User Guide

[Viewing Services](#) | 832

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 756](#).

Modifying a service creates a new service order based on the attribute settings of the existing service.

- [Adding an Endpoint | 837](#)
- [Adding a UNI Interface | 841](#)
- [Deleting a UNI Interface and Deleting an Endpoint | 843](#)

Adding an Endpoint

To add an endpoint to a multipoint-to-multipoint Ethernet service:

1. In the **Network Activate** 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. Open the **Actions** menu and select **Modify Service**.

The **Modify Service** page appears.

Service Provisioning > Manage Services > **Modify**

Modify Service

General Information

Order name: l3vpn_test-SO_modify_2012-10
Customer: Tata
Service name: l3vpn_test-SO
Service definition: l3vpn_test
Comments:

Add Endpoints

Device	UNI Interface	Action
Device: junos-m10-1-space (1 Item)		
junos-m10-1-space	ge-0/0/1	✖
Device: junos-m10-2-space (1 Item)		
junos-m10-2-space	ge-0/0/3	✖

Device: junos-m10-1-space Save Add More

Ethernet option: VLAN
UNI interface: ge-0/0/1
Interface IP address: 10.0.77.49
VLAN ID: 200

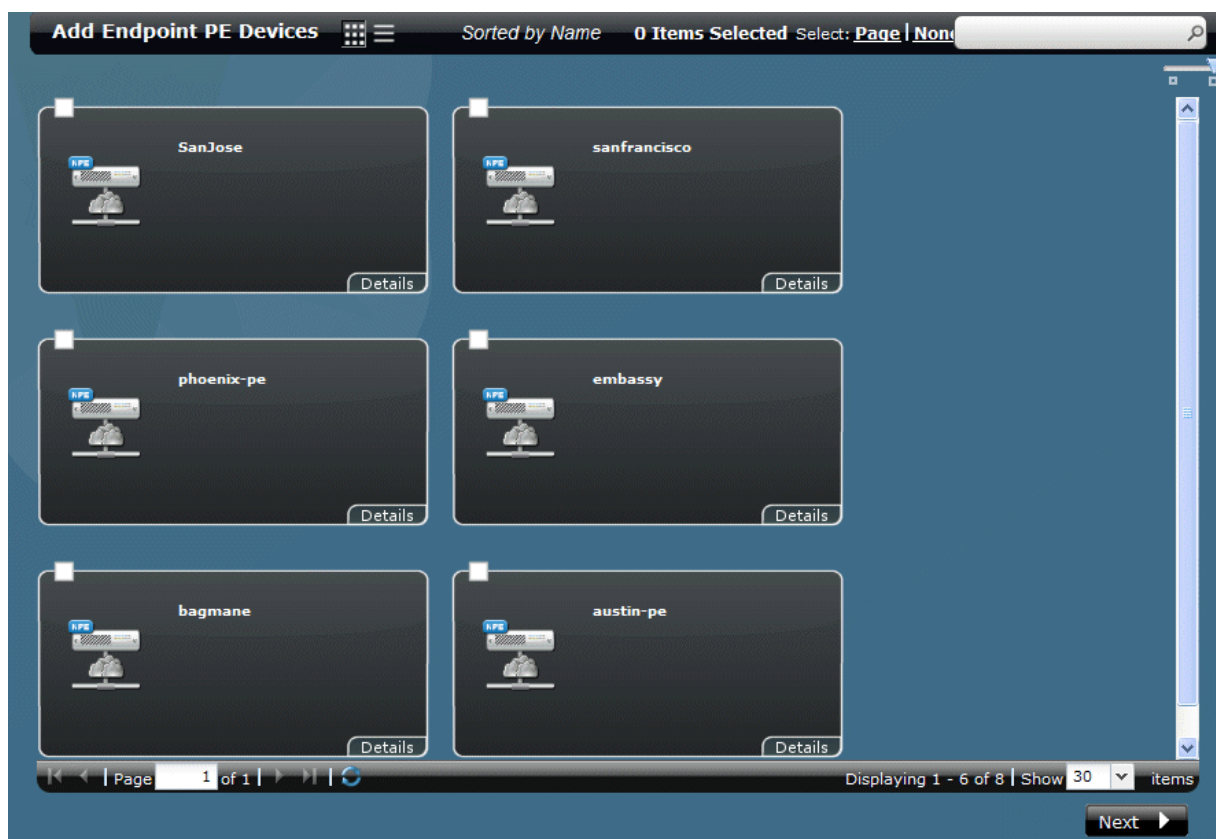
Routing Protocol Settings
Routing protocol: OSPF

Modify Cancel

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. In the **Add Endpoints** table, click **Add Endpoints**.

When you click a device UNI interface, you see the device and routing protocol settings in the right **Device** pane. The **Add Endpoint PE Devices** inventory page shows the available N-PE devices that are not part of the service.

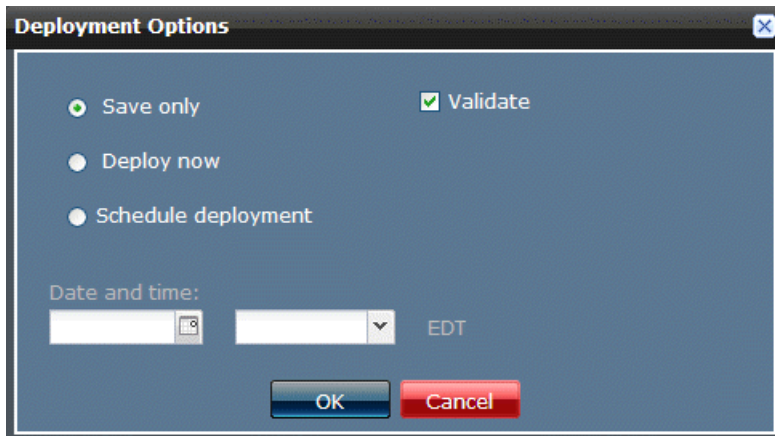


6. Select the devices on which you want to add new endpoints, and then click **Next**.

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 841](#).

7. Click **Modify**.

The **Deployment Options** dialog box appears.



8. In the **Deployment Options** dialog box, select one of the following:

- **Save only** and check **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.

9. Click **OK**.

The service modification deployment Job ID link appears.

10. Click the Job ID.

You see the service modification deployment job details in the **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.

Job Management > Manage Jobs

ID	Name	Percent	State	Job Type	Summary	Sched...	User
196608	Discover Network Elements-196608	75.0	CANCELLED	Discover Network Elements	Job was cancelled by user	Oct 8, 2012 1:45:44 AM EDT	super
196616	Resync Network Elements-196616	0.0	CANCELLED	Resync Network Elements	[Resync job is not required for device junos-mx80-2-space as there are no detecta... configu... change...	Oct 8, 2012 1:50:14 AM EDT	
197219	Resync Network Elements-197219	0.0	CANCELLED	Resync Network Elements	[Resync job is not required for device junos-space5 as there are no detecta... configu...	Oct 8, 2012 6:38:52 AM EDT	

Page 1 of 323 | Displaying 1 - 30 of 9665 | Show 30 items

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 Activate** 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. 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.

- In the **Action** column of the **Endpoint Settings** table, click the green plus sign for the device that you want. An additional UNI appears in the endpoint table for the device. The UNI interface settings fields appear in the **Device** pane on the right.

Service Provisioning > Manage Services > **Modify**

Modify Service

General Information

Order name: l3vpn_test-SO_modify_2012-10

Customer: Tata

Service name: l3vpn_test-SO

Service definition: l3vpn_test

Comments:

Add Endpoints

Device	UNI Interface	Action
Device: junos-m10-1-space (1 Item)		
junos-m10-1-space	ge-0/0/1	✖
Device: junos-m10-2-space (2 Items)		
junos-m10-2-space	ge-0/0/3	✖
junos-m10-2-space	Please select...	✖

Device: junos-m10-2-space Save Add More

Ethernet option: VLAN

UNI interface: Please select...

Autopick interface IP: ☒

IP pool type: Global

IP address pool: Please select ...

IP block size: 28

Modify Cancel

- In the **Device** pane, select an **Ethernet option** from the drop-down list box.
- Select a **UNI interface** from the drop-down list box.
- The **Interface IP** field displays the interface IP address.
- 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.
- Select a routing protocol from the drop-down list box.
- Click **Modify**.
- Click **Modify**.

The **Deployment Options** dialog box appears.

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 **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.

Deleting a UNI Interface and Deleting an Endpoint

To delete a UNI from a multipoint-to-multipoint Ethernet service:

1. In the **Network Activate** 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. 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. In the **Action** column of the **Endpoint Settings** table, find the UNI you want to delete and click the red delete button for that 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.

6. Click **Modify**.

The **Deployment Options** dialog box appears.

7. 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.

8. Click **OK**.

The service modification deployment Job ID link appears.

9. Click the Job ID.

You see the service modification deployment job details in the **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.

To view the modified service in the network topology, select **Platform > Network Monitoring > Topology > Service > NA**. The parameters of the selected service is displayed.

For more information on topology, see [“Junos Space Network Topology Overview” on page 31](#).

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.

The following topics provide instructions for modifying a multipoint-to-multipoint (full mesh) Ethernet service:

- [Adding an Endpoint | 845](#)
- [Adding a UNI Interface | 847](#)
- [Deleting a UNI Interface and Deleting an Endpoint | 849](#)
- [Changing the Endpoint Bandwidth | 850](#)
- [Changing the Primary Device in a Multihomed Group | 851](#)
- [Changing Advanced Settings for an Endpoint | 853](#)

Adding an Endpoint

To add an endpoint to a multipoint-to-multipoint Ethernet service:

1. In the Network Activate 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. Open the **Actions** menu and select **Modify Service**.

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.

Service Provisioning > Manage Services > **Modify**

Modify Service

General Information

Order name: testl3vpn_modify_2012-10-26
 Customer: Tata
 Service name: testl3vpn
 Service definition: L3VPN-BGP-Static
 Comments:

Add Endpoints

Device	UNI Interface	Action
Device: junos-mx80-1-space (1 Item)		
junos-mx80-1-space	ge-1/2/9	
Device: junos-mx80-2-space (1 Item)		
junos-mx80-2-space	ge-1/2/9	

Device: junos-mx80-1-space [Save](#) [Add More](#)

Ethernet option: VLAN
 UNI interface: ge-1/2/9
 Interface IP address: 10.0.88.1
 VLAN ID: 3

Routing Protocol Settings
 Routing protocol: BGP

[Modify](#) [Cancel](#)

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 Information** 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 Information** panel provides an option to enable the CFM service. You can select the CFM definition from the **CFM Definition** list, if desired.
6. In the **Add Endpoints** table, click **Add Endpoints**.
 The **Add Endpoint PE Devices** window shows available N-PE devices that are not part of the service.
7. Select the devices on which you want to add new endpoints, then click **Next**.
 The service modification window shows the added devices with system recommended choices for UNI.
8. Click **Modify**.
9. 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.

10. Click **OK**.

11. Use the **Job Management** workspace to monitor the progress and status of the deployment. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details.

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 Activate 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. Open the **Actions** menu and select **Modify Service**.

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. In the **Action** column of the **Add Endpoints** table, click **UNI Interface** for the device, as shown in the following example, which adds a UNI to the device.

Service Provisioning > Manage Services > **Modify**

Modify Service

General Information

Order name: testl3vpn_modify_2012-10-26
 Customer: Tata
 Service name: testl3vpn
 Service definition: L3VPN-BGP-Static
 Comments:

Add Endpoints

Device	UNI Interface	Action
Device: junos-mx80-1-space (2 Items)		
junos-mx80-1-space	ge-1/2/9	
junos-mx80-1-space	Please select...	
Device: junos-mx80-2-space (1 Item)		
junos-mx80-2-space	ge-1/2/9	

Device: junos-mx80-1-space [Save](#) [Add More](#)

Ethernet option: VLAN
 UNI interface: Please select...
 Autopick interface IP: ☒
 IP pool type: Global
 IP address pool: Please select ...
 IP block size: 30

[Modify](#) [Cancel](#)

An additional UNI appears in the endpoint table.

6. 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.
7. Select an interface from the UNI Interface column.
8. Click **Modify**.
9. In the **Deployment Options** window, select one of the following options:
 - Save the change without scheduling it.
 - Schedule the change for immediate deployment.
 - Schedule the change for later deployment.
10. Click **OK**.
11. Use the **Job Management** workspace to monitor the progress and status of the deployment. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details.

Deleting a UNI Interface and Deleting an Endpoint

To delete a UNI from a multipoint-to-multipoint Ethernet service:

1. In the Network Activate 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. Open the **Actions** menu and select **Modify Service**.

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. In the **Action** column of the **Endpoint Settings** table, find the UNI you want to delete and click **Delete UNI Interface** for that table row.

Add Endpoints							
Device	UNI Interface	Description	Bandwidth	AutoPick VL...	VLAN ID	MTU (Bytes)	Action
<input checked="" type="checkbox"/> Hub	Device: junos-mx240-space (1 Interface)						Add UNI Interface Advanced
junos-mx240-space	ge-0/2/5		10 Mbps	<input type="checkbox"/>	103	1522	Delete UNI Interface
<input type="checkbox"/> Hub	Device: junos-mx480-space (1 Interface)						Add UNI Interface Advanced
junos-mx480-space	ge-5/0/1		10 Mbps	<input type="checkbox"/>	103	1522	Delete UNI Interface

Modify

Cancel

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.

6. Click **Modify**.
7. 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.
8. Click **OK**.
 9. Use the **Job Management** workspace to monitor the progress and status of the deployment. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details.

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 Activate task 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 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. In the **Action** column of the **Endpoint Settings** table, click on the **Bandwidth** entry for the UNI on which you want to change the bandwidth.

Device	UNI Interface	Description	Bandwidth	AutoPick VL...	VLAN ID	MTU (Bytes)	Action
junos-mx240-space	ge-0/2/5	Device: junos-mx240-space (1 Interface)	10 Mbps		103	1522	Delete UNI Interface
junos-mx480-space	ge-5/0/1	Device: junos-mx480-space (1 Interface)	20 Mbps		103	1522	Delete UNI Interface

6. From the list of valid bandwidth settings, select the setting you want, then click **Modify**.
7. 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.
8. Click **OK**.
9. Use the **Job Management** workspace to monitor the progress and status of the deployment. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details.

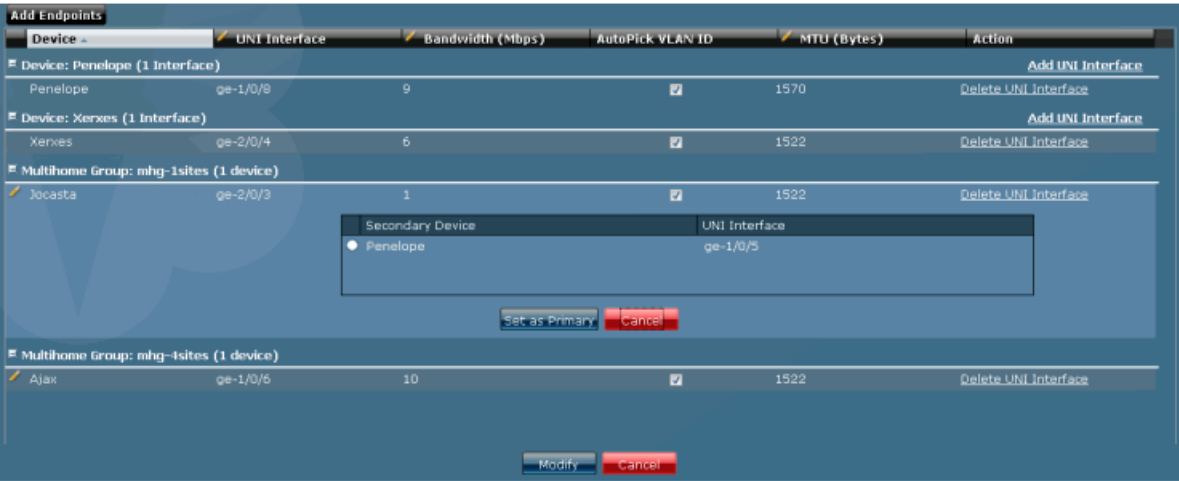
Changing the Primary Device in a Multihomed Group

To change the primary device in a multihomed group in a multipoint-to-multipoint Ethernet service:

1. In the Network Activate task pane, select **Service Provisioning > Manage Services**.
2. In the **Manage Services** page, select the service on which you want to change the primary device in a multihomed group.
3. Open the **Actions** menu and select **Modify Service**.

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 modified service order, if desired.
5. To select a different primary device for the multihomed group, in the **Endpoint Settings** box, click the Edit icon (indicated by a pencil), located to the left of the current primary device for the multihomed group.
6. Select the radio button for the secondary device that you want to specify as the primary device in the multihomed group.



7. Click **Set As Primary**.
 8. Click **Modify**.
- The secondary device is configured as the primary device in the multihomed group.
9. 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.
 10. Click **OK**.
 11. Use the **Job Management** workspace to monitor the progress and status of the deployment. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details.

Advanced Setting: junos-mx240-space

MAC Security Settings

☒ MAC learning

Interface MAC limit:

☐ MAC statistics

MAC table size:

See the ["Service Attributes Overview"](#) on page 152 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 **Modify**.

14. 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.

15. Click **OK**.

16. Use the **Job Management** workspace to monitor the progress and status of the deployment. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details.

To view the modified service in the topology, select **Platform > Network Monitoring > Topology > Service > NA**. The parameters of the selected service is displayed.

For more information on topology, see [“Junos Space Network Topology Overview” on page 31](#)

RELATED DOCUMENTATION

[Creating a Multipoint-to-Multipoint VPLS Service Order | 660](#)

[Deploying a Service Order | 631](#)

[Viewing Jobs in the Junos Space Network Application Platform User Guide](#)

[Viewing Services | 832](#)

[Modifying a Point-to-Point Ethernet Service | 871](#)

[Modifying a Point-to-Multipoint Ethernet Service | 855](#)

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:

- [Adding a Spoke | 856](#)
- [Adding a Hub | 858](#)
- [Changing a Spoke to a Hub | 860](#)
- [Changing a Hub to a Spoke | 861](#)
- [Adding a UNI Interface | 862](#)
- [Deleting a UNI Interface or Deleting an Endpoint | 864](#)
- [Changing the Endpoint Bandwidth | 866](#)
- [Changing the Primary Device in a Multihomed Group | 867](#)
- [Changing Advanced Settings for an Endpoint | 868](#)

Adding a Spoke

To add an endpoint configured as a spoke to a multipoint Ethernet service:

1. In the Network Activate task 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. 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.

Service Provisioning > Manage Services > **Modify**

General Settings

Order name: VPLS_HS_Demo_1_modify_2012-11-13 20:04:31.111

Customer: Coke Inc..

Service name: VPLS_HS_Demo_1

Service definition: ELAN-Hub-Spoke-QinQ-AllVLAN

Comments:

Signaling: BGP

CFM Definition: Please select ...

Add Endpoints

Device	UNI Interface	Description	Bandwidth	AutoPick VL...	VLAN ID	MTU (Bytes)	Action
Hub Device: junos-mx240-space (1 Interface) Add UNI Interface Advanced							
junos-mx240-space	ge-0/2/5		10 Mbps	<input type="checkbox"/>	103	1522	Delete UNI Interface
Hub Device: junos-mx480-space (1 Interface) Add UNI Interface Advanced							
junos-mx480-space	ge-5/0/1		10 Mbps	<input type="checkbox"/>	103	1522	Delete UNI Interface

Modify Cancel

- In the service **Order name** field, change the name of the modification service order, if desired.
- 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 **CFM Definition** list, if desired.
- In the **Endpoint Settings** table, click **Add Endpoints**.
The **Add Endpoint PE Devices** window shows available N-PE devices that are not part of the service.
- 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 862](#). To select a different bandwidth than the applied default, see [“Changing the Endpoint Bandwidth” on page 866](#).

8. Click **Modify**.
9. 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.
10. Click **OK**.
11. Use the **Job Management** workspace to monitor the progress and status of the deployment. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details.

Adding a Hub

To add an endpoint to a multipoint Ethernet service:

1. In the Network Activate task pane, select **Service Provisioning > Manage Services**.
2. In the **Manage Services** page, select the service to which you want to add a hub.
3. Open the **Actions** menu and select **Modify Service**.

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.

Service Provisioning > Manage Services > **Modify**

Modify Service

General Information

Order name: testl3vpn_modify_2012-10-26 2
 Customer: Tata
 Service name: testl3vpn
 Service definition: L3VPN-BGP-Static
 Comments:

Add Endpoints

Device	UNI Interface	Action
Device: junos-mx80-1-space (1 Item)		
junos-mx80-1-space	ge-1/2/9	
Device: junos-mx80-2-space (1 Item)		
junos-mx80-2-space	ge-1/2/9	

Device: junos-mx80-1-space **Save** **Add More**

Ethernet option: VLAN
 UNI interface: ge-1/2/9
 Interface IP address: 10.0.88.1
 VLAN ID: 3

Routing Protocol Settings

Routing protocol: BGP

Modify **Cancel**

4. In the service **Order name** field, change the name of the modification service order, if desired.
5. In the **Endpoint Settings** table, click **Add Endpoints**.
 The **Add Endpoint PE Devices** window shows available N-PE devices that are not part of the service.
6. 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 862](#). To select a different bandwidth than the applied default, see [“Changing the Endpoint Bandwidth” on page 866](#).
7. In the **Endpoint Settings** table, check **Hub** for the device you just added.
8. Click **Modify**.
9. 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.

10. Click **OK**.

11. Use the **Job Management** workspace to monitor the progress and status of the deployment. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details.

Changing a Spoke to a Hub

To change a spoke to a hub in a point-to-multipoint Ethernet service:

1. In the Network Activate task 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. 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. 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.

Add Endpoints			
Device	UNI Interface	Description	Bandwidth
<input checked="" type="checkbox"/> Hub	Device: junos-mx240-space (1 Interface)		
junos-mx240-space	ge-0/2/5		10 Mbps
<input checked="" type="checkbox"/> Hub	Device: junos-mx480-space (1 Interface)		
junos-mx480-space	ge-5/0/1		10 Mbps

6. Click **Modify**.
7. 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.

8. Click **OK**.
9. Use the **Job Management** workspace to monitor the progress and status of the deployment. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details.

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 Activate task 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. 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. In the **Device** column of the **Endpoint Settings** table, find the hub endpoint you want to change to a spoke and clear the **Hub** check box.

Add Endpoints			
Device	UNI Interface	Description	Bandwidth
<input type="checkbox"/> Hub	Device: junos-mx240-space (1 Interface)		
junos-mx240-space	ge-0/2/5		10 Mbps
<input checked="" type="checkbox"/> Hub	Device: junos-mx480-space (1 Interface)		
junos-mx480-space	ge-5/0/1		10 Mbps

6. Click **Modify**.
7. 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.
8. Click **OK**.
 9. Use the **Job Management** workspace to monitor the progress and status of the deployment. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details.

Adding a UNI Interface

To add a UNI on a device that is already part of a multipoint Ethernet service:

1. In the Network Activate 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. 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. In the **Action** column of the **Endpoint Settings** table, click **Add UNI Interface** for the device, as shown in the following example, which adds a UNI to the device named SanFrancisco.

Add Endpoints

Device	UNI Interface	Description	Bandwidth	AutoPick VL...	VLAN ID	MTU (Bytes)	Action
<div><div>Hub</div><div>Device: junos-mx240-space (1 Interface)</div><div>Add UNI InterfaceAdvanced</div></div>							
junos-mx240-space	ge-0/2/5		10 Mbps	<input type="checkbox"/>	103	1522	Delete UNI Interface
<div><div>Hub</div><div>Device: junos-mx480-space (2 Interfaces)</div><div>Add UNI InterfaceAdvanced</div></div>							
junos-mx480-space	ge-5/0/1		10 Mbps	<input type="checkbox"/>	103	1522	Delete UNI Interface
junos-mx480-space	Please select...		10 Mbps	<input checked="" type="checkbox"/>		1522	Delete UNI Interface

Modify

Cancel

An additional UNI appears in the endpoint table.

6. Select an interface from the UNI Interface column.

Add Endpoints

Device	UNI Interface	Description	Bandwidth	AutoPick VL...	VLAN ID	MTU (Bytes)	Action
<div><div>Hub</div><div>Device: junos-mx240-space (1 Interface)</div><div>Add UNI InterfaceAdvanced</div></div>							
junos-mx240-space	ge-0/2/5		10 Mbps	<input type="checkbox"/>	103	1522	Delete UNI Interface
<div><div>Hub</div><div>Device: junos-mx480-space (2 Interfaces)</div><div>Add UNI InterfaceAdvanced</div></div>							
junos-mx480-space	ge-5/0/1		10 Mbps	<input type="checkbox"/>	103	1522	Delete UNI Interface
junos-mx480-space	xe-0/0/0		10 Mbps	<input checked="" type="checkbox"/>		1522	Delete UNI Interface

Modify

Cancel

7. 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.

8. Click **Modify**.

9. 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.
10. Click **OK**.
11. Use the **Job Management** workspace to monitor the progress and status of the deployment. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details.

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 Activate 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. 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. In the **Action** column of the **Endpoint Settings** table, find the UNI you want to delete and click **Delete UNI Interface** for that table row.

Add Endpoints							
Device	UNI Interface	Description	Bandwidth	AutoPick VL...	VLAN ID	MTU (Bytes)	Action
<div> <div>Hub</div> <div>Device: junos-mx240-space (1 Interface)</div> <div>Add UNI Interface Advanced</div> </div>							
junos-mx240-space	ge-0/2/5		10 Mbps	<input type="checkbox"/>	103	1522	Delete UNI Interface
<div> <div>Hub</div> <div>Device: junos-mx480-space (2 Interfaces)</div> <div>Add UNI Interface Advanced</div> </div>							
junos-mx480-space	ge-5/0/1		10 Mbps	<input type="checkbox"/>	103	1522	Delete UNI Interface
junos-mx480-space	xe-0/0/0		10 Mbps	<input checked="" type="checkbox"/>		1522	Delete UNI Interface
junos-mx480-space	xe-0/0/0						
<div> <div>Modify</div> <div>Cancel</div> </div>							

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.

- Click **Modify**.
- 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.
- Click **OK**.
- Use the **Job Management** workspace to monitor the progress and status of the deployment. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* in the Junos Space Network Application Platform User Guide for details.

Changing the Endpoint Bandwidth

To change the rate limit or bandwidth for an endpoint of a multipoint Ethernet service:

1. In the Network Activate task 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. In the **Action** column of the **Endpoint Settings** table, click on the Bandwidth entry for the UNI on which you want to change the bandwidth.

Device	UNI Interface	Description	Bandwidth	AutoPick VL...	VLAN ID	MTU (Bytes)	Action
Device: junos-mx240-space (1 Interface)	ge-0/2/5		10 Mbps	<input type="checkbox"/>	103	1522	Delete UNI Interface
Device: junos-mx480-space (2 Interfaces)	ge-5/0/1		10 Mbps	<input type="checkbox"/>	103	1522	Delete UNI Interface
Device: junos-mx480-space	xe-0/0/0		40 Mbps	<input checked="" type="checkbox"/>		1522	Delete UNI Interface

Modify Cancel

6. From the list of valid bandwidth settings, select the one you want, then click **Modify**.
7. 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.

8. Click **OK**.
9. Use the **Job Management** workspace to monitor the progress and status of the deployment. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* in the Junos Space Network Application Platform User Guide for details.

Changing the Primary Device in a Multihomed Group

To change the primary device in a multihomed group in a point-to-multipoint Ethernet service:

1. In the Network Activate task pane, select **Service Provisioning** > **Manage Services**.
2. In the **Manage Services** page, select the service on which you want to change the primary device in a multihomed group.
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 modified service order, if desired.
5. To select a different primary device for the multihomed group, in the **Endpoint Settings** box, click the Edit icon (indicated by a pencil), located to the left of the current primary device for the multihomed group.
6. Select the radio button for the secondary device that you want to specify as the primary device in the multihomed group.

Device	UNI Interface	Bandwidth (Mbps)	AutoPick VLAN ID	MTU (Bytes)	Action
Device: Penelope (1 Interface)					
Penelope	ge-1/0/8	9	<input checked="" type="checkbox"/>	1570	Delete UNI Interface
Device: Xerxes (1 Interface)					
Xerxes	ge-2/0/4	6	<input checked="" type="checkbox"/>	1522	Delete UNI Interface
Multihome Group: mhq-1sites (1 device)					
Jocasta	ge-2/0/3	1	<input checked="" type="checkbox"/>	1522	Delete UNI Interface
<div> <div>Secondary Device</div> <div> <input checked="" type="radio"/> Penelope <input type="radio"/> Xerxes <input type="radio"/> Jocasta </div> <div>UNI Interface</div> <div>ge-1/0/8</div> </div> <div> Set as Primary Cancel </div>					
Multihome Group: mhq-1sites (1 device)					
Ajax	ge-1/0/5	10	<input checked="" type="checkbox"/>	1522	Delete UNI Interface

[Modify](#)
[Cancel](#)

7. Click **Set As Primary**.

8. Click **Modify**.

The secondary device is configured as the primary device in the multihomed group.

9. 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.

10. Click **OK**.

11. Use the **Job Management** workspace to monitor the progress and status of the deployment. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details.

Changing Advanced Settings for an Endpoint

To change advanced settings for an endpoint of a point-to-multipoint Ethernet service:

1. In the Network Activate task 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. 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 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.

Add Endpoints

Device	UNI Interface	Description	Bandwidth	AutoPick VL...	VLAN ID	MTU (Bytes)	Action
<input checked="" type="checkbox"/> Hub	Device: junos-mx240-space (1 Interface)						Add UNI Interface Advanced
junos-mx240-space	ge-0/2/5		10 Mbps	<input type="checkbox"/>	103	1522	Delete UNI Interface
<input type="checkbox"/> Hub	Device: junos-mx480-space (1 Interface)						Add UNI Interface Advanced
junos-mx480-space	ge-5/0/1		10 Mbps	<input type="checkbox"/>	103	1522	Delete UNI Interface

Modify

Cancel

The **Advanced Setting** window displays the security and advanced settings that you can configure for a device.

Advanced Setting: junos-mx240-space

MAC Security Settings

☒ MAC learning

Interface MAC limit: 1024

☐ MAC statistics

MAC table size: 5120

OK

Cancel

See the [“Service Attributes Overview”](#) on page 152 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 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 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.
14. Click **OK**.
15. Use the **Job Management** workspace to monitor the progress and status of the deployment. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details.

To view the modified service in the topology, select **Platform > Network Monitoring > Topology > Service > NA**.

For more information on topology, see [“Junos Space Network Topology Overview” on page 31](#)

RELATED DOCUMENTATION

[Creating a Point-to-Multipoint VPLS Service Order | 678](#)

[Deploying a Service Order | 631](#)

Viewing Jobs in the *Junos Space Network Application Platform User Guide*

[Viewing Services | 832](#)

[Modifying a Point-to-Point Ethernet Service | 871](#)

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:

1. In the **Network Activate** task pane, select **Service Provisioning** > **Manage Services**.
2. In the **Manage Services** page, select the service you want to modify.
3. Open the **Actions** menu and select **Modify Service**.

A graphical image of the service appears, showing device images that represent the service endpoints and a cloud image that represents the network core. By default, the cloud image is selected, which displays general settings and connectivity information in the right panel. The General Settings box contains a unique name for the service order that will request the change.

Service Provisioning > Manage Services > **Modify**

Definition: ELine-QinQ-AllVLAN
Service Order Name: testp2p_modify_2012-10-26 20:43:13.718
Customer: Tata
Service Name: testp2p

General/Connectivity Settings

General Settings

Order name: testp2p_modify_2012-10-26 2

Comments:

Customer: Tata

Service name: testp2p

Service type: LDP

Service definition: ELine-QinQ-AllVLAN

Connectivity Settings

MTU: 1522

VCID: 2147467295

OAM Settings

CFM Definition: Please select ...

Back Next Modify Cancel

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 **CFM Definition** 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 Network Activate software modifies the service.

13. Use the **Job Management** workspace to check for successful completion of the action. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details.

To view the modified service in the topology, select **Platform > Network Monitoring > Topology > Service > NA**.

For more information on topology, see [“Junos Space Network Topology Overview” on page 31](#)

RELATED DOCUMENTATION

[Viewing Services | 832](#)

[Deploying a Service Order | 631](#)

[Creating a Point-to-Point Service Order | 586](#)

[Modifying a Multipoint-to-Multipoint Ethernet Service | 844](#)

[Modifying a Point-to-Multipoint Ethernet Service | 855](#)

Modifying a Service in Cross Provisioning Platform

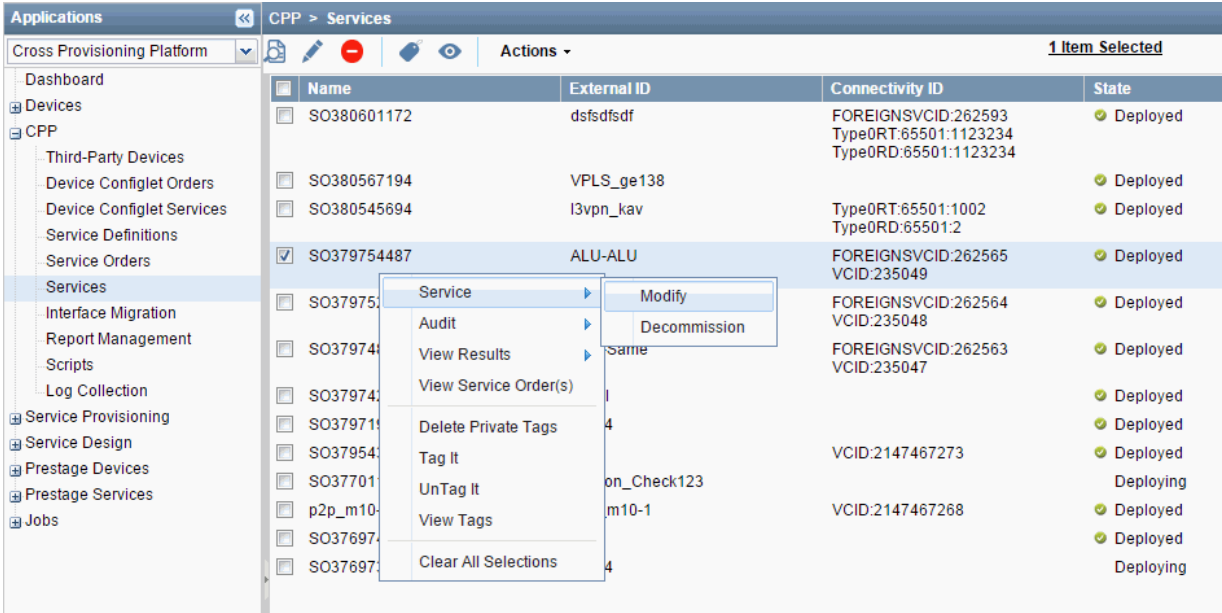
Use the **Device Configlet Services** landing page to modify a device configlet service in Cross Provisioning Platform. You can modify a device configlet service only if a modification script is attached to the device configlet service.

To modify a service in Cross Provisioning Platform:

1. From the **Cross Provisioning Platform** task pane, select **CPP > Services**.

The **Services** page that appears displays a list of existing services.

2. Either select **Service > Modify** or select a service and click the **Modify** icon on the grid tool bar. You can also modify a service by selecting the service and then selecting **Actions > Modify**.



The **Modify Service** page appears.

NOTE: The **Modify Service** page details vary according to the type of the selected service.

- 3. Modify the service details and click **Modify**.
The **Job Details** dialog box appears along with a job ID link.
- 4. Click the **Job ID** link to view the job details.
The **Job Management** page that appears contains a list of the jobs, along with the status of the jobs.

RELATED DOCUMENTATION

Modifying Bulk Services and Devices in Cross Provisioning Platform | 816

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 1064](#)
- [Performing a Configuration Audit on page 1062](#)

RELATED DOCUMENTATION

[Viewing Functional Audit Results | 1081](#)

[Viewing Configuration Audit Results | 1078](#)

[Service Troubleshooting Overview | 875](#)

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
See [“Performing a Functional Audit” on page 1064](#)
- Configuration audit
See [“Performing a Configuration Audit” on page 1062](#)
- Job Management
See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide*

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.

Job Management > Manage Jobs										
<input type="text"/> Actions ▾										
ID	Name	Per...	State	Job T...	Summary	Sche...	Act...	End...	User	R...
1545606	cfm_p2p_testFunctional Audit	100.0	✖ FAIL...	Monit... Audit	No Results from DeliveryEn...	Oct 30, 2012 3:49: PM EDT	Oct 30, 2012 3:4 PM EDT	Oct 30, 2012 3:4 PM EDT	super	

RELATED DOCUMENTATION

[Viewing Configuration Audit Results | 1078](#)

[Viewing Functional Audit Results | 1081](#)

[Resynchronizing Managed Devices with the Network](#)

[Understanding Service Validation | 875](#)

[Canceling a Job](#)

Troubleshooting Services in Cross Provisioning Platform

IN THIS SECTION

● [Troubleshooting Cross Provisioning Platform Services Using Operational Scripts | 878](#)

● [Troubleshooting Cross Provisioning Platform Services Using CLI Configlet Scripts | 880](#)

The troubleshooting feature provides an easy and unique way to troubleshoot the services in Cross Provisioning Platform. You do not have to manually login to a device to check the status of services in the Cross Provisioning Platform application, but you can do the same using the functionality of operational scripts and CLI configlet 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 and the CLI configlet scripts need to be created or imported to the platform from the local machine before you start troubleshooting the services in the Cross Provisioning Platform application.

The following table lists the context in which the OP scripts and CLI configlets are written for different types of services:

Table 37: OP Scripts and 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="30.128"]/interface[name="ge-0/1/5.784"]
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-1/2/2.1881"]

Table 37: OP Scripts and CLI Configlets Contexts for Different Service Types (*continued*)

Service Type	Context
NPS (Network peering)	/* @CONTEXT = "/device/configuration/protocols/bgp/group" */ Example /device[name="MX80-1"]/configuration/protocols/bgp/group[type="external"]

The following are the options to troubleshoot the services in the Cross Provisioning Platform application:

Troubleshooting Cross Provisioning Platform Services Using Operational Scripts

The operational scripts or the OP scripts are written to view the statistics of a service in the Cross Provisioning Platform 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 37 on page 877](#).

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 **Cross Provisioning Platform** task pane, select **CPP > Services**.

The **Services** page that appears displays a list of the services in Cross Provisioning Platform.

7. Double-click any service.

The **CPP Services Details** page that appears displays a list of the devices associated with the service you selected.

You can view the advanced details of any device in the **Advanced Details For Device** section by clicking the device from the list.

8. Right-click any device from the list and select the **Execute OP Scripts** option.

9. Select an OP script on the **Execute OP Scripts** page.

Script Name	Description	Version	Created Date	Last Updated Date
op-p2p-ldp-troubleshoot.slax	Op Script to get l2circuit inf...	1	Nov 03, 2014 10:08:34 AM ...	Nov 03, 2014 10:08:34 AM ...

Enter Parameters for op-p2p-ldp-troubleshoot.slax		
Name	Description	Value
No parameters found		

NOTE: To enter the value for PARAMETERS, click on VALUE column. The value for parameters may be required.

Execute View Last Result Cancel

10. 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.

11. 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**.

12. Click **OK**.

You are redirected to the **Execute OP Scripts** page.

13. Click **View Last Result** to view the previous OP scripts execution results.

NOTE: This is an optional step.

Troubleshooting Cross Provisioning Platform Services Using CLI Configlet Scripts

The CLI configlet scripts are written to set the user-defined configuration to a device in which the cross provisioning platform services are installed. The commands in the CLI configlet scripts are user-defined. To view the contexts for writing CLI configlet scripts for different service types, refer [Table 37 on page 877](#). For more information on applying CLI configlet to devices, see *Junos Space Network Management Platform User Guide*.

The process of providing troubleshooting support to Cross Provisioning Platform services using the CLI configlet scripts is similar to that of the operational scripts. To execute the CLI configlet script and set the configuration to any device:

1. From the **Cross Provisioning Platform** task pane, select **CPP > Services** to view the **CPP Service Details** page.

The **CPP Service Details** page appears.

2. Right-click any device and select the **Execute CLI Configlet** option.

The **Apply CLI Configlet** page appears.

3. Select the **Select Device Manually** option.

CPP > Services > Execute CLI Configlet

Apply CLI Configlet

Device name: buxar
Entity name: buxar: 30.1.2.3: ge-0/0/0.255

View Context ☒ Select Manually ☐ Select by Tags

Name	Domain Name	Category	Description	Created Time	Last Updated Time	Reference Number
Disable Physical Interface	Global	Ops	Disable one or more selected physical interfaces. Interfaces can be selected from either the physical interface inventory view or from within the active configuration view. Supports one or more interfaces or devices.	2014-11-03 10:10:02.177	2014-11-04 11:41:03.357	

Device Entity Name Description Value

☐ Substitute the Information

Back Next Validate Apply Cancel

4. Select the devices onto which you need to apply the CLI configlet script.
5. Enter the required parameters in the **Value** column, besides the ones coded in the CLI configlet script.
6. Click **Next**.
A preview of the CLI configlet script is shown.
7. Click **Validate** to validate the CLI configlet script.
The **Validation Result** page appears showing the status of the validation.

RELATED DOCUMENTATION

- [Importing Scripts Created for Cross Provisioning Platform | 778](#)
- [Adding Scripts Created for Cross Provisioning Platform | 775](#)

27

CHAPTER

NEC iPASOLINK Management

Cross Provisioning Platform for iPASOLINK Devices Overview | **883**

Worldwide Junos OS Adapter Overview | **884**

Installing the Worldwide Junos OS Adapter | **885**

Device Discovery Profiles Overview | **887**

Creating a Device Discovery Profile | **889**

Running Device Discovery Profiles | **900**

Modifying a Device Discovery Profile | **901**

Discovering and Assigning Roles in Cross Provisioning Platform for iPASOLINK Devices | **902**

Predefined Scripts for Provisioning iPASOLINK Devices | **904**

Creating a Cross Provisioning Platform Service Definition for iPASOLINK Devices | **905**

Creating a Cross Provisioning Platform Service Order for iPASOLINK Devices | **909**

Configuring QoS Settings for iPASOLINK Devices | **913**

Cross Provisioning Platform for iPASOLINK Devices Overview

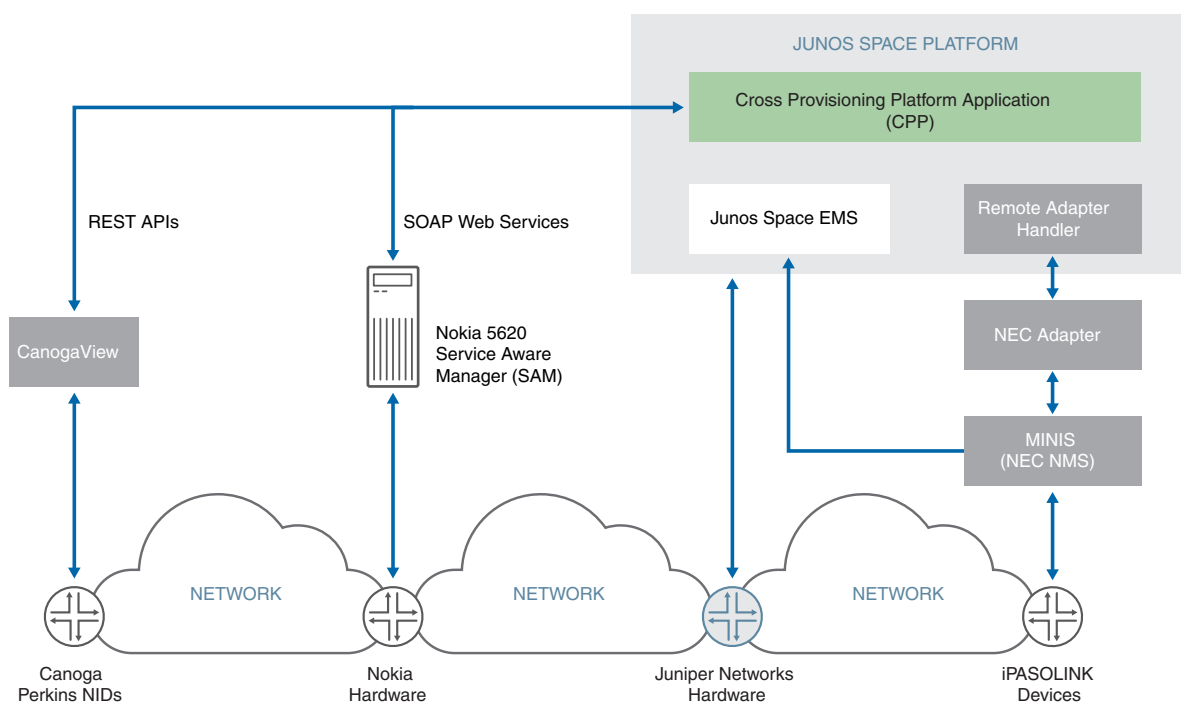
The Cross Provisioning Platform (CPP) software provides a real-time operations support system (OSS) for creating and deploying multivendor LAN or WAN services.

In addition to provisioning Juniper Networks and Nokia devices, the CPP application can provision services (that is, microwave links) on NEC's iPASOLINK devices.

NEC has been involved in developing and providing field-proven, reliable, wireless backhaul solutions through the iPASOLINK series of microwave radio, for service providers all over the world. The iPASOLINK device provide wireless solutions.

Figure 24 on page 883 illustrates the high-level architecture of how CPP communicates with iPASOLINK devices:

Figure 24: Cross Provisioning Platform High-Level Architecture



With Cross Provisioning Platform, you can:

- Provision services across Juniper Networks devices and NEC's iPASOLINK devices

- Provision microwave links along with QoS configurations on iPASOLINK devices. For more information about provisioning QoS settings on an iPASOLINK device, see [“Configuring QoS Settings for iPASOLINK Devices” on page 913](#).
- Provision pseudowire and Layer 3 VPN services across Juniper Networks devices and use iPASOLINK devices to deliver the services that span a wireless network.

For more information about provisioning microwave links across Juniper Networks and iPASOLINK devices, see [“Creating a Cross Provisioning Platform Service Definition for iPASOLINK Devices” on page 905](#) and [“Creating a Cross Provisioning Platform Service Order for iPASOLINK Devices” on page 909](#).

NOTE: The following functions are part of the native CPP functionality, but are not supported on iPASOLINK devices:

- Interface migration
- Service resynchronization

RELATED DOCUMENTATION

[Discovering and Assigning Roles in Cross Provisioning Platform for iPASOLINK Devices | 902](#)

[Predefined Scripts for Provisioning iPASOLINK Devices | 904](#)

Worldwide Junos OS Adapter Overview

The Junos Space wwadapter enables you to manage devices running the worldwide version of Junos OS (ww Junos OS devices) through Junos Space Network Management Platform. ww Junos OS devices use Telnet instead of Secure Shell (SSH2) to communicate with other network elements. Junos Space Network Management Platform uses the failover approach when identifying a ww Junos OS device. It first tries to initiate a connection to the device using SSH2. If it cannot connect to the device, Junos Space Network Management Platform identifies the device as a ww Junos OS device. Since Junos Space Network Management Platform does not support Telnet, it uses an adapter to communicate with ww Junos OS devices. Junos Space Network Management Platform connects to the adapter using SSH2 and the adapter starts a Telnet session with the device.

NOTE: For ww Junos OS devices, Space as a System of Record (SSOR) mode of device management is not supported.

Before you install the wwadapter, complete the following prerequisites:

- Download the adapter image from the local client workstation.
- Ensure that the Junos Space servers have been deployed and are able to access devices.
- Configure Junos Space Network Management Platform to initiate connections with the device.

NOTE: Ensure that you allow at least three Telnet connections between the ww Junos OS device and the Junos Space server. Junos Space Network Management Platform needs a minimum of three Telnet connections with the device in order to be able to manage it.

NOTE: For ww Junos OS devices, the Junos Space Service Now application works only on AI-Scripts version 2.5R1 and later.

The Secure Console workspace and the option in the right-click context menu in the Manage Devices workspace are disabled for ww Junos OS devices.

Installing the Worldwide Junos OS Adapter

You can install and use the wwadapter to manage devices running on the worldwide version of Junos OS (ww Junos OS devices). Before you install the wwadapter, you must upload the ww Junos OS device wwadapter image file.

To upload the wwadapter image file:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Adapter**.
The Device Adapter page is displayed.
2. Select the Add Device Adapter icon on the Actions bar.
3. Browse to the wwadapter image file and select the filename so that the full path appears in the Software File field.
4. Click **Upload** to bring the image into Junos Space Network Management Platform.

A status box shows the progress of the image upload. Adding the wwadapter image file automatically installs the wwadapter.

Before you connect to any device, you must verify that the installation was successful.

To verify that the installation was successful, look at the device console on the Junos Space server.

1. On the server, change the directories to verify that the wwadapter directory has been created.

```
cd /home/jmp/wwadapter
```

2. To verify that the wwadapter is running, enter the following command on the Junos Space server:

```
prompt > service wwadapter status  
wwadapter running
```

If the wwadapter is not active, you see the following status:

```
wwadapter stopped
```

Use the following commands to start or stop the wwadapter:

To start the wwadapter:

```
service wwadapter start
```

To stop the wwadapter:

```
prompt > ps -ef | grep wwadapter  
prompt > kill -9 {wwadapter pid}
```

To see the wwAdapter logs, change the directories to the wwadapter directory.

```
cd /home/jmp/wwadapter/var/errorLog/DmiAdapter.log
```

To view the contents of the error log file, open the log file with any standard text editor.

To view the contents of the log4j configuration file, change the directories to the wwadapter directory.

```
cd /home/jmp/wwadapter /wwadapterlog4j.lcf
```

Device Discovery Profiles Overview

IN THIS SECTION

- [Connections Initiated by Junos Space or the Device | 888](#)
- [Device Information Fetched During Device Discovery | 889](#)

You use the device discovery profile to add devices to Junos Space Network Management Platform from the Devices workspace. *Discovery* is the process of finding a device and then synchronizing the device inventory and configuration with the Junos Space Network Management Platform database. To use device discovery, you must be able to connect Junos Space Network Management Platform to the device.

A device discovery profile contains preferences used to discover devices, such as discovery targets, probes used to discover devices, mode and details for authentication, SSH fingerprints of devices, and the schedule to use this discovery profile. You can start the discovery process using a discovery profile in the following ways: scheduling a discovery after creating a discovery profile, or selecting a discovery profile and clicking Run Now.

Executing or running a discovery profile discovers, authenticates, and manages the device on Junos Space Network Management Platform. With appropriate privileges for discovering devices, you can create multiple discovery profiles with different combinations of targets, probes, and authentication modes on your Junos Space setup. You can clone, modify, and delete the device discovery profiles from Junos Space Network Management Platform. You can also choose whether to share device discovery profiles with other users with device discovery permissions.

To discover network devices using a device discovery profile, Junos Space Network Management Platform uses the SSH, ICMP Ping, and SNMP protocols. When the device is discovered, device authentication is handled through the administrator login SSH v2 credentials and SNMP v1, SNMP v2c, or SNMP v3 settings, keys generated from Junos Space Network Management Platform (RSA, DSS, or ECDSA keys), or custom keys. You can optionally enter the SSH fingerprint for each device and let Junos Space Network Management Platform save the fingerprint in the database during the discovery process and validate the fingerprint when the device connects to Junos Space Network Management Platform. Fingerprint validation is available only for SSH-enabled Juniper Networks devices and not for Junos OS devices and modeled devices.

For device targets, you can specify a single IP address, a DNS hostname, an IP range, or an IP subnet to discover devices on a network. When a device discovery profile is executed or run (either instantly or based on a schedule), Junos Space Network Management Platform connects to the physical device and retrieves the running configuration and the status information of the device. To connect with and configure

devices, Junos Space Network Management Platform uses the Device Management Interface (DMI) of Juniper Networks devices, which is an extension of the NETCONF network configuration protocol.

Connections Initiated by Junos Space or the Device

When a device is discovered, Junos Space Network Management Platform creates an object in the Junos Space Network Management Platform database to represent the physical device and maintains a connection between the object and the physical device so that their information is linked.

Junos Space can manage devices in either of the following ways:

- Junos Space initiates and maintains a connection to the device.
- The device initiates and maintains a connection to Junos Space.

By default, Junos Space manages devices by initiating and maintaining a connection to the device. When Junos Space initiates the connection to the device, you can discover and manage devices irrespective of whether the management system is behind a Network Address Translation (NAT) server. For Junos OS devices, Junos Space uses SSH with an adapter to manage the devices.

If a device-initiated connection to Junos Space is enabled, the DMI channel and port 7804 are used and the following (sample) configuration is added on the device to establish the connection to Junos Space:

```
set system services outbound-ssh client 00111DOCEFAC device-id 7CE5FE
set system services outbound-ssh client 00111DOCEFAC secret "$ABC123"
set system services outbound-ssh client 00111DOCEFAC services netconf
set system services outbound-ssh client 00111DOCEFAC 172.22.199.10 port 7804
```

To discover and manage devices through a device-initiated connection, clear the **Junos Space initiated connection to device** check box on the Modify Application Settings page in the Administration workspace. For information about configuring connections initiated by Junos Space by a device, see *Modifying Junos Space Network Management Platform Settings*.

You can configure a NAT server to route connections between the Junos Space setup and managed devices. Both device-initiated connections to a Junos Space setup and connections initiated by Junos Space to managed devices, when the Junos Space setup is behind the NAT server, are supported on Junos Space Network Management Platform. If a NAT server is used, the managed devices connect to Junos Space Network Management Platform through the IP address of Junos Space Network Management Platform translated by NAT.

When configuration changes are made in Junos Space Network Management Platform—for example, when you deploy service orders to activate a service on your network devices—the configuration is pushed to the physical device.

If the network is the system of record (NSOR), when configuration changes are made on the physical device (out-of-band CLI commits and change-request updates), Junos Space Network Management Platform automatically resynchronizes with the device so that the device inventory information in the Junos Space Network Management Platform database matches the current device inventory and configuration information. If Junos Space Network Management Platform is the system of record (SSOR), this resynchronization does not occur and the database is unchanged.

Device Information Fetched During Device Discovery

The following device inventory and configuration data are captured and stored in relational tables in the Junos Space Network Management Platform database:

- Devices—Hostname, IP address, credentials
- Physical Inventory—Chassis, FPM board, power entry module (PEM), Routing Engine, Control Board (CB), Flexible PIC Concentrator (FPC), CPU, PIC, transceiver, fan tray
 Junos Space Network Management Platform displays the model number, part number, serial number, and description for each inventory component, when applicable.
- Logical Inventory—Subinterfaces, encapsulation (link-level), type, speed, maximum transmission unit (MTU), VLAN ID
- License information:
 - License usage summary—License feature name, feature description, licensed count, used count, given count, needed count
 - Licensed feature information—Original time allowed, time remaining
 - License SKU information—Start date, end date, and time remaining
- Loopback interface

Other device configuration data is stored in the Junos Space Network Management Platform database as binary large objects and is available only to northbound interface (NBI) users.

Creating a Device Discovery Profile

You create a device discovery profile to create a set of preferences for device targets, probes, authentication mode and credentials, SSH fingerprints, and the schedule to discover devices to Junos Space Network Management Platform. In addition to scheduling the discovery, you can manually start the discovery

process by running the device discovery profile. For more information, see [“Running Device Discovery Profiles” on page 900](#).

NOTE: To discover a device with dual Routing Engines, always specify the IP address of the current primary Routing Engine. When the current primary IP address is specified, Junos Space Network Management Platform manages the device and the redundancy. If the primary Routing Engine fails, the backup Routing Engine takes over and Junos Space Network Management Platform manages the transition automatically without bringing down the device.

NOTE: When you initiate discovery on a device running Junos OS, Junos Space Network Management Platform automatically enables the NETCONF protocol over SSH by pushing the following command to the device:

```
set system services netconf ssh
```

To create a device discovery profile, complete the following tasks:

1. [Specifying Device Targets | 890](#)
2. [Specifying Probes | 893](#)
3. [Selecting the Authentication Method and Specifying Credentials | 896](#)
4. [\(Optional\) Specifying SSH Fingerprints | 897](#)
5. [Scheduling Device Discovery | 898](#)

Specifying Device Targets

Device targets are IP addresses or hostnames of devices that you want Junos Space Network Management Platform to discover.

To specify the device targets that you want Junos Space Network Management Platform to discover:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Discovery > Device Discovery Profiles**.

The Discover Discovery Profiles page is displayed.

2. Click the **Create Device Discovery Profile** icon on the toolbar.

The Device Discovery Target page is displayed on the left. The list of different tasks that should be completed to create a profile is displayed on the right: Device Discovery Target, Specify Probes, Specify Credentials, Specify Device FingerPrint, and Schedule/Recurrence.

NOTE: At any point in time, you can click the links to the different tasks (on the right of the page) and navigate to those pages.

3. In the Discovery Profile Name field, enter the name of the device discovery profile.

The device discovery profile name cannot exceed 255 characters and can contain letters, numbers, spaces, and special characters. The special characters allowed are period (.), hyphen (-), and underscore (_). The device discovery profile name cannot start with letters or numbers and cannot contain leading or trailing spaces.

NOTE: The Make Public check box is selected by default so that the device discovery profile is visible to all users.

4. In the Discovery Parameters field, you can add devices manually by specifying the details on the Device Discovery Target page or by uploading the details of the devices through a CSV file.

To add devices manually:

- a. Click the **Add Manually** option button.

- b. In the Target Type area, select how you want to specify the targets: IP addresses or hostnames, IP ranges, or a subnet.

- To enter the IP address or hostname of the device:
 - i. Select the **IP Address/Hostname** option button.
 - ii. In the Target Details field, enter the IP address or hostname.

NOTE: You can enter the IP address in either IPv4 or IPv6 format. Refer to <http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml> for the list of restricted IPv4 addresses and <http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml> for the list of restricted IPv6 addresses.

NOTE: You can enter a combination of the following separated by a comma (,):

- IP addresses
- Hostnames
- IP address range expressions
- Subnet expressions

For example, **192.168.27.1, example.abc.com, 192.168.27.50-192.168.27.60, 192.168.26.0/24**

- To enter a range of IP addresses for the devices:
 - i. Select the **IP Range** option button.
The maximum number of IP addresses for an IP range target is 1024.
 - ii. In the Start IP Address field, enter the first IP address.
 - iii. In the End IP Address field, enter the last IP address.
- To enter an IP subnet for the devices:
 - i. Select the **Subnet** option button.
 - ii. In the IP Subnet/CIDR field, enter the subnet details.

The subnet prefix for IPv4 addresses is 1–32 and for IPv6 addresses is 1–128.

To add devices by using a CSV file:

NOTE: From Junos Space Network Management Platform Release 16.1R1, a Private Key column has been added in the CSV file to support the custom key option for device discovery. Ensure that you use the latest sample CSV file. However, backward compatibility is supported. That is, if you use an existing CSV file (from a previous release), the file is uploaded successfully.

- a. Click the **Upload CSV** option button.

NOTE: The format of the CSV file that you are uploading should exactly match the format of the sample CSV file.

You can add hundreds of devices to Junos Space Network Management Platform by using a CSV file. You can specify the hostnames, IP addresses, device login credentials, tags, and SSH fingerprints in the CSV file.

- b. (Optional) To view a sample CSV file, click the **Sample CSV** link.

- c. Click **Browse**.

The CSV File Upload dialog box appears.

- d. Navigate to the desired CSV file, select it, and then click **Open**.

The name of the CSV file is displayed in the CSV File: field.

- e. Click **Upload** to upload the selected CSV file.

5. Click **Next** to proceed and select probes.

The **Specify Probes** page is displayed.

Specifying Probes

Probes are protocols used to find devices on the network—ping, SNMP, or SSH.

To specify probes on the Specify Probes page:

1. To use the NAT configuration to discover devices using this profile, select the the **Use NAT** check box.

The Use NAT check box is available for selection only if NAT is already configured in Junos Space.

2. To discover devices using ping (if SNMP is not configured on the device), select the **Use Ping** check box.

By default, this check box is selected.

3. To discover devices using SNMP (if SNMP is configured on the device), select the **Use SNMP** check box.

By default, this check box is selected.

NOTE: If you clear both the Use Ping and Use SNMP check boxes, SSH is used to discover devices. When both the Use Ping and Use SNMP check boxes are selected (the default), Junos Space Network Management Platform can discover the target device more quickly, but only if the device is pingable and SNMP is enabled on the device.

4. You can select an appropriate version of SNMP during discovery:

- To use SNMP v1 or v2c:
 - i. Select the **SNMP V1/V2C** option button.
 - ii. Specify a community string, which can be **public**, **private**, or a predefined string.
The default community string is **public**.
- To use SNMP v3:
 - i. Select the **SNMP V3** option button.
 - ii. In the User Name field, enter the username.
 - iii. In the Authentication type field, select the authentication type (**MD5**, **SHA1**, or **None**).
 - iv. In the Authentication password field, enter the authentication password. .
This field is available only if you selected MD5 or SHA1 in the Authentication type field. If you selected **None** as the authentication type, the authentication function is disabled.
 - v. Select the privacy type (**AES128**, **AES192**, **AES256**, **DES**, or **None**).
 - vi. Enter the privacy password (if AES128, AES192, AES256, or DES).
If you specify **None** for the privacy type, the privacy function is disabled.

5. (Optional) Click **Back** to navigate to the Device Discovery Target page and change the details of the device targets.

6. Click **Next** to proceed and select the authentication method.

The **Specify Credentials** page is displayed.

Selecting the Authentication Method and Specifying Credentials

You can choose the mode of authentication for the devices you are about to discover. For credentials-based authentication, if you already specified the device login credentials in the CSV file, you can skip the Specify Credentials page. With credentials-based authentication, you can specify a common administrator name and password to establish an SSH connection to each target device that you are about to discover. If you are using key-based authentication, you must have generated keys from Junos Space Network Management Platform or must have the private key on your computer.

To specify the mode of authentication and credentials on the Specify Credentials page:

1. Select the mode of authentication used to authenticate devices during discovery.

To use credentials-based authentication:

- a. In the Authentication Type area, select the **Credentials-Based Authentication** option button.
- b. In the Username field, enter the administrator username.
- c. In the Password field, enter the administrator password.
- d. In the Confirm Password field, reenter the administrator password.

To use key-based authentication:

- a. In the Authentication Type area, select the **Key-Based Authentication** option button.
- b. In the Username field, enter the administrator username.

You can use a key generated from Junos Space Network Management Platform or a custom private key uploaded to Junos Space Network Management Platform:

- To use a key generated from Junos Space Network Management Platform:
 - i. Select the **Use Space Key** option button.
- To use a custom private key:
 - i. Select the **Use Custom Key** option button.
 - ii. (Optional) In the Passphrase field, enter the passphrase created when you generated the private key.
 - iii. Next to the Private Key field, click the **Browse** button to upload the private key for the managed devices.

NOTE: If you modify the discovery profile, the Private Key field displays **id_rsa** (which is the default filename) instead of the name of the uploaded file.

- c. (Optional) Click **Back** to navigate to the preceding pages and change the probes and device targets.
- d. Click **Next** to proceed and specify device fingerprints.

The **Specify Device FingerPrint** page is displayed.

(Optional) Specifying SSH Fingerprints

Optionally, specify or modify (if you specified the fingerprints by using the CSV file) the SSH fingerprints for target devices. If you do not specify the fingerprints, Junos Space Network Management Platform obtains fingerprint details when it connects to the device for the first time. You can specify fingerprints during device discovery only for Juniper Networks devices. If you already specified the SSH fingerprints in the CSV file, you can skip this task.

To specify the SSH fingerprints on the Specify Device FingerPrint page:

1. Click the Fingerprint column corresponding to the device and enter the SSH fingerprint of the device.

NOTE: You can specify fingerprints for a maximum of 1024 devices simultaneously using this workflow.

2. (Optional) Repeat step 1 for all devices or devices whose fingerprints you know.
3. (Optional) Click **Back** to navigate to the preceding pages and change the authentication details, probes, and device targets.
4. Click **Next** to proceed and schedule discovery by using this profile.

The **Schedule/Recurrence** page is displayed.

Scheduling Device Discovery

Schedule the device discovery profile to discover devices to Junos Space Network Management Platform.

To schedule the device discovery profile to discover devices:

1. Select the **Schedule at a later time** check box.
 - a. Enter the date in the Date field in the MM/DD/YYYY format.
 - b. Enter the time in the Time field in the hh:mm format.
2. Select the **Recurrence** check box.
 - a. (Optional) Select the periodicity of recurrence from the Repeats list.
The options are Minutes, Hourly, Daily, Weekly, Monthly, and Yearly. The default is Weekly.
 - b. (Optional) Select the interval from the Repeat every list.
The default is 1.
 - c. (Optional) If you select Weekly from the Repeats list, the Repeat by field appears. Select the check boxes for the days of the week that you want the job to recur.

- d. (Optional) Click the On option button in the Ends field to specify an end date for the job recurrence.
If you select the Never option button, the job recurs endlessly until you cancel the job manually.
 - e. To specify the date and time when you want to end the job recurrence:
 - i. Enter the date in the Date field in the MM/DD/YYYY format.
 - ii. Enter the time in the Time field in the hh:mm format.
3. (Optional) Click **Back** to navigate to the preceding page and change fingerprints, authentication details, probes, and device targets.
4. Click **Finish** to save the device discovery profile.
- A job is created and the Discover Network Elements Information dialog box displays the link to the job ID. Click **OK** to close the Information dialog box.

Running Device Discovery Profiles

You run a device discovery profile to automatically discover, synchronize device inventory and interface details, and manage devices running Junos OS to Junos Space Network Management Platform. Device discovery is a four-step process in which you specify target devices, credentials to connect to each device (that is, reuse existing credentials or specify new ones), and, optionally, the probe method (ICMP Ping, SNMP, both ICMP Ping and SNMP, or none), and the SSH fingerprint for each device. You can run multiple device discovery profiles by using this workflow. If you run multiple device discovery profiles, all devices targets specified in the device discovery profiles are discovered.

Before you start discovering devices, ensure that the following conditions are met:

- The device is configured with a management IP address that is reachable from the Junos Space server, or the NAT server if you are using a NAT server on your Junos Space setup.
- A user with the privileges of a Junos Space administrator is created and enabled on the device.
- The device is configured to respond to ping requests if you intend to use ping as the probe method to discover devices.
- SNMP is enabled on the device with appropriate read-only v1 or v2c or v3 credentials if you intend to use SNMP as the probe method to discover devices.

To run discovery profiles:

1. On the Junos Space Network Management Platform user interface, select **Devices >Device Discovery > Device Discovery Profiles**.

The Discover Discovery Profiles page is displayed.

2. Select the check boxes corresponding to the discovery profiles you want to run and click the **Run Now** icon on the toolbar.

The Discovery Status report appears. This report shows the progress of discovery in real time. Click a bar in the chart to view information about the devices currently managed or discovered, or for which discovery failed.

A job is created for every device discovery profile you run. From the Job Details page, you can check whether a device was discovered and added to Junos Space Network Management Platform. If a device is discovered, you can view the device on the Device Management page.

To go to the Job Details page, double-click the ID of the device discovery job on the Job Management page. The Description column on this page specifies whether the device was discovered and added to Junos Space Network Management Platform. If the device was not discovered and added to Junos Space Network Management Platform, the column lists the reason for failure. You can also sort all the columns in ascending or descending order to identify the devices that are discovered and devices that are not discovered.

Modifying a Device Discovery Profile

You modify a device discovery profile when you want to expand the range of device targets, change device targets when devices were not discovered, change credentials or other details such as fingerprints or the discovery schedule.

NOTE: Ensure that you have no discovery jobs scheduled for a device discovery profile that you want to modify. All discovery jobs scheduled from the original device discovery profile are canceled after you modify the original device discovery profile.

To modify a device discovery profile:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Discovery > Device Discovery Profiles**.

The Discover Discovery Profiles page is displayed.

2. Select the check box corresponding to the device discovery profile you want to modify and click the **Modify Profile** icon on the toolbar

The Modify Device Discovery Profile page is displayed.

The Device Discovery Target page is displayed on the left. The list of different tasks that should be completed to create a device discovery profile is displayed on the right: Device Discovery Target, Specify Probes, Specify Credentials, Specify Device FingerPrint, and Schedule/Recurrence.

NOTE: At any point in time, you can click the links to the different tasks (on the right of the page), navigate to those pages, and modify the details of the device discovery profile.

3. (Optional) Review and modify the details of the device and click **Next**.

The **Specify Probes** page is displayed.

4. (Optional) Review and modify the probes and click **Next**.

The **Specify Credentials** page is displayed.

5. (Optional) Review and modify the authentication details and click **Next**.

NOTE: If you modify the discovery profile, the Private Key field displays `id_rsa` (which is the default filename) instead of the name of the uploaded file.

The **Specify Device FingerPrint** page is displayed.

6. (Optional) Review and modify the fingerprint details and click **Next**.

The **Schedule/Recurrence** page is displayed.

7. Review and modify the schedule and click **Finish**.

The device discovery profile is modified. A job is created and the Discover Network Elements Information dialog box displays the link to the job ID. Click **OK** to close the Information dialog box.

NOTE: If you modify and run a device discovery profile for which an associated device discovery job is already in progress, the existing job is cancelled and a new job is triggered for the modified discovery profile.

Discovering and Assigning Roles in Cross Provisioning Platform for iPASOLINK Devices

IN THIS SECTION

- [Discovering Device Roles | 903](#)
- [Assigning Device Roles | 903](#)

Before discovering and assigning iPASOLINK devices, you must have already run device discovery in Junos Space Platform. For more information on device discovery in Junos Space Platform, see *Discovering Devices* in the *Junos Space Network Application Platform User Guide*.

Pre-staging all iPASOLINK devices is a powerful yet simple way to prepare your devices for provisioning. Pre-staging has two parts:

Discovering Device Roles

To discover the roles of devices:

1. In the **Cross Provisioning Platform** task pane, select **Prestage Devices > Manage Device Roles > Discover Roles**.

The **Role Discovery Status** window shows the discovery of unassigned devices found in the database.

2. To view the devices for which the CPP software recommends the L2E role, click the L2E bar.

The **Assign Roles** window appears.

NOTE: By default, iPASOLINK devices are discovered as Layer 2 Ethernet (L2E) devices.

Assigning Device Roles

During the prestaging process, iPASOLINK devices are assigned a role of Layer 2 Ethernet (L2E) device. When you create Pseudowire and Layer 3 VPN services across Juniper Networks devices, you can attach multiple iPASOLINK devices as these services support multiple L2E endpoints.

To assign device roles for iPASOLINK devices:

1. In the **Cross Provisioning Platform** task pane, select **Prestage Devices > Manage Device Roles > Assign Roles**.
2. In the **Assign Roles** page, click an iPASOLINK device.
3. Open the **Actions** menu and select **Assign Role**.

iPASOLINK devices are assigned a role of Layer 2 Ethernet (L2E) device.

4. In the confirmation window, click **Assign**.
5. To view the assignment status, in the **Job Management** window, click the job ID of the assignment job.

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.

Predefined Scripts for Provisioning iPASOLINK Devices

Cross Provisioning Platform provides predefined scripts that a service provisioner can use while creating a service.

Predefined scripts for iPASOLINK devices are as follows:

- PD_QOS_Device_Configlet_Create_Script_iPASO—Script used for provisioning QoS configurations on iPASOLINK devices
- PD_QOS_Device_Configlet_Modify_Script_iPASO—Script used for modifying QoS configurations on iPASOLINK devices
- PD_QOS_Device_Configlet_Detail_Script_iPASO—Script used for viewing QoS configurations on iPASOLINK devices
- PD_VLAN-PATH_Create_Script_iPASO—Script used for provisioning VLAN-PATH services on iPASOLINK devices
- PD_VLAN-PATH_Modify_Script_iPASO—Script used for modifying VLAN-PATH services on iPASOLINK devices
- PD_VLAN-PATH_Detail_Script_iPASO—Script used for viewing VLAN-PATH services on iPASOLINK devices
- PD_P2P_LDP_iPaso_Create_Script_JNPR_iPASO—Script used for provisioning LDP-based point-to-point services between Juniper Networks devices and iPASOLINK devices.
- PD_P2P_LDP_iPaso_Modify_Script_JNPR_iPASO—Script used for modifying LDP-based point-to-point services between Juniper Networks devices and iPASOLINK devices
- PD_P2P_LDP_iPaso_Details_Script_JNPR_iPASO—Script used for viewing LDP-based point-to-point services between Juniper Networks devices and iPASOLINK devices
- PD_L3VPN_iPaso_Create_Script_JNPR_iPASO—Script used for provisioning Layer 3 VPN services between Juniper Networks devices and iPASOLINK devices
- PD_L3VPN_iPaso_Modify_Script_JNPR_iPASO—Script used for modifying Layer 3 VPN services between Juniper Networks devices and iPASOLINK devices.
- PD_L3VPN_iPaso_Detail_Script_JNPR_iPASO—Script used for viewing Layer 3 VPN services between Juniper Networks devices and iPASOLINK devices.

To view details of predefined scripts, select and double-click the predefined script on the **CPP > Scripts** page. The Script Details window appears.

The Script Details window contains a Configuration Script tab and a GUI Script tab. The configuration script available on Configuration Script tab is used for generating the configuration and the GUI script available on the GUI Script tab generates the GUI window for you to provision a service.

You can modify a predefined script. For more information on modifying a script, see [“Modifying Scripts Created for Cross Provisioning Platform” on page 779](#).

RELATED DOCUMENTATION

[Adding Scripts Created for Cross Provisioning Platform | 775](#)

[Exporting Scripts Created for Cross Provisioning Platform | 776](#)

[Importing Scripts Created for Cross Provisioning Platform | 778](#)

[Modifying Scripts Created for Cross Provisioning Platform | 779](#)

Creating a Cross Provisioning Platform Service Definition for iPASOLINK Devices

To create a cross provision platform service definition for NEC:

1. In the **Cross Provisioning Platform** task pane, select **CPP > Service Definitions**.
2. In the **CPP > Service Definition** window, click on the + button. The **Create Service Definition** window appears.

Create Service Definition

General

Name:

sd-vlan-path

ID:

Description:

Type:

VLAN-PATH

JUNOS Space Service Scripts

Creation:

PD_VLAN-PATH_Details_Script_JNPR

Modification:

PD_VLAN-PATH_Create_Script_JNPR

SAM Service Scripts

Creation:

Modification:

JUNOS Space Service Scripts

SAM Service Scripts

Select Junos Creation Script

Name

PD_Device_Turn_Up_Modify_Script_JNPR

PD_P2P_LDP_Details_Script_JNPR

PD_P2P_BGP_Details_Script_JNPR

PD_VPLS_Details_Script_JNPR

PD_L3VPN_Details_Script_JNPR

PD_BNG_Details_Script_JNPR

PD_NPS_Details_Script_JNPR

PD_VLAN-PATH_Details_Script_JNPR

PD_Device_Details_Script_JNPR

ipaso_devices

iPasoPW_LDP

iPaso_device_Modify

Select Junos Modification Script

Name

PD_P2P_LDP_Create_Script_JNPR

PD_P2P_LDP_Modify_Script_JNPR

PD_L3VPN_Create_Script_JNPR

PD_L3VPN_Modify_Script_JNPR

PD_P2P_BGP_Create_Script_JNPR

PD_P2P_BGP_Modify_Script_JNPR

PD_VPLS_Create_Script_JNPR

PD_VPLS_Modify_Script_JNPR

PD_VLAN-PATH_Create_Script_JNPR

PD_Interface_Migration_Script_JNPR

PD_Bulk_Service_Modify_Script_JNPR

PD_Bulk_Device_Modify_Script_JNPR

Page 1 of 1

Displaying 1 - 27 of 27

Page 1 of 1

Displaying 1 - 27 of 27

Create

Cancel

3. Enter information in the **Create Service Definition** window according to the descriptions in the following table.

Parameter	Description
Name	Enter a name for the service definition.
ID	<p>Enter a unique ID to associate with this service definition in the range 1 through 2147483647.</p> <p>NOTE: The service definition ID is optional. If you do not provide any value in this field, the default value is -1. In the service definition selection grid, no value is displayed in the ID column. Each service definition is assigned a unique ID. If you give an existing ID value while creating a new service definition, exception occurs.</p>
Description	Enter a description of the service to distinguish its operation from others.

Parameter	Description
Type	<p>Select one of the following type to creating a service definition for iPASOLINK devices:</p> <ul style="list-style-type: none">• <i>VLAN-PATH</i> —Select this service type to provision microwave links across Juniper Networks devices and iPASOLINK devices.• <i>PW-LDP-IPASO</i> —Select this service type to provision LDP-based point-to-point service across Juniper Networks devices and iPASOLINK devices.• <i>PW-LDP-IPASO</i> —Select this service type to provision Layer 3 VPN service across Juniper Networks devices and iPASOLINK devices.• <i>Device</i>—Select this service type to provision QoS settings for an iPasolink device <p>NOTE: For each of these Type, you must select the corresponding script. For example if you are provisioning LDP-based point-to-point service across Juniper Networks devices and iPASOLINK devices you must select PD_P2P_LDP_iPaso_Create_Script_JNPR_iPASO and PD_P2P_LDP_iPaso_Modify_Script_JNPR_iPASO scripts.</p>

Parameter	Description
Junos Space Service Scripts	<p>This parameter provides two fields:</p> <ul style="list-style-type: none"> • Select Junos Space Creation Script—Select a Junos Space service creation script from the list of scripts available in this section and the same would be populated in the corresponding text field. If you need to remove the selected script, deselect the same. Following are the Junos Space service creation scripts for an iPASOLINK device: <ul style="list-style-type: none"> • PD_QOS_Device_Configlet_Create_Script_iPASO—Script used for provisioning QoS configuration on iPASOLINK devices. • PD_VLAN-PATH_Create_Script_iPASO—Script used for provisioning VLAN-PATH service on iPASOLINK devices. • PD_P2P_LDP_iPaso_Create_Script_JNPR_iPASO—Script used for provisioning LDP-based point-to-point service between Juniper Networks and iPASOLINK devices. • PD_L3VPN_iPaso_Create_Script_JNPR_iPASO—Script used for provisioning Layer 3 VPN service between Juniper Networks and iPASOLINK devices. <p>NOTE: You cannot create a service definition if you have not selected the Junos Space creation script.</p> <ul style="list-style-type: none"> • Select Junos Space Modification Script—Select a Junos Space modification script from the list of scripts available in this section and the same would be populated in the corresponding text field. If you need to remove the selected script, deselect the same. Following are the Junos Space service modification scripts for an iPASOLINK device: <ul style="list-style-type: none"> • PD_QOS_Device_Configlet_Modify_Script_iPASO—Script used for modifying QoS configuration on iPASOLINK devices. • PD_VLAN-PATH_Modify_Script_iPASO—Script used for modifying VLAN-PATH service on iPASOLINK devices. • PD_P2P_LDP_iPaso_Modify_Script_JNPR_iPASO—Script used for modifying LDP-based point-to-point service between Juniper Networks and iPASOLINK devices. • PD_L3VPN_iPaso_Modify_Script_JNPR_iPASO—Script used for modifying Layer 3 VPN service between Juniper Networks and iPASOLINK devices. <p>NOTE: For more information on predefined scripts, see “Predefined Scripts for Provisioning iPASOLINK Devices” on page 904.</p>
SAM Service Scripts	No action is required for iPASOLINK devices.

4. Click **Create**.

The service definition is listed on the Service Definition page.

The value in the **ID** field is associated with a service definition. This identifier can be used when you are searching for a particular service definition while creating a service order. You can search the service

definition by its name, type or unique ID. You can modify the ID only during the migration of old service definition IDs.

5. Select the service definition you created and select **Action > Publish Service Definition**. The **State** column indicates when the service definition is published.

You can create the service order based on the service definition you created. For creating a Cross Provisioning Platform service order for iPASOLINK Devices, see [“Creating a Cross Provisioning Platform Service Order for iPASOLINK Devices” on page 909](#).

RELATED DOCUMENTATION

| [Creating a Cross Provisioning Platform Service Order for iPASOLINK Devices | 909](#)

Creating a Cross Provisioning Platform Service Order for iPASOLINK Devices

Before you create a cross provision platform service order, you must create the service definition upon which to base the service order. For example, if you want to create a VLAN-PATH service order you must have created a service definition with **Type** as *VLAN-PATH* and must have attached the corresponding VLAN-PATH-related predefined scripts.

To create a Cross Provisioning Platform service order:

1. in the **Cross Provisioning Platform** task pane, select **CPP > Service Orders**.
2. In the **Service Orders** window, click the + button. The **Create CPP Service Order** window appears.

Create CPP Service Order

General Settings

Select Service Definition

ID	Name	Type
	p2p_ldp	PW-LDP
	vlan_PATH	VLAN-PATH

Page 1 of 1 | Displaying 1 - 2 of 2 | Show 30 items

Description:

Next Cancel

- In the **General Settings** section, select a service definition based on the unique ID, name or type. For configuring VLAN path between iPASOLINK devices you must select the service definition with service type as VLAN-PATH.

NOTE: The value in the **ID** field is associated with a service definition. This identifier can be used when you are searching for a particular service definition while creating a device configlet order. You can search the service definition by its name, type or unique ID. You can modify the ID only during the migration of old service definition IDs.

- In the **Order description** field, enter a description of the service that distinguishes its operation from others.
- Click **Next**.

The iPASOLINK VLAN Path Provisioning page appears.

NOTE: The following representation of a iPASOLINK VLAN Path Provisioning page window is a sample only. The appearance of this window is based on the scripts that are associated with the service definition upon which the service is based.

The screenshot shows the 'iPASOLINK VLAN Path Provisioning' window. It has a title bar with a close button. The main content area is divided into four sections:

- General:** A text field labeled 'Name:' with the value 'SO938680498'.
- Step1: Select Device:** A table with two columns: 'Device Name' and 'IP Address'. It lists several devices, with 'Device_device_8.8.1.100' selected. Below the table is a pagination bar showing 'Page 1 of 20' and 'Displaying 1 - 5 of 10'.
- Step2: Select Interface:** A table with three columns: 'Device Name', 'Port', and 'Status'. It lists interfaces for the selected device, with 'modem_ea/4/1' selected. Below the table is a pagination bar showing 'Page 1 of 19' and 'Displaying 1 - 10 of 190'.
- Add to Staged Interfaces:** A button located between Step2 and Step3.
- Step3: Enter Staged Interface Details:** A table with six columns: 'Device Name', 'Location Id', 'VLAN ID', 'VLAN Service Name', 'Port Type', and 'Action'. It shows one entry for 'Device_device_8.8.1.100' with 'modem_ea/4/1' in the Port Type column. Below the table is a pagination bar showing 'Page 1 of 1' and 'Displaying 1 - 1 of 1'.

At the bottom of the window are five buttons: 'Create', 'Clear', 'Cancel', 'Verify', and 'Cancel'.

6. In the **Step1: Select Device** section, select a device.
7. In the **Step2: Select Interface** section, select the corresponding interfaces.
8. Click **Add to Staged Interfaces**.
The selected devices will be listed in the **Step3: Enter Staged Interface Details** section.
9. In the **Step3: Enter Staged Interface Details**, specify the following parameters for each interface:
 - VLAN ID
 - VLAN Service Name

- Port Type
- QOS Settings

NOTE: This is applicable for VLAN-PATH service type only.

- L2 Extension

The L2 Extension section is available for L3VPN-IPASO or P2P-IPASO service types only.

NOTE: iPASOLINK devices are assigned a role of Layer 2 Ethernet (L2E) device. When you create Pseudowire and Layer 3 VPN or point-to-point services across Juniper Networks devices, you can attach multiple iPASOLINK devices as these services support multiple L2E endpoints.

10. (Optional) Click **Clear** if you want to reset the selections.

11. (Optional) Before you click **Create**, to verify the configuration click **Verify**.

12. Click **Create** to create the service order.

13. Deploy the service order.

For more information on deploying a service order, see [“Deploying a Service Order” on page 631](#).

After you successfully deploy the service order, the service order is listed on the Services page.

On the Services page, you can perform the following actions:

- View a service.
- Modify a service
- Decommission a service
- Perform Functional Audit
- Perform Configuration Audit

NOTE: The Cross Provisioning Platform application does not support two-phase commit and delete partial configurations options for iPASOLINK devices.

RELATED DOCUMENTATION

[Creating a Cross Provisioning Platform Service Definition | 305](#)

[Viewing Cross Provisioning Platform Service Order Details | 622](#)

[Viewing Services | 832](#)

[Editing a Service Name | 834](#)

[Decommissioning a Service | 834](#)

[Modifying a Service in Cross Provisioning Platform | 873](#)

[Understanding Service Validation | 875](#)

[Service Troubleshooting Overview | 875](#)

[Troubleshooting Services in Cross Provisioning Platform | 876](#)

Configuring QoS Settings for iPASOLINK Devices

To configure QoS settings for an iPASOLINK device:

1. In the **Cross Provisioning Platform > CPP > Service Definitions**, create a service definition with the service type as **DEVICE**. Ensure you select a script from the following list of QoS-related predefined scripts:
 - PD_QOS_Device_Configlet_Create_Script_iPASO—Script used for provisioning QoS configurations on iPASOLINK devices
 - PD_QOS_Device_Configlet_Modify_Script_iPASO—Script used for modifying QoS configurations on iPASOLINK devices
 - PD_QOS_Device_Configlet_Detail_Script_iPASO—Script used for viewing QoS configuration on iPASOLINK devices

For more information about creating a service definition, see [“Creating a Cross Provisioning Platform Service Definition for iPASOLINK Devices” on page 905](#).

2. Publish the service definition.

To publish the service definition that you have created:

- a. On the Service Definitions page, select the service definition that you have created.
- b. From the Actions menu, select **Publish Service Definition**.

The Publish Service Definitions window that is displayed prompts you to confirm your action.

- c. Click **Publish**.

The Service Definitions page reappears. The selected service definition is now in the published state.

3. Provision the configuration on the iPASOLINK device.

- a. On the **Cross Provisioning Platform** task pane, select **CPP** > **Device Configlet Orders**.

The Device Configlet Order page appears.

- b. On the Device Configlet Orders page, click the + icon.

The Create CPP Device Configlet Order page appears.

- c. On the Create CPP Device Configlet Order page, select the service definition that you have created in step 1.
- d. (Optional) Specify the description in the **Description** field.
- e. Click **Next**.

The QoS Provisioning window appears.

NOTE: The appearance of the QoS Provisioning window is based on the scripts that are associated with the service definition upon which the device configlet is based.

- f. Select an iPASOLINK device in Site name, and fill in the QoS-settings-related fields on the Classify Settings, Ingress Settings, and Egress Settings tabs.

4. (Optional) If you want to verify the modified QoS Settings, click **Verify**.

5. Click **Create**.

The QoS Settings is deployed on the selected iPASOLINK device and you can view the device configlet order on the Device Configlet Orders page.

For more information about administering the device configlet order, see [“Administering a Device Configlet Service Order for Cross Provisioning Platform” on page 795](#).

NOTE: You cannot decommission a device configlet order.

6. Deploy the device configlet order.

The QoS configuration is deployed on the iPASOLINK device.

28

CHAPTER

Canoga Perkins Network Interface Device Management

Cross Provisioning Platform for Canoga Perkins NIDs Overview | **916**

Configuring OSS Parameters for Canoga Perkins NIDs | **918**

Confirming Communication with Canoga Perkins OSS Server | **920**

Adding a Canoga Perkins NID to Cross Provisioning Platform | **921**

Synchronizing Canoga Perkins NIDs with OSS | **922**

Adding Canoga Perkins Scripts | **925**

Creating a Service Definition for Canoga Perkins NIDs | **926**

Creating a Cross Provisioning Platform Service Order for Canoga Perkins NIDs | **929**

Performing Service Activation Test | **931**

Cross Provisioning Platform for Canoga Perkins NIDs Overview

The Cross Provisioning Platform (CPP) application provides a real-time operations support system (OSS) for creating and deploying services across multivendor devices.

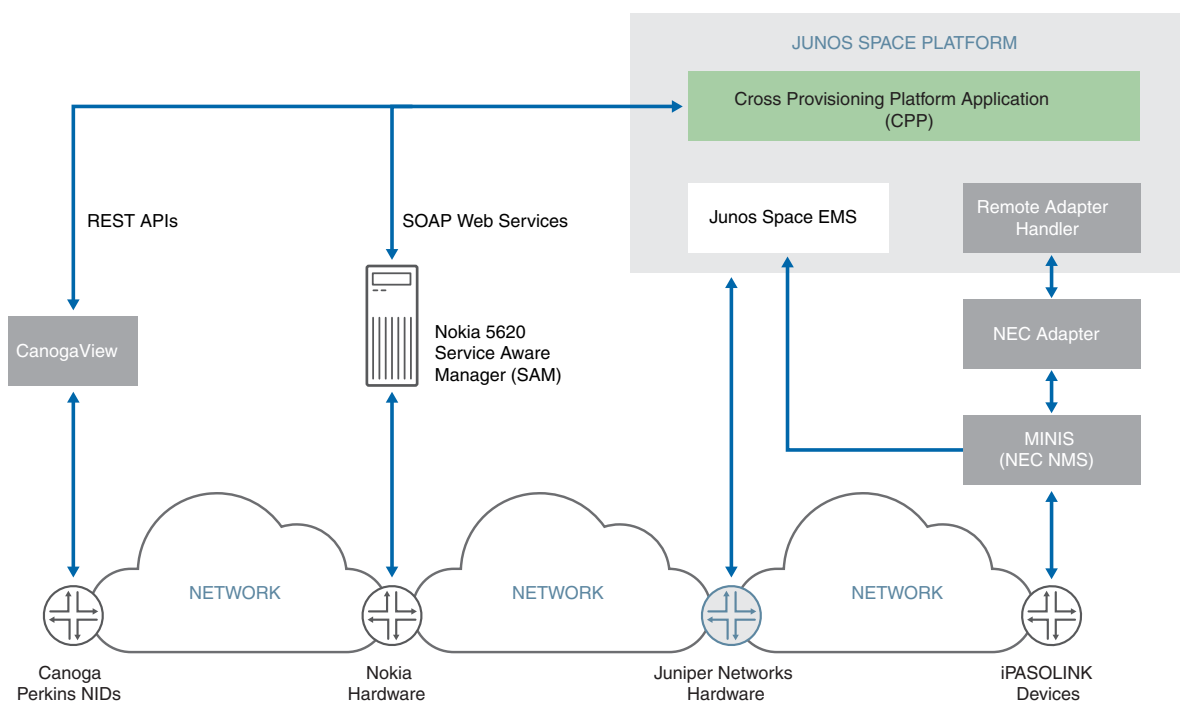
In addition to provisioning Juniper Networks devices, Nokia devices, and NEC's iPASOLINK devices, the CPP application can provision services across Juniper Networks devices and Canoga Perkins network interface devices (NIDs).

To provision end-to-end services across Juniper Networks devices and Canoga Perkins NIDs, Cross Provisioning Platform integrates with an Element Management System, CanogaView. The CanogaView has a customized Bell Canada proprietary software, Bell Interface Module.

The Cross Provisioning Platform application integrates with CanogaView and uses the Bell Interface Module's REST APIs to provision end-to-end services across Juniper Networks devices and Canoga Perkins NIDs.

[Figure 24 on page 883](#) illustrates the high-level architecture of how CPP communicates with multivendor devices including Canoga Perkins devices:

Figure 25: Cross Provisioning Platform High-Level Architecture



The Cross Provisioning Platform application supports the following Canoga Perkins NIDs:

- Model 9145E
- Model 9145ELB
- Model 9145EMP

The Vendor Type **Canoga** and the Device Role **NID** are added to existing Vendor Types and Device Roles in CPP to facilitate provisioning of services across the Juniper Networks devices and Canoga Perkins NIDs.

NOTE: The following functions that are part of the native CPP functionality are not supported on Canoga Perkins NIDs:

- Device Configlets
- Configuration audit
- Bulk Operations
- Interface migration
- Report Management

To provision services for Canoga Perkins NIDs by using CPP, you must:

- Configure the OSS parameters. For more information about configuring OSS parameters, see [“Configuring OSS Parameters for Canoga Perkins NIDs” on page 918](#).
- Add and synchronize Canoga Perkins NIDs. For more information about adding and synchronizing devices, see [“Adding a Canoga Perkins NID to Cross Provisioning Platform” on page 921](#) and [“Synchronizing Canoga Perkins NIDs with OSS” on page 922](#).
- Create service definitions. For more information about creating service definitions, see [“Creating a Service Definition for Canoga Perkins NIDs” on page 926](#).
- Create and deploy service orders. For more information about creating and deploying service orders, see [“Creating a Cross Provisioning Platform Service Order for Canoga Perkins NIDs” on page 929](#).

RELATED DOCUMENTATION

[Configuring OSS Parameters for Canoga Perkins NIDs | 918](#)

[Adding a Canoga Perkins NID to Cross Provisioning Platform | 921](#)

Configuring OSS Parameters for Canoga Perkins NIDs

Before you add Canoga Perkins network interface devices (NIDs), you must configure the Canoga Perkins operations support system (OSS) in the Network Management Platform.

To configure the Canoga Perkins OSS:

1. From the Network Management Platform UI, select **Administration > Applications**.

The Applications window appears.

2. Select **Cross Provisioning Platform** from the list of applications.

3. From the **Actions** menu, select **Modify Application Settings**.

The Modify Application Settings window appears.

4. Select **OSSConfigParameters**.

The OSSConfigParameters pane lists the OSS configuration parameters that you must configure for the following vendors:

- Alcatel OSS Configuration
- Canoga OSS Configuration

You can view or configure the OSS parameters.

5. In the OSSConfigParameters pane, select **Canoga OSS Configuration**.

The OSSConfigParameters pane lists a set of parameters that you can configure for Canoga Perkins NIDs.

6. Enter values for the required parameters.

OSS Parameter	Description
Primary Server IP	IP address of the primary server.
Primary Server Port	Port number of the primary server.
Backup Server IP	IP address of the backup server.
Backup Server Port:	Port number of the backup server.

OSS Parameter	Description
HTTP Connection Timeout (milliseconds)	Duration of HTTP connection (in milliseconds) before the timeout elapses.
Maximum API Requests	Maximum number of simultaneous API requests permitted.
Number of devices for sync with OSS request	The number of devices that must be queried in a single request while performing the synchronization.
OSS User Name	Username for accessing the OSS server.
OSS User Password	Password for accessing the OSS server.
Synchronize OSS Inventory daily at given time	<p>Time at which the CPP system synchronizes third-party devices, added or deleted from the CPP system, with the OSS server.</p> <p>NOTE: The time at which the synchronization job runs is associated with the location of the browser in which you are using the Junos Space software. That is, the synchronization job runs according to the browser time where the job is scheduled, not according to the time where the Junos Space server is located.</p>
Use primary server	<p>Specifies whether the CPP system communicates with the primary OSS server or the backup server.</p> <p>If this check box is selected, the CPP system communicates with the primary OSS server. If the check box is not selected, the system interacts with the backup server.</p>
Use HTTP protocol	<p>Specifies whether the CPP system must use the HTTP protocol.</p> <p>If this check box is selected, the CPP system uses the HTTP protocol.</p> <p>The default protocol is HTTPS.</p>

7. Click **Modify** after you finish entering values for **OSSConfigParameters** fields.

The Canoga Perkins OSS is configured. You can test if the OSS is configured correctly by following the procedure described in [“Confirming Communication with Canoga Perkins OSS Server”](#) on page 920.

RELATED DOCUMENTATION

[Cross Provisioning Platform for Canoga Perkins NIDs Overview](#) | 916

[Confirming Communication with Canoga Perkins OSS Server | 920](#)

[Adding a Canoga Perkins NID to Cross Provisioning Platform | 921](#)

[Synchronizing Canoga Perkins NIDs with OSS | 922](#)

Confirming Communication with Canoga Perkins OSS Server

You can check if the Cross Provisioning Platform can establish a communication with the CanogaView OSS. Before you check the communication between Cross Provisioning Platform and the CanogaView operations support system (OSS), ensure that the OSS parameters are configured in the Network Management Platform application.

To confirm if Cross Provisioning Platform can establish a communication with the CanogaView OSS:

1. In the Cross Provisioning Platform task pane, select **CPP > Third-Party Devices**.

The Third-Party Devices window appears.

2. Click the **Ping OSS Server** icon in the command bar.

The Select Vendor window appears.

3. Select the Vendor Type as **Canoga**.

The primary IP address and the secondary IP address of the vendor is displayed.

4. Click **Ok**.

The Cross Provisioning Platform application pings the primary IP address of the CanogaView OSS to establish communication. If the primary IP address is not reachable, the Cross Provisioning Platform application pings the secondary IP address to establish communication.

The **Ping OSS – Status** window appears, which indicates:

- Whether or not the CPP system has access to the CanogaView OSS server.
- Whether the primary IP address or the secondary IP address is used for establishing the communication.

[RELATED DOCUMENTATION](#)

Adding a Canoga Perkins NID to Cross Provisioning Platform

The Cross Provisioning Platform application supports the following Canoga Perkins network interface devices (NIDs):

- Model 9145E
- Model 9145ELB
- Model 9145EMP

The device role for Canoga Perkins network interface devices is **NID**, with service capability of **L2** and **L3**.

To add a Canoga Perkins NID to the Cross Provisioning Platform application:

1. In the Cross Provisioning Platform task pane, select **CPP > Third-Party Devices**.
2. Click the **Add Third-Party Device** icon.

The Add Third-Party Device appears.

3. Click **IP Address** option

You can add a third-party device either using the host name of the device or IP address of the device. Because the Canoga Perkins NIDs do not have a host name and are identified by a non-unique ID along with the device name, you cannot add a Canoga Perkins NID using the host name.

4. In the **IP Address** field, specify the IP address of the Canoga Perkins NID.
5. In the Vendor field, select **Canoga**.

6. Click **Add**.

After the job completion, the Third-Party Devices landing page lists the Canoga Perkins NID that you have added.

The Third-Party Devices landing page allows you to view and filter third-party devices that you have added based on the vendor type.

RELATED DOCUMENTATION

[Cross Provisioning Platform for Canoga Perkins NIDs Overview | 916](#)

[Configuring OSS Parameters for Canoga Perkins NIDs | 918](#)

[Confirming Communication with Canoga Perkins OSS Server | 920](#)

Synchronizing Canoga Perkins NIDs with OSS

IN THIS SECTION

- [Synchronize All Canoga Perkins NIDs with OSS | 922](#)
- [Synchronize Selected Canoga Perkins NIDs with OSS | 923](#)
- [Resynchronize Failed Canoga Perkins NIDs based on the Port Number | 924](#)
- [Schedule OSS Synchronization for Canoga Perkins NIDs | 924](#)
- [Cancel OSS Synchronization for Canoga Perkins NIDs | 924](#)

You can perform the following synchronization operations after you have added Canoga Perkins network interface devices (NIDs):

Synchronize All Canoga Perkins NIDs with OSS

You can synchronize all Canoga Perkins NIDs with the OSS to ensure that all the Canoga Perkins NIDs managed in the CanogaView OSS are staged to the Cross Provisioning Platform application.

To synchronize all Canoga Perkins NIDs:

1. In the Cross Provisioning Platform task pane, select **CPP > Third-Party Devices**.

The Third-Party Devices window appears.

2. Select the **Synchronize all the devices with OSS** icon.

The OSS Synchronization window appears.

3. In the Vendor field, select **Canoga**.

NOTE: Select **All** in the Vendor field to synchronize all third-party devices.

4. Click **Sync**.

A job is created to synchronize all Canoga Perkins NIDs with OSS.

Synchronize Selected Canoga Perkins NIDs with OSS

You can synchronize selected Canoga Perkins NIDs with the OSS to ensure that the selected Canoga Perkins NIDs managed in CanogaView are staged to the Cross Provisioning Platform application.

To resynchronize information for Canoga Perkin NIDs that you have selected:

1. In the Cross Provisioning Platform task pane, select **CPP > Third-Party Devices**.

The Third-Party Devices window appears.

2. Select one or more Canoga Perkins NIDs.

You can select up to 10 NIDs. If you want to select more than 10 NIDs, you must increase the value of the **Number of devices for sync with OSS request** field in **OSSConfigParameters > Canoga OSS Configuration**.

3. Select the **Synchronize selected devices with OSS** icon.

The Synchronize selected devices with OSS window appears.

4. In the **Vendor** field, select Canoga.

NOTE: Select **All** in the Vendor field to synchronize all third-party devices.

5. Click **Sync**.

A job is created to resynchronize the selected Canoga Perkins NIDs with OSS.

Resynchronize Failed Canoga Perkins NIDs based on the Port Number

This operation is not applicable for Canoga Perkins NIDs as the ports are synchronized and fetched statically.

Schedule OSS Synchronization for Canoga Perkins NIDs

You can schedule a synchronization of Canoga Perkins NIDs with the OSS.

To schedule synchronization of Canoga Perkins NIDs:

1. In the Cross Provisioning Platform task pane, select **CPP > Third-Party Devices**.

The Third-Party Devices window appears.

2. Select the **Schedule OSS Synchronization Job** icon.

The Schedule OSS Synchronization window appears.

You can configure the synchronization schedule time in **OSSConfigParameters > Canoga OSS Configuration > Synchronize OSS Inventory daily at given time**. The default value is 5:00 AM.

3. In the **Vendor** field, select Canoga.

NOTE: Select **All** in the Vendor field to schedule synchronization of all third-party devices.

4. Click **Schedule**.

The synchronization schedule for Canoga Perkins NIDs is updated.

Cancel OSS Synchronization for Canoga Perkins NIDs

You can cancel the synchronization of Canoga Perkins NIDs that you have scheduled.

To cancel synchronization of Canoga Perkins NIDs:

1. In the Cross Provisioning Platform task pane, select **CPP > Third-Party Devices**.

The Third-Party Devices window appears.

2. Select the **Cancel OSS Synchronization** icon.

The Cancel OSS Synchronization window appears.

3. In the Vendor field, select **Canoga**.

NOTE: Select **All** in the Vendor field to cancel synchronization of all third-party devices.

4. Click **OK**.

A status of the cancelled synchronization is listed.

RELATED DOCUMENTATION

[Configuring OSS Parameters for Canoga Perkins NIDs | 918](#)

[Confirming Communication with Canoga Perkins OSS Server | 920](#)

[Adding a Canoga Perkins NID to Cross Provisioning Platform | 921](#)

[Synchronizing Canoga Perkins NIDs with OSS | 922](#)

Adding Canoga Perkins Scripts

Before you can create a Cross Provisioning Platform service definition, you must add scripts that enable management of the Juniper Networks devices and Canoga Perkins NIDs.

There are three types of scripts:

- GUI Script—Provides the code that renders the Cross Provisioning Platform GUI window required for provisioning a Juniper Networks device.
- Junos Configuration Script—Provides the code that enables provisioning of a particular Juniper Networks device.
- Canoga Configuration Script—Provides the code that enables provisioning of the Canoga Perkins NID.

To add a script into the system:

1. In the Cross Provisioning Platform task pane, select **CPP > Scripts**.
2. Select the **Create Scripts** icon on the command bar (+).

The Create Script window appears.

3. In the Name field, specify the name of the script.
4. In the Description field, specify a short description for the script that you are adding.
5. In the Version field, view the version number. This is a read-only field.
6. In the Vendor Type field, select **Canoga**.

NOTE: If you remotely access the server on which the Junos Space software is installed, you must copy the scripts you intend to add to the CPP system, to your local client file system. That is, when you click on **Browse** to select a script, which you want to add, Junos Space opens the local client file system, not the file system of the server on which Junos Space is installed.

7. In the Configuration Script field, click **Browse** to add scripts from your local client file system to the Cross Provisioning Platform application.

If you select a third-party in the Vendor type field, the Add Script window displays a field for selecting a Configuration Script only.

8. Click **Create**.

The script is added to the CPP application.

RELATED DOCUMENTATION

[Importing Scripts Created for Cross Provisioning Platform | 778](#)

[Modifying Scripts Created for Cross Provisioning Platform | 779](#)

[Exporting Scripts Created for Cross Provisioning Platform | 776](#)

[Viewing Scripts Created for Cross Provisioning Platform | 781](#)

Creating a Service Definition for Canoga Perkins NIDs

Before you create a Cross Provisioning Platform (CPP) service definition, you must complete the following tasks:

- Import scripts that define Juniper Networks devices into the system.
- Import scripts that define Canoga Perkins NIDs into the system.

To create a service definition for Canoga Perkins NIDs:

1. In the **Cross Provisioning Platform** task pane, select **CPP > Service Definition**.

The Service Definition window appears.

2. Click **+**. The Create Service Definition window appears.

3. Enter values for the required parameters.

Parameter	Description
Name	Enter a name for the service definition.
ID	<p>Enter a unique ID to associate with this service definition in the range 1 through 2147483647.</p> <p>NOTE: The service definition ID is optional. If you do not provide any value in this field, the default value is -1. In the service definition selection grid, no value is displayed in the ID column. Each service definition is assigned a unique ID. If you give an existing ID value while creating a new service definition, an error occurs.</p>
Description	Enter a description of the service to distinguish the operation from others.
Type	<p>Select the service type from the list of available types:</p> <ul style="list-style-type: none"> • Predefined service types <ul style="list-style-type: none"> • PW-LDP • PW-BGP • VPLS • L3VPN • BNG • NPS • VLAN-PATH • Device • Report • PW-LDP-IPASO • L3VPN-IPASO • Customized service types <p>NOTE: You can create additional service types in the CPP > Service Types page.</p>

Parameter	Description
Operation Type	<p>Select one of the following operation type:</p> <ul style="list-style-type: none"> • Create—Select this operation type to associate service creation scripts to the service definition. • Modify—Select this operation type to associate service modification scripts to the service definition.
Select Scripts	<p>Select a Canoga Perkins script.</p> <p>The Select Scripts section lists the scripts that belong to various vendors along with the script version number. To find the script that you want to add, you can perform a search by using the search box.</p>
Add Script	Click Add Scripts to add a script to the service definition.
Selected Script	<p>The Selected Scripts section lists the scripts that you have selected. The scripts are listed based on the vendor type and operation type.</p> <p>To delete a script, in the Action column click the delete icon.</p>

4. Click **Create**.
5. In the **Cross Provisioning Platform** task pane, select **CPP > Service Definitions**.
6. Select the service definition you just created and select **Action > Publish Service Definition**. The **State** column indicates when the service definition is published.

The value in the **ID** field is associated with a service definition. This identifier can be used when you are searching for a particular service definition while creating a service order. You can search the service definition by its name, type or unique ID. You can modify the ID only during the migration of old service definition IDs.

During migration, the default value of the ID is -1. You can modify this value using database executable scripts during migration.

The migration scripts enable you to update the existing service definitions with IDs. A **csv** file that contains the service definition names and their unique identifiers is provided as an input. The migration script reads the names of the service definitions and the corresponding unique identifiers from the file and updates the service definitions in the database service policy table.

RELATED DOCUMENTATION

Creating a Cross Provisioning Platform Service Order for Canoga Perkins NIDs

Before you create a service order, you must:

- Import into the system the scripts that define the Juniper Networks devices.
- Import into the system the scripts that define Canoga Perkins NIDs.
- Create the service definition upon which to base the service order.

To create a Cross Provisioning Platform service order:

1. In the **Cross Provisioning Platform** task pane, select **CPP > Service Orders**.

The Service Orders window appears.

2. Click the + button.

The **Create CPP Service Order** window appears.

3. In the **General Settings** section, select a Canoga Perkins service definition that you have created.

NOTE: The value in the **ID** field is associated with a service definition. This identifier can be used when you are searching for a particular service definition while creating a device configlet order. You can search the service definition by its name, type or unique ID. You can modify the ID only during the migration of old service definition IDs.

4. In the **Order Description** field, enter a description of the service that distinguishes its operation from others.

5. Click **Next**.

The Endpoint Settings window appears.

NOTE: The following representation of the Endpoint Settings window is a sample only. The fields displayed in this window are dependent based on scripts that are associated with the service definition on which the service order is based.

Elina LDP -- Endpoint Settings

General

Name: SO1126190777

Description:

Signaling: LDP

VCID

Manual VCID ? ☐

VCID: Please enter

Site A - Endpoint

Site name: Please select

Port: Please select **View**

Speed: 1mbps

Traffic type: Please select

SVLAN: Please enter **Validate**

CVLAN: Please enter

L2E-NID Extension: ☐

NID Extension: ☒

L2E Setting **NID Setting**

EVC ID: Please enter

Site name: Please select

UNI port: Please select

Policer Bandwidth Profile: Please select

CVID: Please enter

Multiplexing: Please select

COS: Please select

Site B - Endpoint

Site name: Please select

Port: Please select **View**

Speed: 1mbps

Traffic type: Please select

SVLAN: Please enter **Validate**

CVLAN: Please enter

L2E-NID Extension: ☐

NID Extension: ☒

L2E Setting **NID Setting**

EVC ID: Please enter

Site name: Please select

UNI port: Please select

Policer Bandwidth Profile: Please select

CVID: Please enter

Multiplexing: Please select

COS: Please select

Create Clear Create More Verify Cancel

6. For a Canoga Perkins NID, enter information for NID parameters in the NID Settings tab according to the descriptions in the following table:

Parameter	Description
EVC ID	Enter Ethernet virtual connection (EVC) ID of the specific NID endpoint.
Site Name	Select a Canoga Perkins NID from the list of NIDs displayed.
UNI Port	Select a UNI port from the list of ports displayed.
Policer Bandwidth Profile	Select a policy bandwidth profile from the list. This list is based on the device family type that you have selected in the Site Name field.

Parameter	Description
CVID	Specify the CVID. NOTE: The maximum value for this field is 4095.
Multiplexing	Select one of the option: <ul style="list-style-type: none"> • SERVICE_MUX • ALL_TO_ONE
COS	Select one of the option: <ul style="list-style-type: none"> • STD • PRI • MCOS

7. Click **Create**.

8. (Optional) Click **Create More** to provision additional endpoints.

The service order is created.

After you create a service order, you must deploy the service order. For more information about deploying a service order, see [“Deploying a Service Order” on page 631](#).

RELATED DOCUMENTATION

[Cross Provisioning Platform for Canoga Perkins NIDs Overview | 916](#)

[Creating a Service Definition for Canoga Perkins NIDs | 926](#)

[Performing Service Activation Test | 931](#)

Performing Service Activation Test

You can perform service activation test on services between Juniper Networks devices and Canoga Perkins NIDs.

Before you perform the service activation test you must load the Stylesheet Language Alternative Syntax (SLAX) script in **Network Management Platform > Images and Scripts > Scripts**.

To perform service activation test :

1. In the **Cross Provisioning Platform** task pane, select **CPP > Services**.

The Services page appears.

2. Select and double-click a service.

The View Service window appears.

3. Select a Canoga Perkins NID for which you have to perform the service activation test.

4. Right-click the Canoga Perkins NID that you have selected, and select **Execute Op Script** to execute a SLAX script for performing the service activation test.

The Execute OP Scripts window appears.

5. Specify values for the required parameters.

NOTE: The parameters that are displayed are based on the script that you have attached.

6. Click **Execute**.

A job is created. After the job is successfully completed you can view the results in the Job Details window.

RELATED DOCUMENTATION

[Creating a Service Definition for Canoga Perkins NIDs | 926](#)

[Creating a Cross Provisioning Platform Service Order for Canoga Perkins NIDs | 929](#)

29

CHAPTER

Service-Level Alarms

[Viewing Service-Level Alarms in Network Activate](#) | 934

Viewing Service-Level Alarms in Network Activate

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.

To access the OpenNMS tool, in **Network Activate** task pane, select **Service Provisioning** > **Manage Services**.

1. When the **Manage Services** page appears, select the entry for the service you want to look at.
2. Right-click or open the **Actions** menu.
3. Select **View Service Alarms**.

Service Provisioning > Manage Services

0 Actions

Name	Customer	State	FA Status	Fault Status	
VPLS_SO_withST	October	✔ Deployed	Pending	✔ Up	
SO_ELine-BGP-Dot1q-SingleVLAN_bulk_2	October	✔ Deployed	Pending	None	
SO_ELine-BGP-Dot1q-SingleVLAN_bulk_1	October	✔ Deployed	Pending	✖ Down	
LVPN_SO1	October	✔ Deployed	Pending	✔ Up	
VPLSSO_1	October	✔ Deployed	✖ Down	✔ Up	
P2P_QinQ_ALL_V...	October	✔ Deployed	✖ Down	None	
cfm_p2p_test	October	✔ Deployed	✔ Up	✔ Up	

Service

Audit

View Results

PM Statistics

View Service Alarms

Tag It

View Tags

UnTag It

None

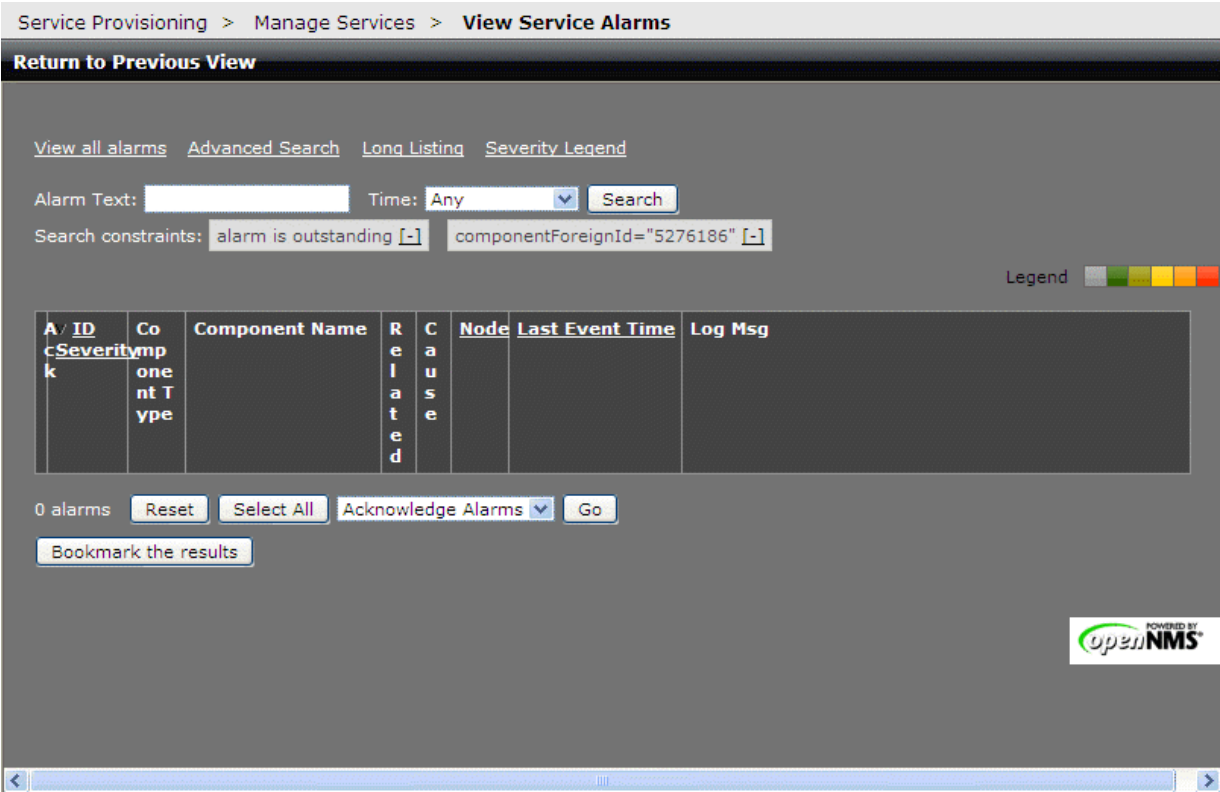
None

Page 1 of 1

Displaying 1 - 7 of 7

Show 30 items

4. From the actions list, select **View Service Alarms**.
- The OpenNMS **Network Monitoring** window appears.



From this window you can view the alarms associated with the service and search for specific alarms.

NOTE: The events listed here are based on the status of the **Decouple Service Status From Port Status** check box in the Point-to-Point and the Layer 3 Virtual Private Network service definition window.

RELATED DOCUMENTATION

- Viewing Services | 832
- SNMP MIBs and Traps Reference
- Junos Space Network Monitoring Reference

30

CHAPTER

Flexible Services

Configuring Flexible Service Attributes to Modify Service Template Attributes | **938**

Recovering Flex Services with Cross Provisioning Platform | **940**

Configuring Flexible Service Attributes to Modify Service Template Attributes

In addition to modifying a default service template attribute, you have the flexibility to:

- Add one or more optional service templates along with the existing default service template.
- Select a value for the attributes that are marked as dynamic. These values are listed from the devices.

If you have attached a service template to the service definition, you can modify the service template attributes by accessing the **Flexible Service Attributes** link. This link appears only in the Create Service Order and Modify Service windows.

NOTE: The **Flexible Service Attributes** link appears in the Modify Service window if you have attached a service template to the service definition, and enabled **Allow template modification for service** in the Junos Space Network Application Platform.

To enable **Allow template modification for service**:

1. Select **Network Management Platform > Administration > Manage Applications > Network Activate**.
2. Right-click the Network Activate application and select **Modify Application Settings**.
The Modify Network Activate Settings window is displayed.
3. Select **UI** in the left pane.
4. Select the **Allow template modification for service** check box.

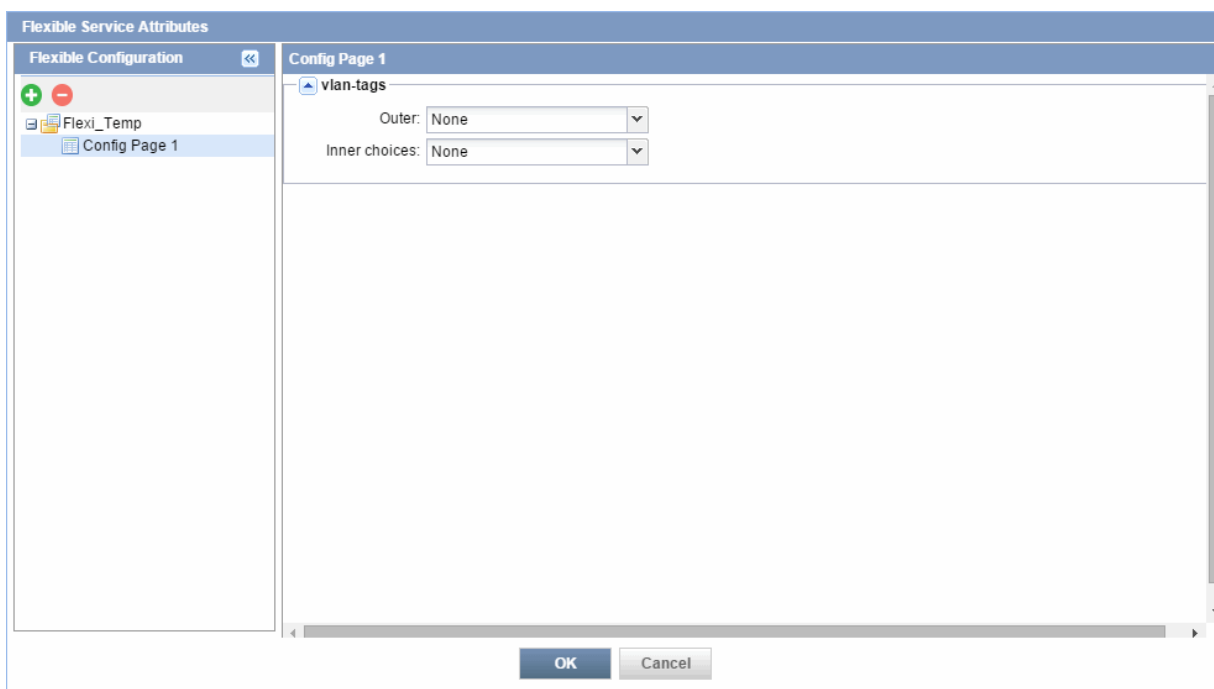
To modify the service template attributes in the Create Service Order or Modify Service window:

1. To access the **Flexible Service Attributes** link in the Create Service Order window, select **Service Provisioning > Manage Service Orders > Create Service Order**.

To access the **Flexible Service Attributes** link in the Modify Service window, select and right-click a service in **Service Provisioning > Manage Service**.

2. Click the **Flexible Service Attributes** link.

The Flexible Services Attributes window appears.



The Flexible Configuration pane lists all the service templates. The right pane lists the attributes of the selected template.

To add an optional template, click the plus symbol and select the templates.

3. (Optional) Modify the attributes, if necessary.

NOTE: Only for dynamic attributes, you can select a value from the list. These values are listed from the devices.



WARNING:

If an attribute is dynamic and the specified XPath contains no values, the following error message is displayed if you click the warning symbol:

No configuration present on device DeviceName for xpath. Default values from templates are shown. Please confirm that default configuration is present on device before deploying.

4. Click **OK**.

The service template attributes are modified.

RELATED DOCUMENTATION

Provisioning Dynamic Attributes to Specify the Device XPath	139
Creating a Point-to-Point ATM or TDM Pseudowire Service Order	578
Creating a Point-to-Point Service Order	586
Creating a Multipoint-to-Multipoint VPLS Service Order	660
Creating a Point-to-Multipoint VPLS Service Order	678
Creating a Full Mesh Layer 3 VPN Ethernet Service Order	718
Creating a Hub-and-Spoke Layer 3 VPN Service Order	733

Recovering Flex Services with Cross Provisioning Platform

IN THIS SECTION

- Before You Recover Flex Services | 941
- High-Level Workflow for Recovering a Flex Service | 941
- Workflow for Recovering a Complete Flex Service | 942
- List of REST APIs for Recovering a Flex Service | 943
- Mandatory Tags in the Payload for Recovering a Flex Service | 944

With Cross Provisioning Platform (CPP), you can schedule flex services to be periodically recovered from, imported to, and managed in Juniper Networks and Nokia devices by using REST APIs.

With Cross Provisioning Platform Release 15.1R1, you can recover only the following flex services:

- PW-LDP—The following combinations are supported: JNPR-JNPR, JNPR-ALU, ALU-JNPR, and ALU-ALU.
- PW-BGP—Only the JNPR-JNPR combination is supported.

This topic has the following sections:

Before You Recover Flex Services

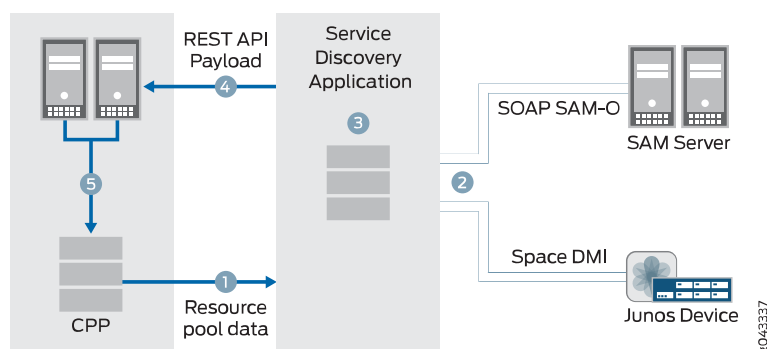
Before you recover flex services, ensure that:

- You have discovered and prestaged devices in the Cross Provisioning Platform application before you execute the REST API request from the Service Discovery application.
- You have created and published the service definition that is mentioned in the request payload.
- You have mentioned all mandatory tags in the payload.

High-Level Workflow for Recovering a Flex Service

Figure 26 on page 941 shows the high-level workflow for recovering a flex service with Cross Provisioning Platform.

Figure 26: High-Level Workflow for Recovering a Flex Service



The following high-level steps are included in the workflow for recovering a flex service:

1. The Service Discovery application collects resource pool data from the Cross Provisioning Platform database.
The Service Discovery application also collects data from Juniper Networks and Nokia devices.
2. The Service Discovery application compares the resource pool data in the Cross Provisioning Platform database with the data from the devices, based on the flex service type. The difference is converted into equivalent REST API payloads.

3. The Service Discovery application sends the payloads to the NetworkApps REST API.
4. The NetworkApps REST API validates the tags in the payload and manages the flex service without pushing the configuration to the devices.

The recovered flex service is listed on the CPP Services page.

Workflow for Recovering a Complete Flex Service

NOTE: With Cross Provisioning Platform Release 15.1R1, you cannot recover a flex service partially.

The following steps are involved in recovering a complete flex service:

1. When the Service Discovery application sends the REST API payload with the operation type as Recover, the NetworkApps REST API searches for an old service order whose status is Failed and has the same payload resources.

If such a service order exists, then the NetworkApps REST API removes it and proceeds with validation.

NOTE: While discovering services, a service order state can be Failed_Recovered, Completed, Invalid, or Scheduled.

2. The NetworkApps REST API constructs the service recovery service order and validates the tags in the payload.

NOTE: If the service recovery service order fails, an error message is logged and propagated to the Service Discovery application.

3. The NetworkApps REST API sends the service recovery service order to the service activation workflow.
If the service recovery is successful, the NetworkApps REST API saves the recovered service in the Cross Provisioning Platform database.
Otherwise, an error message is logged.

NOTE: The **Recreate Service Order** option is unavailable for the recovered service orders whose status is Failed or Invalid.

List of REST APIs for Recovering a Flex Service

Table 38 on page 943 lists the REST APIs used to recover a flex service:

Table 38: REST APIs for Recovering a Flex Service

REST API	Description
<code>getAllAllocatedVCID(@Context HttpServletRequest request)</code>	Lists all allocated VCIDs Every Virtual Chassis configuration has a unique ID (VCID) that is automatically assigned when the Virtual Chassis configuration is formed.
<code>getAllAllocatedForeignSvcId(@Context HttpServletRequest request)</code>	Lists all allocated foreign VCIDs
<code>getAllAllocatedTypeORT(@PathParam("serviceType") String serviceType, @Context HttpServletRequest request)</code>	Lists all allocated route targets based on the service type
<code>getAllAllocatedTypeORD(@PathParam("serviceType") String serviceType, @Context HttpServletRequest request)</code>	Lists all allocated route distinguishers based on the service type
<code>getAllServiceCommonAttributeValues(@PathParam("resourceName") String resourceName, @Context HttpServletRequest request)</code>	Lists the resource value based on the resource name from the common service attributes
<code>getAllServiceEndpointsAttributeValues(@PathParam("resourceName") String resourceName, @Context HttpServletRequest request)</code>	Lists the resource value based on the resource name from the service endpoints
<code>createRecoveredServiceOrder(JAXBElement<ServiceOrderBean> requestBean, @Context HttpServletRequest request)</code>	Lists the difference used to construct the bundle of recovery request payloads. These payloads are called using this REST API.

Mandatory Tags in the Payload for Recovering a Flex Service

The Service Discovery application sends the payloads to the NetworkApps REST API. The `HttpServletRequest/ServiceOrderbean` API must include the recovery payload and operation type.

NOTE: The operation type must be either `Recover` or `Modify_Recover`.

The following tags are mandatory in the payload:

- resources

This tag is mandatory in the payload, except for Juniper Networks local switching services. Based on the service type, the tag includes data such as, `VCID`, `TypeORT`, `TypeORD`, and `FOREIGNSVCID`.

[Table 39 on page 944](#) lists the mandatory attributes for the **resources** tags for recovering a flex service:

Table 39: Mandatory Attributes for the resources Tag

Recovery Types	Devices	Mandatory Attributes
PWD-LDP Flex Service	JNPR-JNPR	<resources>[{"VCID":332}]</resources>
	JNPR-ALU	<resources>[{"VCID":332},{"FOREIGNSVCID":3332}]</resources>
	ALU-JNPR	<resources>[{"VCID":332},{"FOREIGNSVCID":3332}]</resources>
	ALU-ALU	<resources>[{"VCID":332},{"FOREIGNSVCID":3332}]</resources>
PWD-BGP Flex Service	JNPR-JNPR	<resources>[{"TypeORT":"14"},{"TypeORD":"14"}]</resources>

- allocateResource

The default value for the `allocateResource` tag is `True`.

If the `allocateResource` tag is `True`, the payload allocates and validates the provided resources in the resource pool database.

If the `allocateResource` tag is `False`, the payload only saves the resource data in the CPP database and processes the service recovery workflow.

NOTE: `FOREIGNSVCID` is validated even if the `allocateResource` tag is `True`.

RELATED DOCUMENTATION

[Cross Provisioning Platform Overview | 33](#)

[Example: Creating Cross Provisioning Platform Services | 996](#)

31

CHAPTER

Device Configuration and Prestaging Examples

Example: Base Configuration for N-PE Device in a Multipoint Service | **947**

Example: Base Configuration for N-PE Device in a Point-to-Point Ethernet (LDP) Service | **949**

Example: Base Configuration for a P Router | **950**

Example: Base Configuration for BX7000 Multi-Access Gateway Supporting ATM and TDM Pseudowires | **953**

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 | 949](#)

[Example: Base Configuration for a P Router | 950](#)

[Example: Base Configuration for BX7000 Multi-Access Gateway Supporting ATM and TDM Pseudowires | 953](#)

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 | 947](#)

[Example: Base Configuration for a P Router | 950](#)

[Example: Base Configuration for BX7000 Multi-Access Gateway Supporting ATM and TDM Pseudowires | 953](#)

Example: Base Configuration for a P Router

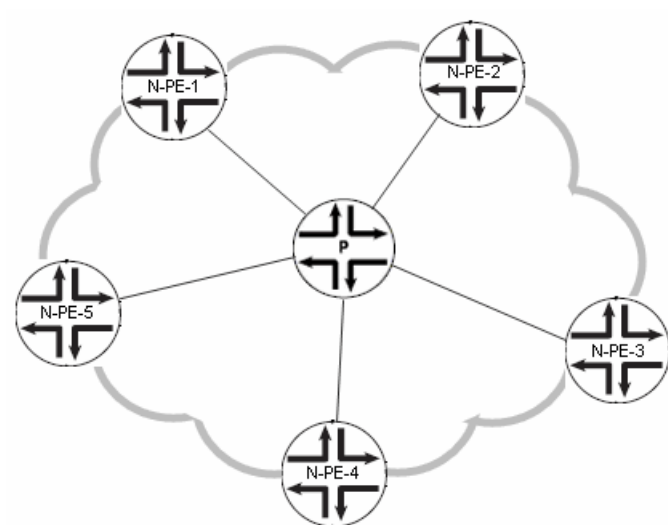
P routers in your MPLS network must have the following entities configured before these devices are prestaged:

- A Gigabit Ethernet interface to each router in the network
- Loopback interface
- MPLS protocol

- OSPF protocol
- LDP protocol

Figure 27 on page 951 shows a simple network with one P router connecting five N-PE routers.

Figure 27: Connectivity in a Simple Network



The following example shows a P router configuration for the simple network shown in Figure 27 on page 951.

```

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 | 947](#)

[Example: Base Configuration for N-PE Device in a Point-to-Point Ethernet \(LDP\) Service | 949](#)

[Example: Base Configuration for BX7000 Multi-Access Gateway Supporting ATM and TDM Pseudowires | 953](#)

Example: Base Configuration for BX7000 Multi-Access Gateway Supporting ATM and TDM Pseudowires

The configuration shown here is the base configuration required for a BX7000 Multi-Access Gateway to support ATM and TDM Pseudowires. This configuration shows 3 Gigabit Ethernet interfaces and 16 T1 interfaces that can be used for ATM or TDM pseudowires.

```

root@bx-csr0> show configuration
system {
    host-name bx-csr0;
    services ntp ;
    framer-mode t1;
    manual-mode config disable;
    zerotouch config disable;
    ssh protocol-version both;
    services ssh enabled;
}
interface {
    ge-1/0/0 {                                #ge interfaces are NNI interfaces
        admin-state enable;
        unit 0 {

```

```

        family inet address 192.168.183.138/25;
    }
}
ge-1/0/1 {
    admin-state enable;
    unit 0 {
        family inet address 10.10.183.138/25;
    }
}
ge-1/0/2 {
    admin-state enable;
    unit 0 {
        family inet address 10.0.88.2/30;
    }
}
lo0 {                                #lookback
    admin-state enable;
    unit 0 {
        family inet address 100.100.200.1/32;
    }
}
t1-0/0/0 { #t1-0/0/0, t1-0/0/1,t1-0/0/10-t1-0/0/15 here are for TDM P/W service
deployment
    admin-state enable;
}
t1-0/0/1 {
    admin-state enable;
}
t1-0/0/10 {
    admin-state enable;
}
t1-0/0/11 {
    admin-state enable;
}
t1-0/0/12 {
    admin-state enable;
}
t1-0/0/13 {
    admin-state enable;
}
t1-0/0/14 {
    admin-state enable;
}
t1-0/0/15 {

```

```

        admin-state enable;
    }
    t1-0/0/2 { #t1-0/0/2 -t1-0/0/9 here are for ATM P/W service deployment
        admin-state enable;
        encapsulation atm;
    }
    t1-0/0/3 {
        admin-state enable;
        encapsulation atm;
    }
    t1-0/0/4 {
        admin-state enable;
        encapsulation atm;
    }
    t1-0/0/5 {
        admin-state enable;
        encapsulation atm;
    }
    t1-0/0/6 {
        admin-state enable;
        encapsulation atm;
    }
    t1-0/0/7 {
        admin-state enable;
        encapsulation atm;
    }
    t1-0/0/8 {
        admin-state enable;
        encapsulation atm;
    }
    t1-0/0/9 {
        admin-state enable;
        encapsulation atm;
    }
}
protocols {
    ospf {
        admin-state enable;
        spf-delay 200;
        traffic-engineering enable;
        area 0.0.0.0 {
            interface ge-1/0/2 {
                admin-state enable;
            }
        }
    }
}

```

```

        interface lo0 {
            admin-state enable;
            mode passive;
        }
    }
}
ldp {
    admin-state enable;
    mpls ldp targeted-hello send remote-peer-ip; #this needs to be added
manually
    interface ge-1/0/2 {
        admin-state enable;
    }
    interface ge-1/0/1 {
        admin-state enable;
    }
    interface ge-1/0/0 {
        admin-state enable;
    }
}

rsvp {
    admin-state enable;
    interface ge-1/0/2 {
        admin-state enable;
        reliable enable;
        hello-interval 20;
    }
}

mpls {
    label-switch-path p2pdbhx1_32793 { #existing LSP is optional; one may use
Space Transport Activate to create such
        to-address 192.168.5.1;
        from-address 100.100.200.1;
        primary p2pdbhx1_32793 {
            priority 7 0;
        }
        path 10.100.200.100 loose;
    }

    static-path-inet st1_32770 { #existing static LSP is optional; one may use
Space Transport Activate to create such
        push 3;
        next-hop-address 10.0.88.1;
    }
}

```



```

        out-interface ge-1/0/2;
        ingress-address 100.100.200.1;
        egress-address 192.168.5.1;
    }

    interface ge-1/0/2 {
        admin-state enable;
    }
    interface ge-1/0/1 {
        admin-state enable;
    }
    interface ge-1/0/0 {
        admin-state enable;
    }
}

snmp {
    community-name public
    contact bx-admin;
}

connection {
}

policy-options {
}

bridge-domains {
}

static-route {
    route 0.0.0.0/0 {
        next-hop 192.168.183.254;
    }
}

routing-options {
    autonomous-system 65410;
}

```

RELATED DOCUMENTATION

[Prestaging Devices Overview | 36](#)

[Creating a Point-to-Point Service Order | 586](#)

[Discovering and Assigning All N-PE Devices | 68](#)

Prestaging ATM and TDM Pseudowire Devices | 46

Prestaging ATM and TDM Pseudowire Devices | 46

Creating a Point-to-Point ATM or TDM Pseudowire Service Order | 578

Creating a Point-to-Point ATM or TDM Pseudowire Service Definition | 270

32

CHAPTER

End-to-End Configuration Examples

Example: Configuring and Deploying a Point-to-Point Ethernet Service | **960**

Example: Configuring and Deploying a Multipoint-to-Multipoint VPLS Service | **972**

Example: Configuring and Deploying a Layer 3 VPN Full-Mesh Service | **986**

Example: Creating Cross Provisioning Platform Services | **996**

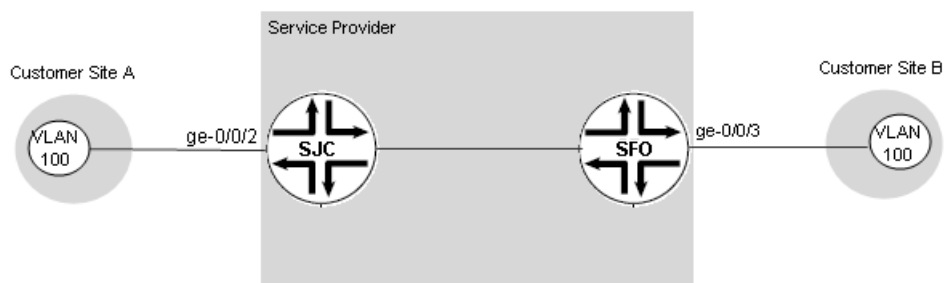
Example: Configuring and Deploying a Point-to-Point Ethernet Service

IN THIS SECTION

- [Preparing Devices for Discovery | 961](#)
- [Discovering Devices | 961](#)
- [Preparing Devices for Prestaging | 963](#)
- [Discovering and Assigning N-PE Roles | 965](#)
- [Choosing or Creating a Service Definition | 965](#)
- [Creating a Customer | 968](#)
- [Creating and Deploying a Point-to-Point Service Order | 969](#)
- [Performing a Functional Audit and a Configuration Audit | 970](#)

This example deploys and verifies a point-to-point Ethernet service starting with two MX Series devices. [Figure 28 on page 960](#) shows the service.

Figure 28: 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

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
```

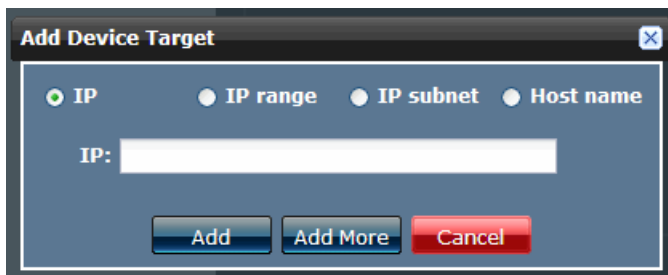
- The device is configured with a static management IP address that is reachable from the Junos Space server. The IP address can be in-band or out-of-band.
- A user with full administrative privileges is created on the device for the Junos Space administrator.
- If you plan to use SNMP to probe devices 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:

1. Log in to Junos Space using your credentials.
2. In the Network Activate task pane, select **Devices > Discover Devices > Discover Targets**.
3. In the **Discover Targets** window, click +.

The **Add Device Target** window appears.

A screenshot of a software dialog box titled "Add Device Target". The dialog has a dark blue header bar with the title and a close button (X). Below the header, there are four radio buttons: "IP" (selected), "IP range", "IP subnet", and "Host name". Under the "IP" radio button, there 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).

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...	Conne...	Manag...	Authen...
access-bt750	View	View	3.0.0	B-7510	Juniper Networ...	3.0.0	10.216...	up	In Sync	Crede... Based
access-hd-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...	M7I	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 Activate software for N-PE devices and UNIs.

1. In the **Network Activate** task pane, select **Prestage Devices > Manage Device Roles**.

This action launches the role discovery process in which the Network Activate software 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 Activate software has discovered two such devices.

2. In the **Assign Roles** window, switch to multiple selection mode and select both N-PE devices.

3. Open the **Actions** menu and select **Assign NPE role**.

4. In the **Assign NPE** window, click **Assign** to confirm the assignment.

5. To view the assignment status, in the **Job Details** window, click the job ID of the assignment job.

The **Job Management** page shows the progress and status of the role assignment job.

6. To verify the result, in the Network Activate task pane, select **Prestage Devices > Manage Device Roles**.

The **Manage Device Roles** window shows two devices that can be used for provisioning.

SEE ALSO

[Prestaging Devices Overview | 36](#)

[Discovering and Assigning All N-PE Devices | 68](#)

[Discovering and Assigning N-PE Devices with Exceptions | 71](#)

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 Activate software ships with standard service definitions. First, we check the standard service definitions to determine whether one already exists that will work.

1. In the Network Activate task pane, select **Service Design > Manage Service Definitions**.

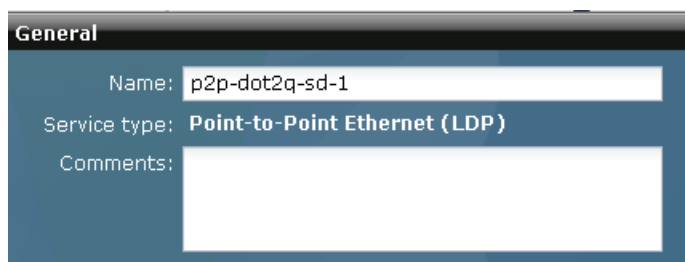
The **Manage Service Definitions** page lists all service definitions in the system. In a new system, the screen lists only predefined service definitions.

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.

2. In the **Network Activate** task pane, select **Service Design > Manage Service Definitions > Create P2P Service Definition**.

The General window appears.

3. Enter a name for the service definition. For this example, enter **p2p-dot1q-sd-1**.



General

Name: p2p-dot2q-sd-1

Service type: Point-to-Point Ethernet (LDP)

Comments:

4. Click **Next**.

The **UNI Settings** window appears.

5. In the **Connectivity Settings** window, to pick the default connectivity settings, click **Next**.

6. In the **UNI Settings** window, in the **Ethernet option** field, select **dot1q**.

7. In the **Customer traffic type** field, select **Transport single VLAN**.

8. In the **VLAN ID selection** field, select **Select manually**.

9. In the **VLAN range for manual input** field, specify the range.

10. In the **Outer Tag protocol ID** field, select **0x88a8**

11. In the **Physical IF encapsulation** field, select **flexible-ethernet-services**.

12. In the **Logical IF encapsulation** field, select **vlan-ccc**.

13. In the **Bandwidth Settings** panel, select the **Enable rate limiting** check box.

14. In the **Default Bandwidth** field, enter **10**, for a default bandwidth of 10 Mbps.

15. 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.

16. In the **Min Bandwidth (Kbps)** field, enter **100**.

17. In the **Max Bandwidth (Mbps)** field, enter **10000**.

18. 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.

Service Design > Manage Service Definitions > Create P2P Service Definition

UNI Settings

Traffic Treatment

Ethernet option: dot1q

Customer traffic type: Transport single vlan

VLAN ID selection: Select manually

VLAN range for auto-pick:

VLAN range for manual input: 25

Outer Tag protocol ID: 0x88a8

Inner Tag protocol ID: Please select ...

Interface Settings

Physical IF encapsulation: flexible-ethernet-services

Logical IF encapsulation: vlan-ccc

MTU Settings

Physical MTU (B): 1500

Create P2P Service Definition

General

UNI Settings (*)

Connectivity (*)

Back Next Finish Cancel

19. 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.

20. To publish the service definition, in the **Manage Service Definitions** page, select the **p2p-dot1q-sd-1** service definition; then in the **Actions** menu, select **Publish Service Definition**.

The **Publish Service Definition** window appears.

21. 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.

SEE ALSO

[Predefined Service Definitions | 408](#)

[Creating an E-Line Service Definition | 188](#)

[Publishing a Custom Service Definition | 308](#)

Creating a Customer

Before you can provision the service, customer details must be present in the Junos Space database. To add a customer:

1. In the **Network Activate** task pane, select **Service Provisioning > Manage Customers > Create Customer**.
2. In the **Name** field, enter **Best Customer**.
3. In the **Account number** field, enter **1234**.
4. Click **Create**.

The **Manage Customers** page shows the new customer.

SEE ALSO

[Adding a New Customer | 1056](#)

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. In the **Network Activate** task pane, select **Service Provisioning > Manage Service Orders > Create P2P Service Order**.

2. In the **Create P2P Service Order** window, select the service named **p2p-dot1q-sd-1**.

This is the customized service definition you created earlier.

3. Click **Next**.

4. In the **General/Connectivity Settings** window, in the **Name** field, enter **so_1**.

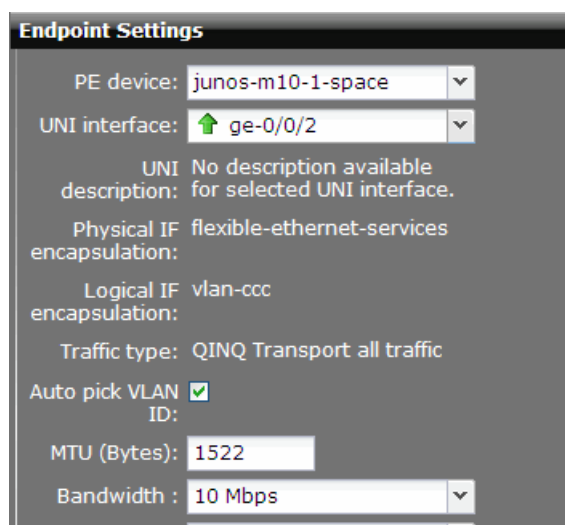
5. In the **Customer** field, select **Best Customer**.

6. Click **Next**.

The **Endpoint Settings** window appears.

7. For endpoint A, in the **PE device** field, select **SJC**.

8. In the **UNI interface** field, select **ge-0/0/2**.



The screenshot shows the **Endpoint Settings** window with the following configuration:

- PE device:** junos-m10-1-space
- UNI interface:** ge-0/0/2
- UNI description:** No description available for selected UNI interface.
- Physical IF encapsulation:** flexible-ethernet-services
- Logical IF encapsulation:** vlan-ccc
- Traffic type:** QINQ Transport all traffic
- Auto pick VLAN ID:** ☒
- MTU (Bytes):** 1522
- Bandwidth:** 10 Mbps

9. In the **VLAN-ID** field, enter **100**.

10. Click **Next**.
11. In the **Endpoint Settings** window for endpoint Z, in the **PE device** field, select **SFO**.
12. In the **UNI interface** field, select **ge-0/0/3**.
13. In the **Bandwidth** field, select **25**.
14. Click **Create**.
15. In the **Deployment Options** window, select **Deploy now**.
16. Click **OK** to start the deployment.
17. 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.
18. When you see in the **Job Management** window that the deployment is successful, in the **Network Activate** task pane, select **Service Provisioning > Manage Services**.
The **Manage Services** page shows the new service.

SEE ALSO

[Creating a Point-to-Point Service Order | 586](#)

[Deploying a Service Order | 631](#)

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. In the **Manage Services** page, select the service instance you just deployed.
2. Right-click on the service instance or open the **Actions** menu and select **Perform Functional Audit**.

3. 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**.
4. In the **Order Information** screen, click **OK**.
5. Right-click on the service instance or open the **Actions** menu and select **Perform Configuration Audit**.
6. 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**.
7. 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.

8. To view the functional audit results:
 - a. In the **Manage Services** page, select the **so_1** service instance.
 - b. Open the **Actions** menu and select **View Functional Audit Results**.
 - c. In the **Functional Audit Results** window, select each device to view the results.
9. To view the results of the configuration audit:
 - a. Open the **Actions** menu and select **View Configuration Audit Results**.
 - b. 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

[Prestaging Devices Overview | 36](#)

[Discovering and Assigning All N-PE Devices | 68](#)

[Discovering and Assigning N-PE Devices with Exceptions | 71](#)

Predefined Point-to-Point Service Definitions	477
Creating an E-Line Service Definition	188
Publishing a Custom Service Definition	308
Adding a New Customer	1056
Creating a Point-to-Point Service Order	586
Performing a Functional Audit	1064
Deploying a Service Order	631
Understanding Service Validation	875
Deploying a Service Order	631
Monitoring Performance Management Statistics	1091
Viewing Performance Management Statistics	1094

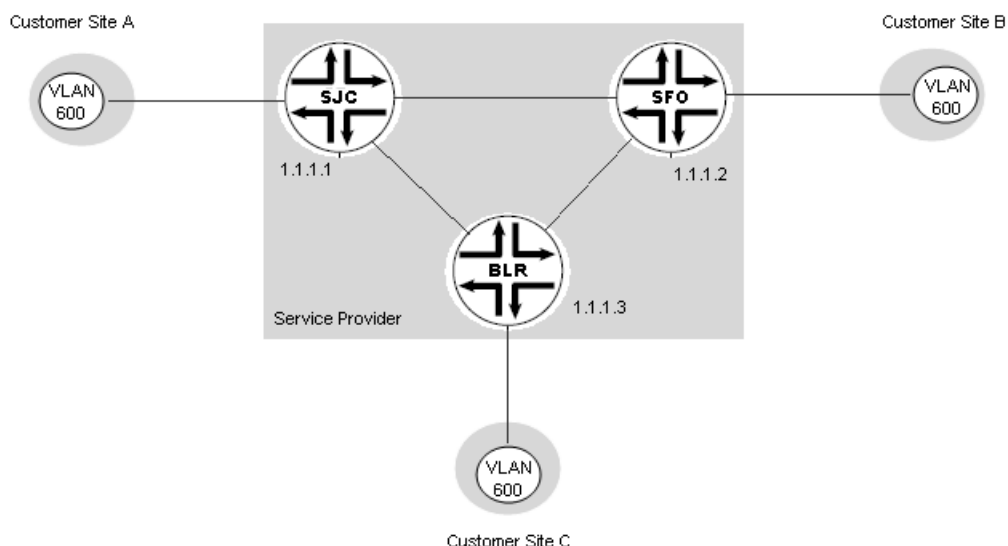
Example: Configuring and Deploying a Multipoint-to-Multipoint VPLS Service

IN THIS SECTION

- [Preparing Devices for Discovery | 973](#)
- [Discovering Devices | 974](#)
- [Preparing Devices for Prestaging | 975](#)
- [Discovering and Assigning N-PE Roles | 978](#)
- [Choosing or Creating a Service Definition | 979](#)
- [Creating a Customer | 982](#)
- [Creating and Deploying a Multipoint-to-Multipoint Service Order | 983](#)
- [Performing a Functional Audit and a Configuration Audit | 984](#)

This example shows how to deploy and verify a multipoint-to-multipoint VPLS service starting with three MX Series routers. [Figure 29 on page 973](#) shows the service.

Figure 29: 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 . Customer site B connects to the network through an N-PE device named SFO . Customer site C connects to the network through an N-PE device named BLR. 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

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
```

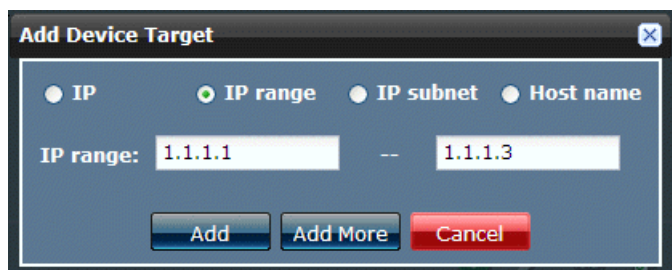
- The device is configured with a static management IP address that is reachable from the Junos Space server. The IP address can be in-band or out-of-band.

- 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.

1. Log in to Junos Space using your credentials.
2. In the Applications Chooser, select **Platform > 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 > Discover Devices > Specify Probes** window, select both **Ping** and **SNMP** as probes.
8. Click **Next**.
9. In the **Devices > Discover 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.

- 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.

The screenshot shows the 'Manage Devices' page in Junos Space. The page header indicates '0 Items Selected'. The table below lists various network devices, including access routers, embassy, exora, jaipur, and Junos MX series devices. Each row provides details on the device name, physical and logical interfaces, OS version, platform, vendor, schema, IP address, connection status, management status, and authentication method.

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...	M7I	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

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**:

<Device name> should be configured with static VPLS no tunnel service rule.

To discover the roles of the various network elements configured:

1. Select **Network Activate > Prestage Devices > Manage Device Roles**.
2. Select **Discover Roles** to view the relevant window.
3. Click **Continue** to view the **Role Discovery Status** window.

The **Role Discovery Status** window displays a graph which shows the number of unassigned devices that could be assigned the role of **N-PE** or **PE**.

To re-sync the role of the network elements configured:

1. Select **Network Activate > Prestage Devices > Manage Device Roles**.
2. To re-sync the role capability of a network element, right-click the network element's name.
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 Activate software for N-PE devices and UNIs.

1. In the Application Chooser, select **Network Activate**:
2. In the Network Activate task pane, select **Prestage Devices > Manage Device Roles > Discover Roles**.

This action launches the role discovery process in which the Network Activate software examines the devices under Junos Space management looking for devices that match predefined rules that identify N-PE devices. The Role Discovery Status graph shows that, in this case, the Network Activate software has discovered three such devices.
3. In the **Assign Roles** window, switch to multiple selection mode and select both N-PE devices.
4. Open the **Actions** menu and select **Assign NPE role**.
5. In the **Assign NPE** window, click **Assign** to confirm the assignment.
6. To view the assignment status, in the **Job Details** window, click the job ID of the assignment job.

The **Job Management** page shows the progress and status of the role assignment job.
7. To verify the result, in the task pane, select **Prestage Devices > Manage Device Roles**.

The **Manage Device Roles** page shows devices you can use for provisioning.

SEE ALSO

[Prestaging Devices Overview](#) | 36

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 Activate software ships with standard service definitions. First, we check the standard service definitions to determine whether one already exists that can work.

1. In the Network Activate 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.

2. In the Network Activate task pane, select **Service Design > Manage Service Definitions > Create VPLS Service Definition**.

The **General** window appears.

3. Enter a name for the service definition.

4. Click **Next**.
5. In the **Connectivity Settings** window—because we intend to select a specific VLAN for each endpoint in the service—leave the Normalized VLAN setting as the default **Normalize to VLAN none**, and then click **Next**.
6. In the **UNI Settings** window, in the **Ethernet option** field, select **dot1q**.
7. In the **Customer traffic type** field, select **Transport single VLAN**.
8. In the **VLAN ID selection** field, choose **Select manually**.
9. In the **VLAN range for manual input**, specify the range.
10. In the **Outer Tag protocol ID**, select **0x8100**
11. In the **Physical IF encapsulation** field, select **flexible-ethernet-service**.
12. In the **Logical IF encapsulation** field, select **vlan-vpls**.
13. In the **Bandwidth Settings** panel, select the **Enable rate limiting** check box.

14. In the **Default Bandwidth** field, enter **10**, for a default bandwidth of 10 Mbps.

15. To the right of the value you just entered, select the **Editable in service order** check box.

The **Default Bandwidth (Mbps)** field becomes active.

16. Select the **Enable in Service Order** check box for the Default Bandwidth (Mbps) field.

The Min Bandwidth (Kbps), Max Bandwidth (Mbps), and Increment (Kbps) fields become active.

17. In the **Bandwidth range** fields, enter **10** and **64** respectively.

18. In the **Increment** field, enter **64**.

The screenshot shows the 'UNI Settings' configuration window for a 'Create VPLS Service Definition'. The window is divided into three main sections: Traffic Treatment, Interface Settings, and MTU Settings. On the right, there is a sidebar with tabs for General, UNI Settings (selected), Connectivity, and Advanced (optional). At the bottom, there are navigation buttons: Back, Next, Finish, and Cancel.

Traffic Treatment

- Ethernet option: dot1q
- Customer traffic type: Transport single vlan
- VLAN ID selection: Select manually
- VLAN range for auto-pick: (empty)
- VLAN range for manual input: 1
- Outer Tag protocol ID: 0x8100
- Inner Tag protocol ID: Please select ...
- Editable in Service Order checkboxes are present for Outer Tag protocol ID and Inner Tag protocol ID.

Interface Settings

- Physical IF encapsulation: flexible-ethernet-services
- Logical IF encapsulation: vlan-vpls

MTU Settings

- Default MTU (Bytes): 1522
- MTU range (Bytes): 1522
- 9192
- Editable in Service Order checkbox is present.

19. 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.

20. To publish the service definition, in the **Manage Service Definitions** page, select the vpls-dot1q-sd-1 service definition, and then in the **Actions** menu, select **Publish Service Definition**.

The **Publish Service Definition** window appears.

21. 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.

SEE ALSO

[Predefined Service Definitions | 408](#)

[Creating a Multipoint-to-Multipoint VPLS Service Definition | 214](#)

[Publishing a Custom Service Definition | 308](#)

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. In the Network Activate task pane, select **Service Provisioning > Manage Customers > Create Customer**.
2. In the **Name** field, enter **Best Customer**.
3. In the **Account number** field, enter **1234**.
4. Click **Create**.

The **Manage Customers** page shows the new customer.

SEE ALSO

[Adding a New Customer | 1056](#)

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. In the Network Activate task pane, select **Service Provisioning > Manage Service Orders > Create VPLS Service Order**.
2. In the **Manage Service Definitions** page, select the service definition named **vpls-dot1q-sd-1**.
This service definition is the customized service definition you created earlier.
3. Click **Next**.
4. In the **General Settings** box of the **Enter Order** window, in the **Name** field, enter **vpls_so_1**.
5. In the **Customer** field, select the customer for which you are creating the service order..
6. In the **Endpoint Settings** box of the **Enter Order Information** window, in the **Bandwidth** field, select **25**.

The screenshot shows the 'Enter Order Information' window with the following settings:

- General Settings:**
 - Service definition: ELAN-BGP-QinQ-AllVLAN
 - Name:
 - Customer: Please select ...
 - Comments:
 - Customer traffic type: Transport all traffic
 - Signaling: BGP
- Connectivity Settings:**
 - ☒ Autopick Route Target
 - Route Target:
- End Point Settings:**
 - These settings from the selected Service Definition can be applied to all end points.
 - Bandwidth range: 10000Kbps - 100Mbps
 - Bandwidth: 10 Mbps
 - MTU (Bytes): 1522
 - Auto-pick VLAN range 1-4094 constraint: ☒ Autopick VLAN ID
 - Physical IF encapsulation: flexible-ethernet-services
 - Logical IF encapsulation: vlan-vpls
- OAM Settings:**

At the bottom, there are 'Next' and 'Cancel' buttons.

7. Clear the **Autopick VLAN ID** check box.

The **End Point Settings** box expands to include the **VLAN ID** field.

8. In the **VLAN ID** field, enter **600**.
9. Click **Next**.
10. In the **Select Endpoint PE Devices** window, select **BLR**, **SFO**, and **SJC**.
11. Click **Create**.
12. In the **Endpoint Settings** window click **Next** to accept the system-selected endpoints.

In the **Deployment Options** window, you can save the service order for later deployment, schedule the service order for later deployment, or deploy the service order now. Select **Deploy now**.
13. Click **OK** to start the deployment.
14. 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.
15. When you see in the **Job Management** window that the deployment is successful, in the Network Activate task pane, select the **Service Provisioning** workspace again.
16. In the task pane, select **Manage Services**.

The **Manage Services** page shows the new service.

SEE ALSO

[Creating a Multipoint-to-Multipoint VPLS Service Order | 660](#)

[Deploying a Service Order | 631](#)

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. In the **Manage Services** page, select the service instance you just deployed.
2. Open the **Actions** menu and select **Perform Functional Audit**.
3. In the **Schedule Functional Audit** window, you can choose to perform the audit now or schedule it for later. Select **Audit now**, and then click **OK**.
4. In the **Order Information** window, click **OK**.
5. Open the **Actions** menu and select **Perform Configuration Audit**.
6. 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**.
7. In the **Order Information** window, click **OK**.
8. To view the functional audit results,
 - In the **Manage Services** page, select the **vp1s_so_1** service instance.
 - Right-click or open the **Actions** menu to see the list of tasks available for this device, and select **View Functional Audit Results**.
 - In the **Functional Audit Results** window, select each device to view the results.
9. To view the results of the configuration audit,
 - Right-click or open the **Actions** menu to see the list of tasks available for this device, and select **View Configuration Audit 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 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

[Prestaging Devices Overview | 36](#)

[Discovering and Assigning All N-PE Devices | 68](#)

Discovering and Assigning N-PE Devices with Exceptions	71
Predefined Multipoint-to-Multipoint Ethernet Service Definitions	521
Creating a Multipoint-to-Multipoint VPLS Service Definition	214
Publishing a Custom Service Definition	308
Adding a New Customer	1056
Creating a Multipoint-to-Multipoint VPLS Service Order	660
Deploying a Service Order	631
Understanding Service Validation	875

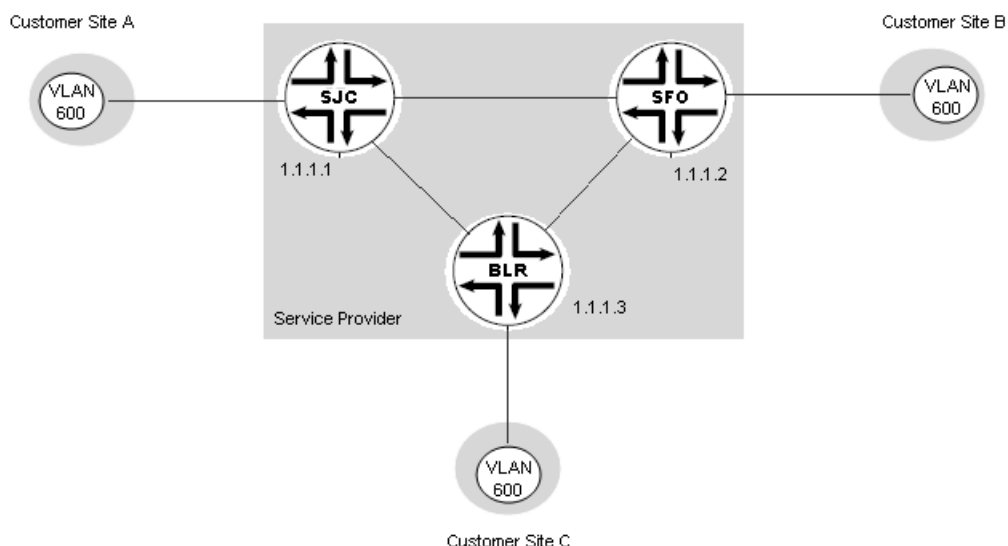
Example: Configuring and Deploying a Layer 3 VPN Full-Mesh Service

IN THIS SECTION

- Preparing Devices for Discovery | 987
- Discovering Devices | 988
- Preparing Devices for Prestaging | 989
- Discovering and Assigning N-PE Roles | 990
- Choosing or Creating a Service Definition | 991
- Creating a Customer | 993
- Creating and Deploying a Layer 3 VPN Service Order | 993
- Performing a Functional Audit and a Configuration Audit | 995

This example shows how to set up a simple full-mesh service provider VPN configuration, as shown in [Figure 30 on page 987](#).

Figure 30: Simple Layer 3 VPN Full-Mesh Service



This service provides connectivity for one VLAN, (VLAN ID = 600). Customer site A connects to the network through an N-PE device named SJC. Customer site B connects to the network through an N-PE device named SFO. Customer site C connects to the network through an N-PE device named BLR.

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:

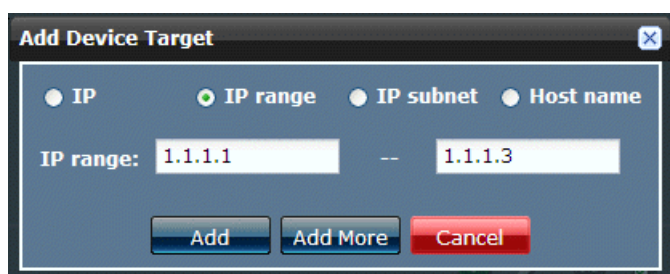
```
set system services netconf ssh
```

- 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.

1. Log in to Junos Space using your credentials.
2. In the **Network Activate** task pane, 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 Activate software for N-PE devices and UNIs.

1. In the **Network Activate** task pane, select **Prestage Devices > Manage Device Roles > Discover Roles**.

This action launches the role discovery process in which the Network Activate software examines the devices under Junos Space management looking for devices that match predefined rules that identify N-PE devices. The Role Discovery Status graph shows that, in this case, the Network Activate software has discovered three such devices.

2. In the **Assign Roles** window, switch to multiple selection mode and select both N-PE devices.
3. Open the **Actions** menu and select **Assign NPE role**.

4. In the **Assign NPE** window, click **Assign** to confirm the assignment.
5. To view the assignment status, in the **Job Management** window, click the job ID of the assignment job.
The **Job Management** page shows the progress and status of the role assignment job.
6. To verify the result, in the **Network Activate** task pane, select **Prestage Devices > Manage Device Roles**.
The **Manage Device Roles** window shows three devices that can be used for provisioning.

SEE ALSO

[Prestaging Devices Overview | 36](#)

[Discovering and Assigning All N-PE Devices | 68](#)

[Discovering and Assigning N-PE Devices with Exceptions | 71](#)

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 Activate software ships with standard service definitions. First, we check the standard service definitions to determine whether one already exists that will work.

1. In the Network Activate 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.

2. In the **Network Activate** task pane, select **Service Design > Manage Service Definitions > Create L3 VPN Service Definition**.

The **General** window appears.

3. In the name field, enter the name "l3vpn-ospf-static-full-mesh-sd" for the service definition.
4. 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.

5. Click **Next** to save the General step information.

Continue with “UNI Settings” next.

6. In the VLAN ID selection field, select **Select manually** to have the service provisioner select a VLAN ID for the service.
7. To enable the service provisioner to override this setting in a service order, select the **Editable in service order** check box.
8. 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.
9. Click **Next** to save the UNI settings.
Continue with “Connectivity” next.
10. In the **PE-Core Settings** box, select **Auto pick** to allow the Network Activate software to automatically select the route distinguisher.
11. 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.
12. Click **Finish** to save and create the Layer 3 VPN service definition.

13. 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.

14. To publish the service definition, in the **Manage Service Definitions** page, select the vpls-dot1q-sd-1 service definition, and then in the **Actions** menu, select **Publish Service Definition**.

The **Publish Service Definition** window appears.

15. 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.

SEE ALSO

[Predefined Full Mesh Layer 3 VPN Service Definitions | 571](#)

[Publishing a Custom Service Definition | 308](#)

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. In the **Network Activate** task pane, select **Service Provisioning > Manage Customers > Create Customer**.
2. In the **Name** field, enter **Best Customer**.
3. In the **Account number** field, enter **1234**.
4. Click **Create**

The **Manage Customers** window shows the new customer.

SEE ALSO

[Adding a New Customer | 1056](#)

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. In the **Network Activate** task pane, select **Service Provisioning > Manage Service Orders > Create L3 VPN Service Order**.
2. 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.
3. Click **Next**.
4. In the **General Settings** box of the **Enter Order** window, in the **Name** field, enter **l3vpn_ospf_full_mesh_so**.
5. In the **Customer** field, select **Best Customer**.
6. In the **VPN Settings** box of the **Enter Order Information** window, select the **Apply to All** check box.
7. In the **VLAN ID** field, enter "600".
8. Click **Next**.
9. In the **Select Endpoint PE Devices** window, select **BLR, SFO, and SJC**.
10. In the **Endpoint Settings** window, in the **Interface IP** field, enter an IP address/subnet for the device, for example, 10.255.245.68/28.
11. In the **Endpoint Settings** window, in the **OSPF area ID** field, enter an IP address for the OSPF area.
12. Click **Save**.
13. Repeat Step 10 through Step 12, for each endpoint device that you want to include in the service.
14. In the **Endpoint Settings** window, click **Next** to accept the system-selected endpoints.
15. Click **Create** to display the **Deployment Options** window where you can save the service order to deploy it later, schedule the deployment for a specific time, or deploy the service now. Select **Deploy now** and click **OK** to start the deployment.

16. 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.
17. When you see in the **Job Management** page that the deployment is successful, in the **Network Activate** task pane, select the **Service Provisioning > Manage Services**.
The **Manage Services** page shows the new Layer 3 VPN full mesh service.

SEE ALSO

[Creating a Full Mesh Layer 3 VPN Ethernet Service Order | 718](#)

[Deploying a Service Order | 631](#)

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. In the **Manage Services** page, select the service instance you just deployed.
2. Right-click or open the **Actions** menu and select **Perform Functional Audit**.
3. In the **Schedule Functional Audit** window, you can choose to perform the audit now or schedule it for later. Select **Audit now**, and then click **OK**.
4. In the **Order Information** window, click **OK**.
5. Right-click or open the **Actions** menu and select **Perform Configuration Audit**.
6. 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**.

7. In the **Order Information** window, click **OK**.
8. When the audit jobs have finished, success is indicated by an up arrow in the top right corner of the **Manage Services** page.

To view the functional audit results:

- a. In the **Manage Services** page, select the **l3vpn_ospf_full_mesh_so** service instance.
- b. Right-click or open the **Actions** menu and select **View Functional Audit Results**.
- c. In the **Functional Audit Results** window, select each device to view the results.

To view the results of the configuration audit:

- a. Right-click or open the **Actions** menu and select **View Configuration Audit Results**.
- b. 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 inconsistent with the Junos Space database.

Following a successful audit, the service is deployed and ready to be used.

RELATED DOCUMENTATION

[Junos Space Layer 3 Services Overview | 171](#)

[Creating a Full Mesh Layer 3 VPN Service Definition | 376](#)

[Creating a Full Mesh Layer 3 VPN Ethernet Service Order | 718](#)

Example: Creating Cross Provisioning Platform Services

IN THIS SECTION

- [Requirements | 997](#)
- [Overview | 998](#)
- [Developing Scripts | 999](#)

- [Debugging a Cross Provisioning Platform Script | 1026](#)
- [Provisioning the Services Using the Scripts | 1028](#)

The Cross Provisioning Platform (CPP) is an extension to the Network Activate application, which provides a real-time, operations support system (OSS) for creating and deploying services across multi-vendor devices. With the Cross Provisioning Platform application, you can:

- Provision services between Juniper Networks devices and Nokia devices.
- Use SOAP API to manage Nokia 5620 Service Aware Manager

The Cross Provisioning Platform application uses Network Activate as the underlying framework and adds flexibility in designing services. You can:

- Create a data model for a new service
- Create user interface to define new service
- Define business logic to deploy the new service on Juniper Networks devices and Nokia devices.

Creating services for Cross Provisioning Platform requires the coordination of tasks performed in several areas of expertise including script design, system administration, and service provisioning. When you create the Cross Provisioning Platform service definition, you can attach scripts designed for the service.

This guide describes the process you must follow to create scripts for the Cross Provisioning Platform (CPP) system and the steps required to provision the scripts.

Requirements

This example uses the following hardware and software components:

- Sencha Ext-JS 4.1.x JavaScript library for RIA (which is included in Junos Space)
- Sencha Architect
- XSLT 2.0 and XPath 2.0
- Junos Space Network Management Platform
- Junos Space Cross Provisioning Platform application

NOTE: You can acquire Sencha Architect software through <http://www.sencha.com/products/architect/>

Before you begin to develop the scripts, must be able to:

- Proficiently use JavaScript and Cascading style sheets (CSS)
- Use Sencha Ext-JS 4.1.x JavaScript library for RIA (which is included in Junos Space)
- Use Sencha Architect
- Develop scripts proficiently using XSLT 2.0 and XPath 2.0
- Develop XML scripts that can be processed correctly with the third-party SOAP API
- Develop a Junos configuration script using the Juniper XML API

Overview

To deploy services to run across both Juniper Networks platforms and the devices of third-party vendors, you must perform the following steps:

1. Create the following types of scripts

- GUI script
- Third-party (SAM)Flex scripts
- Juniper Networks Flex Scripts

NOTE: The Flex scripts are also termed as configuration scripts.

2. Provision the scripts in the Cross Provisioning Platform application.

Developing Scripts

IN THIS SECTION

- [Creating the GUI Scripts | 999](#)
- [Creating the Flex Scripts for Juniper Network | 1011](#)
- [Creating the Flex Scripts for Third-party Vendors \(SAM\) | 1016](#)

You must create the following scripts:

Creating the GUI Scripts

Step-by-Step Procedure

In the Junos Space CPP context, the GUI script generates the user interface for interacting with the Cross Provisioning Platform service. The GUI defines the parameters for which a user specifies values. The GUI can define hidden fields and values that are passed to the server. The GUI also guides a user to enter valid values for the parameters to define a service order. In addition, the GUI script can provide some client-side validation.

To develop the GUI scripts that render the CPP windows through which you can enter information to define a service, you must be able to:

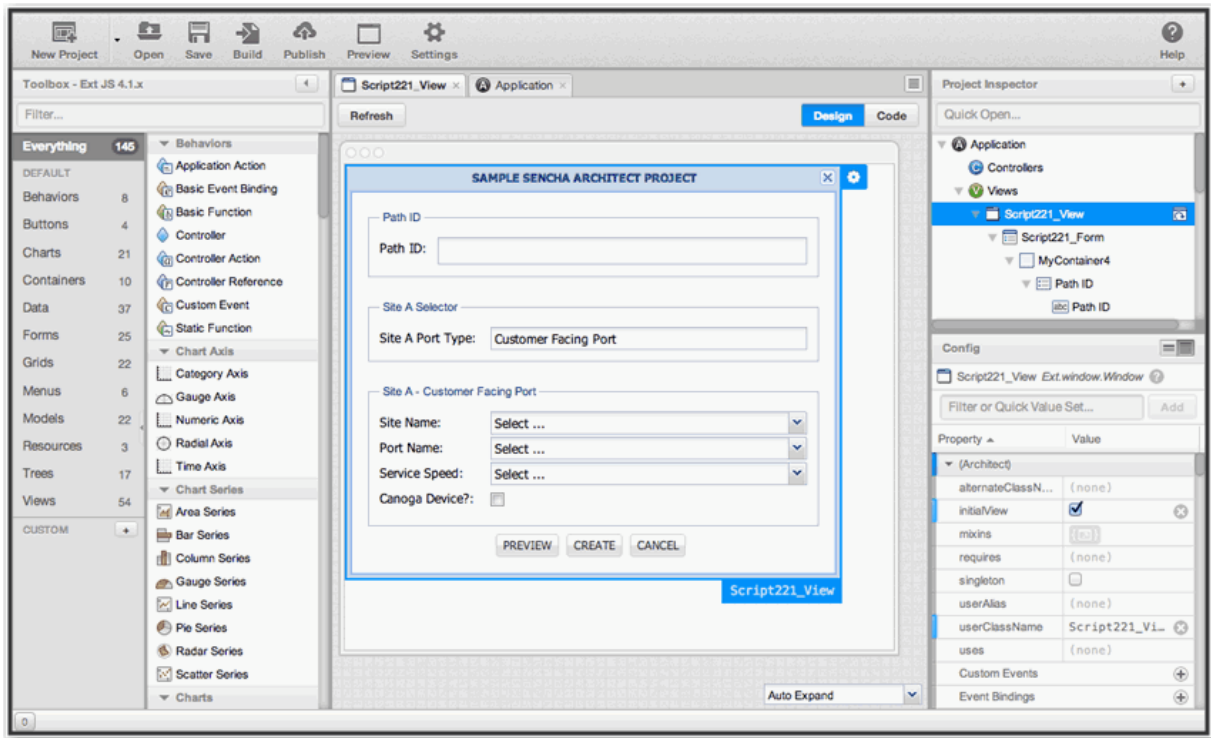
- Develop scripts proficiently using JavaScript and Cascading style sheets (CSS)
- Use Sencha Ext-JS 4.1.x JavaScript library for RIA (which is included in Junos Space)
- Use Sencha Architect

To develop the GUI Scripts:

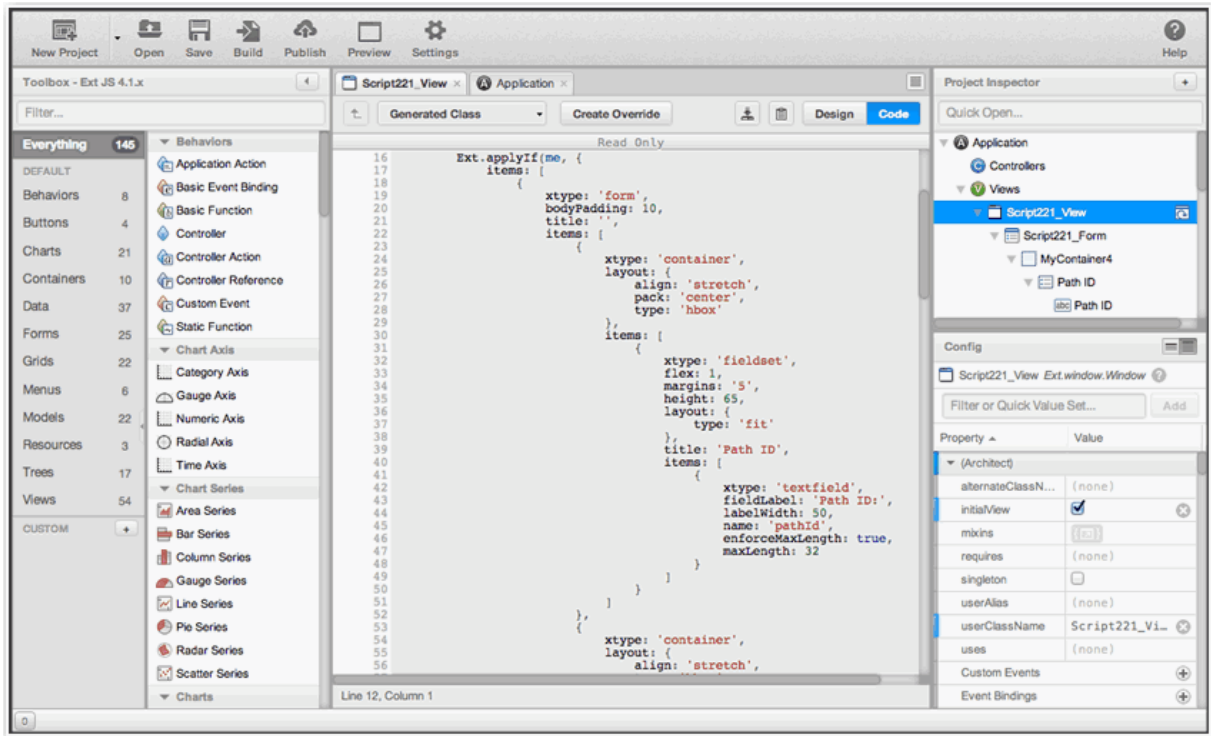
1. Use the Sencha Architect to build the GUI.

The Sencha EXT-JS library supplies a set of widgets that the script designer can use to develop the GUI forms.

The following illustration shows a typical GUI designer's view of a Sencha Architect Project page.



The following illustration shows generated code displayed within a Sencha Architect project page.



NOTE: As an alternative to using the Sencha Architect to build the GUI, you can hand-code the GUI forms. If you decide to hand-code the GUI, you can access one of the following development resources, which are available online at no cost:

- An online GUI development environment at : <https://fiddle.sencha.com/>
- An online API reference and code examples at: <http://docs.sencha.com/extjs/4.1.1/>

2. Use the CPP Script Utilities that provide hooks into a Juniper Networks platform to obtain device and interface information.

The script utilities provides helper functions which are exposed by application, intended to be used by designers who create a GUI script for CPP service provisioning

You can choose to assign a short variable to these classes prototype for making it easier to access functions.

Function	Description
getMainForm (window)	This function returns the form, from the main popup window, assuming the user layout is such that the form is inserted directly inside the window as first child.
getFormValues (window)	This function gets all the user filled input form data values within a window.

Function	Description
getFieldsByProperty (property,name)	This function gets any components inside a window dialog by any custom or predefined property. If more than one component match is found, then it returns an array of all matched components.
getFieldByName (name)	This function returns any field or component inside the form, based on its name. This returns fields from within field sets. If more than one match is found it returns the first match always. Typically field are never same, to avoid getting more than one result you should always assign unique names to fields.
getDeviceStore (data)	This function makes a connection to devices resource and get all the Junos devices and autoloads into the device store. This function pass the common data from previous screen to determine if the service definition selected has a SAM script attached. If data is not specified, then only Juniper Networks devices are returned from server by default.
getL2ExtDeviceStore ()	This function makes a connection to the devices resource and get all the Junos devices which have L2E role and autoloading into the device store.
getInterfaceStore ()	This function gets all the interfaces based on the selected devices. This is not autoloading, loads only when the device is selected. Therefore the store load must be handled in the device combo box select listener.
getL2ExtInterfaceStore ()	This function gets all the interfaces based on the selected devices which have L2E role. This is not autoloading, and loads only when the device is selected. Therefore the store load must be handled in the device combo box select listener .
setFieldValues (window,data)	This function populates the data coming from server and show it into the form.
saveForm (window,data)	This function gets the data from user dialog and send it to the back end for persistence and validation. Any server error or information is shown as popup dialog. If all validation goes well, the job link dialog is displayed for the user to either exit or go to job page for a status check.
saveBulkForm (window,data)	This function gets user data and save the form in bulk. No job dialogs are shown. You need to manually close the dialog after saving the data.
saveAndCreateMore (window,data)	This function gets the data from user dialog and send it to back end for persistence and validation. Any server error or information is shown as popup dialog and the screen is ready for another input from user.

Function	Description
saveModifyForm (window,data)	This function is called when you try to modify a service. This function receives the data from the user dialog and send it to the back end for persistence and validation. Any server error or information is shown as a popup dialog. If all validation goes well, the job link dialog is displayed for the user to either exit or go to job page for a status check.
validateVLAN (siteId,port,encap,checkbox)	The UI designer must call this event handling function, to validate the encapsulation field. This can be added as a callback for any change event (text field change or check box). The objective is to send <i>siteId</i> , <i>port</i> , <i>encap</i> to validate from the back end. The result is shown in a pop-up dialog. Pass "null" if you are not using a check box, otherwise it will be unchecked.
showInterfaceDetails (siteId,port,vendor)	Based on the site and port, this function fetches the port details and show it to user in a pop up dialog. the vendor can be either <i>Junos Space</i> or <i>Alcatel</i> .
createGroupingGridPanel (name,height,store>window)	<p>This function groups grid from the user GUI script, params :- name : grid name, height : grid height, store : grid store, window : reference of the user script main window.</p> <p>You should implement <i>addSiteHandler</i> and <i>deleteUNInterfaceHandler</i> and <i>addUNInterfaceHandler</i> in their respective script for <i>addsite</i>, <i>addport</i>, <i>deleteport</i> button actions.</p>
createStore (fields,groupField)	This function creates grouping grid store from the user GUI script, params :- fields : fields used in grid store - should be array of fields, groupField : group Name
createForm (initialConfig,items)	This function creates a field of form, from the user GUI script, params:- initialConfig - configurations like name, height, default, layout, bodyPadding, title and so on.
createDefaultServiceOrderName (field)	This function creates default service order name and set to service order name text field, params:- field :service order name textfield component return current Time with prefixed with 'SO' string.
getNodeList (deviceId,vendor,inventoryType,xpath)	<p>This function returns the inventory in Stringified JSON format. Based on device ID, vendor type, inventory Type, XPath, param deviceId - Id of the device, param vendor - Default to Juniper, param inventoryType -the inventorytype is the string value from the following DeviceInventoryXMLType enum,</p> <p>INTERFACES("interface-information"), CONFIGURATION ("configuration"), SOFTWARE_INVENTORY("software-inventory"), HARDWARE_INVENTORY ("chassis-inventory"), SYSTEM_INVENTORY ("system-information"), LICENSE_INVENTORY ("license-inventory"), DEVICE ("device"), param xpath - the xpath to apply For configuration, use Xpath starting with "/device/configuration", For hardware inventory, use Xpath starting with "/device/chassis-inventory"</p>

Function	Description
navigateTo (taskName)	This function navigates other tasks using the task name, params:- taskName :name of the task
getEndpointAdvanceSettings (String deviceId, String portName, String customerId)	This function retrieves the advanced attributes for the service endpoints.
getNetworkDetails	This function sends the SOAP message to retrieve the network device details from the Nokia SAM server based on the device IP.
getEquipmentPort	This function sends the SOAP message to retrieve the equipment port details from the Nokia SAM server based on the device IP and port name
getEquipmentPortSpeed	This function sends the SOAP message for fetching the equipment port speed details from the Nokia SAM server, based on the device IP and port name.
getEquipmentPortAttribute	This function sends the SOAP message for fetching the equipment port details from the Nokia SAM server based on the device IP and port name.
getDeviceInterfaceStatus	This function sends the SOAP message for fetching the interface status based on the specified device and port name.
getSubscriber	This function sends the SOAP message for fetching the subscriber details from the Nokia SAM server based on the customer name.
getSubscriberDetailsById	This function sends the SOAP message for fetching the subscriber details from the Nokia SAM server based on the customer ID.
getAccessEgressPolicyObject	This function sends the SOAP message for fetching the egress policy details from the Nokia SAM server based on the policy name.
getAccessIngressPolicyObject	This function sends the SOAP message for fetching the ingress policy details from the Nokia SAM server based on the policy name.
getAccessEgressFilterObject	This function sends the SOAP message for fetching the egress filter details from the Nokia SAM server based on the policy name.
getSDPBinding	This function sends the SOAP message for fetching the SDP binding details from the Nokia SAM server based on the site IP address and the MTU value.
getDeviceIP	This function finds the service IP from the PE device ID.

Function	Description
getLoopbackIP	This function finds the loopback IP of the Juniper Networks device IP, based on the device ID from the Service request.
createSDPBinding	This function sends the SOAP message for creating the SDP binding to the Nokia SAM server based on the from and to site IP address and the MTU value.
pingSAMServer	This function sends the SOAP message to ping and check the availability of the Nokia SAM server.
getL3VPNIPAddressPool	This function sends the SOAP message to check if the given IP Address is already in use.
getASNumber	This function fetches the AS number from the Nokia SAM server. The class name used is "topology.BgpAutonomousSystem". This can be used for the Route Distinguisher setting for VPRN services.
getNetworkSnmpReachability	This function queries the Nokia SAM server for the network details of the device, and finds the SNMP reachability value.
getNetworkReachability	This function queries the Nokia SAM server for the network details of the given device, and finds the network reachability value
getNetworkElementAttribute	This function queries the Nokia SAM server for the network details of the given device. The user can specify any attribute value to be fetched for the given device.
getVprnServiceIdForCustomer(This function queries the Nokia SAM server to get the VPRN ID for the specified service ID and subscriber.
getPrefixListDisplayedName	This function queries the Nokia SAM server to find the displayed name for the prefix list ID. This is used to find out if the given prefix list exists in the system.
getCommunityDisplayedName	This function queries the Nokia SAM server to find the displayed name for the community ID. This is used to find out if the given community exists in the system.
getPolicyStatementDisplayedName	This function queries the Nokia SAM server to find the displayed name for the policy statement. This is used to find out if the given policy statement exists in the system.
getVprnSiteServiceId	This function queries the Nokia SAM server to find the ID of the specified device in the specified VPRN service.

Function	Description
<code>deleteInstance</code>	This function is called through the XSLT for deleting any instance from the Nokia SAM server. Based on the ID specified, the corresponding instance is deleted from the Nokia SAM server.
<code>getForeignSVCID</code>	This function returns the service ID used by the Nokia SAM server for the specified CPP service ID.
<code>executeCliCommand(</code>	This function executes the specified CLI command directly on the device through the Nokia SAM server, and returns the response.
<code>sendScriptBasedSoapRequest</code>	This function sends any type of request to Nokia SAM server based on the input and sends the output response.
<code>getSubscriberInformation(String serviceId, String displayName, String siteId)</code>	This function sends a request to the Nokia SAM server, and retrieves the subscriber's name based on the service ID, site ID and the displayed name.
<code>getVPRNIPAddress (String serviceId, String displayName, String siteId)</code>	This function sends a request to the Nokia SAM server and retrieves the primary IPv4 address for the VPRN service, based on the service ID, site ID and the displayed name.
<code>isValidRD (String Rd)</code>	Based on the route distinguisher, this function validates the route distinguisher value from the Nokia 5620 Service Aware Manager server.
<code>isValidServiceId (String serviceId)</code>	Based on the service ID, this function validates the service ID value from the Nokia 5620 Service Aware Manager server.
<code>isValidServiceIdandRd (String serviceId, String rd)</code>	Based on the route distinguisher and service ID, this function validates the route distinguisher and service ID value from the Nokia 5620 Service Aware Manager server.
<code>isValidResource (String key, String value)</code>	Based on input parameters of the customer, this function retrieves the object's full name from the Nokia 5620 Service Aware Manager server.

The following code fragment is a sample of the importation or declaration of the CPP ScriptUtils.

```
initComponent: function() {
    var me = this;

    Ext.applyIf(me, {
        scriptUtils: ui.common.utils.ScriptUtils.prototype
    });
}
```

The following two code fragments are samples of script utility function calls:

getDeviceStore()

```
Ext.applyIf(me, {
    deviceStore : this.scriptUtils.getDeviceStore(commonData),
    items: [
        {
```

getInterfaceStore()

```
minChars: 1,
queryMode: 'local',
store: this.scriptUtils.getInterfaceStore(),
typeAhead: true,
```

3. The CPP software populates values for the attributes policy, bundleName, samScriptBundleName, and the description. The script populates values for the remaining attributes. The script designer determines values for attributes within ServiceCommonAttributes and ServiceEndpointAttributes. The attributes pedeviceId and vendorType are mandatory. All of the attributes are converted directly into XML and passed to ServiceRequest.xml.

The script designer can use the attribute *children* to nest ServiceEndpointAttributes to represent topology structure. The attribute topologyIndex is optional. The designer can use it to describe the topology structure of service endpoints.

The following parameters are the mandatory parameters that must be present in the ServiceRequest.xml:

NOTE: These parameters are case sensitive.

Parameters	Description
pedeviceId	<p>PE Device ID</p> <p>You obtain this value by fetching all the devices from the database through the <i>ScriptUtil</i> helper functions.</p>
vendorType	<p>Vendor type</p> <p>The vendor type can be <i>Juniper</i>, or <i>Alcatel</i>, or <i>SpacePlatform</i>.</p> <p>NOTE: <i>SpacePlatform</i> is used only while writing Device Order Configlet scripts, that is, Flex script with Service Type as <i>Device</i>.</p>

Parameters	Description
Interface	Interface Name You can obtain this value by fetching all the interfaces from the database through the <i>ScriptUtil</i> helper functions.
outerEncap	Outer encapsulation of the VLAN ID.
seld	Service Element ID. This value should be not set while creating a service. This value is mandatory while modifying a service. This value is populated using Modify APIs defined to retrieve all the endpoints.
recordOPType	Record operation type The record operation type can be <i>ADD</i> , or <i>MODIFY</i> , or <i>DELETE</i> . For Create Default the value is <i>ADD</i> . For Modify the value can be <i>ADD</i> , or <i>MODIFY</i> , or <i>DELETE</i> .
ServiceEndpointAttributes	The user defined attributes of the service endpoint. You can provide any valid JSON data to this attribute. This is specific to each service endpoint
ServiceCommonAttributes	The attributes that are common for all the service endpoints or services.

The following illustration displays sample code of a *ServiceRequest.xml* document. Within the sample:

- The element *ServiceEndpointAttributes* is the mandatory attribute of any individual *ServiceElement*. Note that *pedeviceId* and *vendorType* are mandatory items of a *ServiceRequest.xml* document.
- The element *ServiceCommon Attributes* is the common attribute of a service.
- Both elements, *ServiceEndpointAttributes* and *ServiceCommonAttributes*, are converted from the JSON data derived from the GUI script. *ServiceEndpointAttributes* and *ServiceCommonAttributes* are artifacts that pass information from GUI scripts to the XSLT Flex scripts.
- The CPP engine generates the other part of a *ServiceRequest.xml* file.

```

<ns2:ServiceRequest xmlns:ns2="http://provisioning.jmp.juniper.net
  <ID>3506246</ID>
  <Name>S300_MOD_1398711974687</Name>
  <TypeOfRequest>Modification</TypeOfRequest>
  <ServiceType>FLEX</ServiceType>
  <RecoveryState>Default</RecoveryState>
  <OpType>MODIFY</OpType>
  <ServiceID>3506241</ServiceID>
  <Createdby>super</Createdby>
  <CreateDate>2014-04-28T11:06:14-08:00</CreateDate>
  <LastModificationDate>2014-04-28T11:06:14-08:00</LastModificationDate>
  <State>Scheduled</State>
  <Customer/>
  <ServiceCommonAttributes>
    <e>
      <serviceOrderName>S300</serviceOrderName>
    </e>
  </ServiceCommonAttributes>
  <Policy>
    <ID>622592</ID>
    <Name>S980</Name>
  </Policy>
  <ExtRef/>
  <ServiceElementList>
    <ServiceElement>
      <deviceID>557424</deviceID>
      <deviceName>freia</deviceName>
      <vendorType>Juniper</vendorType>
      <operation>ADD</operation>
      <entityID>3506247</entityID>
      <seID>0</seID>
      <elementState>0</elementState>
      <elementRecoveryState>Default</elementRecoveryState>

```

```

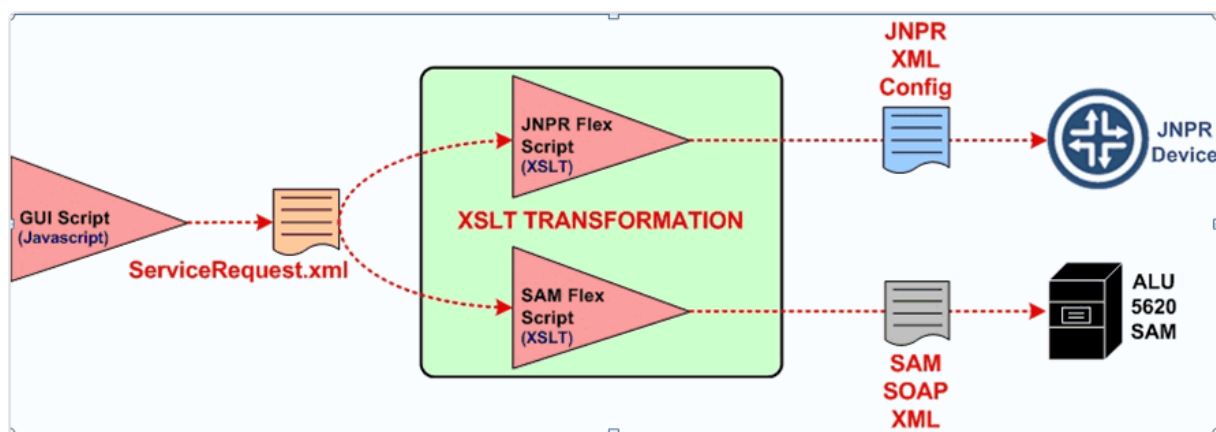
  <ServiceEndpointAttributes>
    <Interface>ge-2/0/5</Interface>
    <isActive>true</isActive>
    <isDummy>false</isDummy>
    <outerEncap>990</outerEncap>
    <pedeviceId>557424</pedeviceId>
    <recordOPType>ADD</recordOPType>
    <seId>0</seId>
    <site>freia</site>
    <vendorType>Juniper</vendorType>
  </ServiceEndpointAttributes>
</serviceElement>
<serviceElement>
  <deviceID>557075</deviceID>
  <deviceName>Penelope</deviceName>
  <vendorType>Juniper</vendorType>
  <operation>MODIFY</operation>
  <entityID>3506249</entityID>
  <seID>0</seID>

```

Every ServiceRequest must have an OpType under the ServiceRequest, which indicates the type of operation defined.

The OpType under each ServiceElement specifies whether the ServiceElement is to be added or modified when the ServiceRequest is deployed.

4. The output of GUI scripts is presented in JSON format. JSON data is rendered into an XML document known as ServiceRequest.xml. The ServiceRequest.xml document is the input to the JUNOS and SAM Flex XSLT transformations.



Designers develop Extensible Stylesheet Language Transformations (XSLT) scripts to transform one XML document into one or more other XML documents.

For Cross Provisioning Platform, an XSLT script transforms the ServiceRequest.xml document into two new XML documents:

- A SOAP XML document for the third-party (SAM) device
- A Juniper device configuration XML document

Results

When you have created GUI and configuration scripts and added them to the CPP system, you can create a service definition to which you associate specific scripts. Thereafter, you can create and deploy a service order based on a particular service definition.

While creating a service order, the **Endpoint Settings** window appears. The appearance of the **Endpoint Settings** window is based on the GUI scripts that are associated with the service definition upon which the service is based.

Creating the Flex Scripts for Juniper Network

Step-by-Step Procedure

To develop the Juniper Flex scripts that transform a service request into an XML configuration script that is sent to a Juniper device, you must be able to:

- Develop scripts proficiently using XSLT 2.0 and XPath 2.0
- Develop a Junos configuration script using the Juniper XML API

To develop the XSLT Flex script for a Juniper device:

1. The Juniper Networks XSLT Flex script derives input variables from the ServiceRequest.xml document, which is created from data a user inputs into the Junos Space CPP GUI, and generates JUNOS XML configuration that is passed to the intended Juniper Networks device.
2. An XSLT Flex script for a Juniper device has two major components:
 - Derivations Logic—In this section of code, input variables are extracted and additional parameters are derived.
 - Configuration Logic—In this section of the code, parameters derived from the derivation logic are used to construct the XML configuration that activates the service on a Juniper Networks device.

The following illustrations show the transformation from a Juniper Networks XSLT Flex script to a JUNOS XML configuration.

```
<?xml version='1.0'?>
<! -- Copyright 2009-2011 Juniper Networks, Inc. All rights reserved. -- >
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
  xmlns:ns2="http://provisioning.jmp.juniper.net/servicerequest/dto" xmlns:Map="java.util.Map"
  xmlns:java="http://xml.apache.org/xalan/java" exclude-result-prefixes="java.Map">
  <xsl:output method="xml" indent="yes" encoding="UTF-8"/>
  <xsl:template match="/">
    <serviceRequestConfig>
      <xsl:apply-templates/>
    </serviceRequestConfig>
  </xsl:template>
  <xsl:template match="ns2:ServiceRequest[OpType='ADD']">
    ...
    <xsl:for-each select="serviceElementList/serviceElement/ServiceEndpointAttributes[topologyIndex = 1 or topologyIndex = 2]">
      <deviceConfiguration>
        <entityID>
          <xsl:value-of select="../entityID"/>
        </entityID>
        ...
        <xsl:variable name="port">
          <xsl:value-of select="Interface"/>
        </xsl:variable>
        <xsl:variable name="filterName">
          <xsl:value-of select="concat($port, 'CVLAN', outerEncap)"/>
        </xsl:variable>
```



```

<configuration>
  <interfaces>
    <interface>
      <name>
        <xsl:value-of select="$port"/>
      </name>
      <flexible-vlan-tagging/>
      <encapsulation>flexible-ethernet-services</encapsulation>
      <unit>
        <name>
          <xsl:value-of select="outerEncap"/>
        </name>
        <encapsulation>vlan-ccc</encapsulation>
        <vlan-tags>
          <outer>
            <xsl:value-of select="outerEncap"/>
          </outer>
          <xsl:if test="canogaDevice = 'true' and untaggedDotq1 = 'false'">
            <inner>
              <xsl:value-of select="innerEncap"/>
            </inner>
          </xsl:if>
        </vlan-tags>
        ...
      </unit>
    </interface>
    ...
  </interfaces>
  ...
  <family>
    <ccc>
      <filter>
        <input>
          <xsl:value-of select="$filterName"/>
        </input>
      </filter>
    </ccc>
  </family>
  ...
</configuration>

```

JUNOS XML Configuration

```

<serviceRequestConfig>
  <deviceConfiguration>
    <entityID>123456</entityID>
    <configuration>
      <interfaces>
        <interface>
          <name>ge-1/0/7</name>
          <flexible-vlan-tagging/>
          <encapsulation>flexible-ethernet-services</encapsulation>
          <unit>
            <name>101</name>
            <encapsulation>vlan-ccc</encapsulation>
            <vlan-tags>
              <outer>101</outer>
              <inner>4000</inner>
            </vlan-tags>
            <input-vlan-map>
              <pop/>
            </input-vlan-map>
            <output-vlan-map>
              <push/>
            </output-vlan-map>
            <family>
              <ccc>
                <filter>
                  <input>ge-1/0/7CVLAN101</input>
                </filter>
              </ccc>
            </family>
          </unit>
        </interface>
      </interfaces>
      ...
    </configuration>
  </deviceConfiguration>
</serviceRequestConfig>
...

```

An XSLT Flex script for a Juniper Networks device includes an OpType to specify when the script is used:

- Creation—Used to create a new service and to decommission a previous service
- Modification—Used to modify an existing service

The following illustration shows the presence of OpTypes in a ServiceRequest.

```

<ns2:ServiceRequest xmlns:ns2+"http://provisioning.jmp.juniper.net
  <ID>3506246</ID>
  <Name>S300_MOD_1398711974687</Name>
  <TypeOfRequest>Modification</TypeOfRequest>
  <ServiceType>FLEX</ServiceType>
  <RecoveryState>Default</RecoveryState>
  <OpType>MODIFY</OpType>
  <ServiceID>3506241</ServiceID>
  <Createdby>super</Createdby>
  <CreatedDate>2014-04-28T11:06:14-08:00</CreatedDate>
  <LastModificationDate>2014-04-28T11:06:14-08:00</LastModificationDate>
  <State>Scheduled</State>
  <Customer/>
  <ServiceCommonAttributes>
    <e>
      <serviceOrderName>S300</serviceOrderName>
    </e>
  </ServiceCommonAttributes>
  <Policy>
    <ID>622592</ID>
    <Name>S980</Name>
  </Policy>
  <ExtRef/>
  <ServiceElementList>
    <ServiceElement>
      <deviceID>557424</deviceID>
      <deviceName>freia</deviceName>
      <vendorType>Juniper</vendorType>
      <operation>ADD</operation>
      <entityID>3506247</entityID>
      <seID>0</seID>
      <elementState>0</elementState>
      <elementRecoveryState>Default</elementRecoveryState>
      <ServiceEndpointAttributes>
        <Interface>ge-2/0/5</Interface>
        <isActive>true</isActive>
        <isDummy>false</isDummy>
        <outerEncap>990</outerEncap>
        <pedeviceId>557424</pedeviceId>

```

```

      <recordOpType>ADD</recordOpType>
      <seId>0</seId>
      <site>freia</site>
      <vendorType>Juniper</vendorType>
    </ServiceEndpointAttributes>
  </serviceElement>
  <serviceElement>
    <deviceID>557075</deviceID>
    <deviceName>Penelope</deviceName>
    <vendorType>Juniper</vendorType>
    <operation>MODIFY</operation>
    <entityID>3506249</entityID>
    <seID>0</seID>

```

Results

When you have created GUI and configuration scripts and added them to the CPP system, you can create a service definition to which you associate specific scripts. Thereafter, you can create and deploy a service order based on a particular service definition.

Creating the Flex Scripts for Third-party Vendors (SAM)

Step-by-Step Procedure

To develop third-party(SAM) Flex scripts that transform a service request into a Simple Object Access Protocol (SOAP) script that is sent to the Nokia device, you must be able to:

- Develop scripts proficiently using XSLT 2.0 and XPath 2.0
- Develop XML scripts that can be processed correctly with the third-party SOAP API

To develop the XSLT Flex script for SAM:

1. The third-party (SAM) XSLT Flex script derives input variables from the ServiceRequest.xml document, which is created from data a user inputs into the Junos Space CPP GUI, and generates a SOAP message that is passed to the intended third-party vendor's device.
2. The third-party XSLT Flex script includes two major components:
 - Derivations Logic—In this section of code, input variables are extracted and additional parameters are derived.
 - Configuration Logic—In this section of the code, parameters derived from the derivation logic are used to construct the third-party(SAM) SOAP call that activates the service on a third-party vendor's (SAM) device.

The following illustration includes sample code fragments that present the derivations logic and configuration logic sections of a XSLT Flex script for a third-party (SAM) device.

```

<?xml version="1.0"?>
<xsl:stylesheet version="2.0" xmlns:xsl=http://www.w3.org/1999/XSL/Transform
xmlns:xs=http://www.w3.org/2001/XMLSchema xmlns:xalan=http://xml.apache.org/xalan/java
xmlns:OSSClient="net.juniper.jmp.external.oss.sam.inventory.SAMOSSMediation" exclude-result-
prefixes="java OSSClient">
  <xsl:template match="/">
    <!--VALIDATIONS & DERIVATIONS -->
    <xsl:variable name="mtu" select="1596"/>
    <xsl:variable name="ingressFilterName" select="MAC Filter:20"/>
    <xsl:variable name="sapSeries">9</xsl:variable>
    <xsl:variable name="isJumbo"
select="ServiceRequest/ServiceCommonAttributes/e/jumboFrame3900"/>
    <xsl:variable name="jumbo">
      <xsl:if test="$isJumbo = true">
        <xsl:value-of select="3900"/>
      </xsl:if>
    </xsl:variable>
    ...
    <!-- Encap Details -->
    <xsl:variable name="innerEncapA"
select="ServiceRequest/serviceElementList/serviceElement/ServiceEndpoint
Attributes[seId='0']/innerEncap"/>
    <xsl:variable name="outerEncapA"
select="ServiceRequest/serviceElementList/serviceElement/ServiceEndpoint
Attributes[seId='0']/outerEncap"/>
    <xsl:variable name="canogaDevice"
select="ServiceRequest/serviceElementList/serviceElement/ServiceEndpoint
Attributes[seId='0']/canogaDevice"/>
    <xsl:variable name="speed"
select="ServiceRequest/serviceElementList/serviceElement/ServiceEndpoint
Attributes[seId='1']/speed"/>
    ...

```

```

<!--SOAP MESSAGE CONVERSION -->
  <xsl:choose>
    <xsl:element name="xmlApiRequest">
      <xsl:element name="deployer">immediate</xsl:element>
      <xsl:element name="synchronousDeploy">true</xsl:element>
      <xsl:element name="distinguishedName">svc</xsl:element>
      <xsl:element name="childConfigInfo">
        <xsl:element name="epipe.Epipe">
          <xsl:element
            name="actionMask">
              <xsl:element
                name="bit">create</xsl:element>
              </xsl:element>
            </xsl:element>
          </xsl:element>
          <xsl:element
            name=:serviced">
              <xsl:attribute name="rangePolicy">auto</xsl:attribute>
              <xsl:value-of
                select="0"/>
            </xsl:element>
          <xsl:element name="subscriberPointer">
            <xsl:value-of
              select="$subscriberPointer"/>
            </xsl:element>
          <xsl:element name="defaultVcid">0</xsl:element>
          <xsl:element name="displayName">
            <xsl:value-of select="ServiceRequest/Name"/>
          </xsl:element>
          <xsl:element name="description">
            <xsl:value-of select="ServiceRequest/Name"/>
          </xsl:element>
          <xsl:element
            name="administrativeState">up</xsl:element>
          <xsl:element
            name="topologyAutoCompletion">true</xsl:element>
          <xsl:element
            name="transportPreference">Idp</xsl:element>
          <xsl:variable name="siteNum" select="position()"/>
          <xsl:element name="children-Set">

```

The configuration logic in the third-party XSLT script converts to XSLT format the SOAP message generated by the third-party(SAM) service script. The following pseudo code sample demonstrates the logic to accomplish the conversion.

Pseudo Code Logic:

```

<!-- SOAP Message Conversion -->
When (Sitecheck='1') {
  Send single Ended Epipe SOAP Message
}

Otherwise {
  Send Double Ended Epipe SOAP Message
}

```

To work with the third-party (SAM) XSLT script, login to the third-party (SAM) server. The following illustration presents a third-party(SAM) GUI window that enables entering data for third-party (SAM) XSLT Flex script.

The screenshot shows a GUI window titled "Create VLL Epipe Service From Template: 'NGCE VPN'". The window is divided into two main sections:

- Customer Facing Port or PP8600 Gateway:**
 - Path ID:** A text field containing "94750948509".
 - Canoga Device?:** A checkbox that is checked.
 - Site:** A text field containing "COTKPG03R07", with "Select...", "Properties", and "Clear" buttons to its right.
 - Outer Encapsulation Value:** A spinner box set to "412".
 - Inner Encapsulation Value:** A spinner box set to "565", with an "UnTagged Port?" checkbox to its right.
 - Port:** A text field containing "Port 1/2/2", with "Select...", "Properties", and "Clear" buttons to its right.
- Network Facing Port (Ex. DR/PE):**
 - Site:** A text field containing "COTKPG01R12", with "Select...", "Properties", and "Clear" buttons to its right.
 - Outer Encapsulation Value:** A spinner box set to "420".
 - Port:** A text field containing "Port 1/2/3", with "Select...", "Properties", and "Clear" buttons to its right.

The following illustration shows a sample of the corresponding code that is generated when a user requests to preview the SOAP code from the GUI window.

```

Kepipe.Epipe>
  <actionMask>
    <bit>create</bit>
  </actionMask>
  <serviceId rangePolicy="auto">0</serviceId>
  <subscriberPointer>subscriber:3000</subscriberPointer>
  <defaultVcId>0</defaultVcId>
  <displayedName>94750948509</displayName>
  <description>94750948509</description>
  <administrativeState>up</administrativeState>
  <topologyAutoCompletion>true</topologyAutoCompletion>
  <transportPreference>ldp</transportPreference>
  <children-Set>
    <epipe.Site>
      <actionMask>
        <bit>create</bit>
      </actionMask>
      <mtu>1596</mtu>
      <description/>
      <siteId>10.11.77.103</siteId>
      <administrativeState>serviceUp</administrativeState>
      <children-Set>
        <v11.L2AccessInterface>
          <actionMask>
            <bit>create</bit>
          </actionMask>
          <description>94750948509</description>
          <administrativeState>serviceUp</administrativeState>
          <portPointer>network:10.11.17.103:shelf-1:cardslot-1:card:daughterCardSlot-
2:daughterCard:port-2</portPointer>
          <innerEncapValue>565</innerEncapValue>
          <outerEncapValue>412</outerEncapValue>
          <ingressPolicyObjectPointer>Access Ingress:25</ingressPolicyObjectPointer>
          <egressPolicyObjectPointer>Access Egress:25</egressPolicyObjectPointer>
          <egressFilterPointer />
          <ingressFilterPointer />
        </v11.L2AccessInterface>
      </children-Set>
    </epipe.Site>
  </children-Set>
</epipe.Epipe>

```

The following illustration shows a sample of the code that results when the script designer substitutes variables included in the SOAP code with variable names obtained from the XSLT Flex script derivation logic.


```

<epipe.Epipe>
  <actionMask>
    <bit>create</bit>
  </actionMask>
  <serviceId rangePolicy="auto">0</serviceId>
  <subscriberPointer>$customer</subscriberPointer>
  <defaultVcId>0</defaultVcId>
  <displayedName>$Description</displayedName>
  <description>$Description</description>
  <administrativeState>up</administrativeState>
  <topologyAutoCompletion>true</topologyAutoCompletion>
  <transportPreference>ldp</transportPreference>
  <children-Set>
    <epipe.Site>
      <actionMask>
        <bit>create</bit>
      </actionMask>
      <mtu>$serviceMTU</mtu>
      <description/>
      <siteId>$NodeA</siteId>
      <administrativeState>serviceUp</administrativeState>
      <children-Set>
        <v11.L2AccessInterface>
          <actionMask>
            <bit>create</bit>
          </actionMask>
          <description>$Description</description>
          <administrativeState>serviceUp</administrativeState>
          <portPointer>$port</portPointer>
          <innerEncapValue>$innerEncap</innerEncapValue>
          <outerEncapValue>$outerEncap</outerEncapValue>
          <ingressPolicyObjectPointer>$AccessIngress </ingressPolicyObjectPointer>
          <egressPolicyObjectPointer>$AccessIngress </egressPolicyObjectPointer>
          <egressFilterPointer />
          <ingressFilterPointer />
        </v11.L2AccessInterface>
      </children-Set>
    </epipe.Site>
  </children-Set>
</epipe.Epipe>


```

The following illustration demonstrates the process of converting SOAP code variables in the third-party (SAM) XSLT Flex script code. The script designer adds logic to define the variables Default MTU and Jumbo MTU. The code also indicates how Canoga or L2E is selected.

```

<children-Set>
  <epipe.Site>
    <actionMask>
      <bit>create</bit>
    </actionMask>
    <mtu>$serviceMTU</mtu>
    <description/>
    <siteId>$NodeA</siteId>
    <administrativeState>serviceUp</administrativeState>
  </epipe.Site>
</children-Set>

```



```

<xsl:element name="<children-Set">
  <xsl:element name="epipe.Site">
    <xsl:element name="actionmask">
      <xsl:element name="bit">create</xsl:element>
    </xsl:element>
    <xsl:element name="mtu">
      <xsl:choose>
        <xsl:when test="$jumbo2 = '9000'">
          <xsl:value-of select="$jumbo2"/>
        </xsl:when>
        <xsl:otherwise>
          <xsl:value-of select="$jumbo"/>
        </xsl:otherwise>
      </xsl:choose>
    </xsl:element>
    <xsl:element name="description">description</xsl:element>
    <xsl:element name="siteId">
      <xsl:value-of select="OSSClient:getDeviceIP($client, string($siteAid))"/>
    </xsl:element>
    <xsl:element name="administrativeState">
      <xsl:value-of select="administrativeState"/>
    </xsl:element>
  </xsl:element>
</xsl:element>

```

NOTE: Most of the logic that the designer adds is reused for all scripts.

The following illustrations show the transformation from a third-party XSLT Flex script to a SOAP Message.

```

<?xml version="1.0"?>
<xsl:stylesheet version="2.0" xmlns:xsl=http://www.w3.org/1999/XSL/Transform xmlns:xs=http://www.w3.org/2001/XMLSchema
xmlns:xalan="http://xml.apache.org/xalan"
xmlns:java="http://xml.apache.org/xalan/java" xmlns:OSSClient="net.juniper.jmp.external.oss.sam.inventory.SAMOSSMediator"
exclude-result-prefixes="java OSSClient">
  <xsl:template match="/">
    <!-- VALIDATIONS & DERIVATIONS -->
    <xsl:variable name="mtu" select="1596"/>
    <xsl:variable name="ingressFilterName" select="MAC Filter:20"/>
    <xsl:variable name="sapSeries">9</xsl:variable>
    <xsl:variable name="is.Jumbo" select="ServiceRequest/ServiceCommonAttributes//e/jumboFrame/3900"/>
    <xsl:variable name="jumbo">
      <xsl:if test="$is.Jumbo = 'true'">
        <xsl:value-of select="3900"/>
      <xsl:if>
    <xsl:variable>
    ...
    <!-- Encap Details -->
    <xsl:variable name="innerEncapA"
select="ServiceRequest/serviceElementList/serviceElement/ServiceEndpointAttributes[seld='0']/innerEncap"/>
    <xsl:variable name="outerEncapA"
select="ServiceRequest/serviceElementList/serviceElement/ServiceEndpointAttributes[seld='0']/outerEncap"/>
    <xsl:variable name="canogaDevice"
select="ServiceRequest/serviceElementList/serviceElement/ServiceEndpointAttributes[seld='0']/canogaDevice"/>
    <xsl:variable name="speed"
select="ServiceRequest/serviceElementList/serviceElement/ServiceEndpointAttributes[seld='0']/speed"/>
    ...

```

```

<!-- SOAP MESSAGE CONVERSION -->
<xsl:element name="xmlApiRequest">
    <xsl:element name="generic.GenericObject.configureChildInstance">
        <xsl:element name="deployer">immediate</xsl:element>
        <xsl:element name="synchronousDeploy">true</xsl:element>
        <xsl:element name="distinguishedName">svc-mgr</xsl:element>
        <xsl:element name="childConfigInfo">
            <xsl:element name="epipe.Epipe">
                <xsl:element name="actionMask">
                    <xsl:element name="bit">create</xsl:element>
                </xsl:element>
                <xsl:element name="serviced">
                    <xsl:attribute name="rangePolicy">auto</xsl:attribute>
                    <xsl:value-of select="0"/>
                </xsl:element>
                <xsl:element name="subscriberPointer">
                    <xsl:value-of select="$subscriberPointer">
                </xsl:element>
                <xsl:element name="defaultVcid">0</xsl:element>
                <xsl:element name="displayName">
                    <xsl:value-of select="ServiceRequestName"/>
                </xsl:element>
                <xsl:element name="description">
                    <xsl:value-of select="ServiceRequestName"/>
                </xsl:element>
                <xsl:element name="administrativeState">up</xsl:element>
                <xsl:element name="topologyAutoCompletion">true</xsl:element>
                <xsl:element name="transportPreference">ldp</xsl:element>
                <xsl:variable name="siteNum" select="position()"/>
                <xsl:element name="children-Set">
                    <xsl:element name="epipe.Site">
                        <xsl:element name="actionMask">
                            <xsl:element name="bit">create</xsl:element>
                        </xsl:element>
                    ...

```

SOAP message

```

<xmlapiRequest xmlns="xmlapi_1.0">
  <generic.GenericObject.configureChildInstance xmlns="xmlapi_1.0"
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance>
    <deployer>immediate</deployer>
    <synchronousDeploy>true</synchronousDeploy>
    <distinguishedName>svc-mgr</distinguishedName>
    <childConfigInfo>
      <epipe.Epipe>
        <actionMask>
          <bit>create</bit>
        </actionMask>
        <serviced rangePolicy="auto">0</serviced>
        <subscriberPointer>subscriber:1234</subscriberPointer>
        <defaultVcid>0</defaultVcid>
        <displayName>SamplePathID</displayName>
        <description>SamplePathID</description>
        <administrativeState>up</administrativeState>
        <topologyAutoCompletion>true</topologyAutoCompletion>
        <transportPreference>ldp</transportPreference>
        <children-Set>
          <epipe.Site>
            <actionMask><bit>create</bit></actionMask>

```

The SOAP script communicates directly with the third-party vendor's Service Aware Manager(SAM) module by way of a SAM adaptor plugin. The third-party vendor forwards the configuration to a device using its chosen communication protocol.

Debugging a Cross Provisioning Platform Script

IN THIS SECTION

- [Modifying a Cross Provisioning Platform Script | 1026](#)
- [Previewing a Cross Provisioning Platform Script | 1027](#)
- [Verifying a Cross Provisioning Platform Script | 1027](#)
- [\[xref target has no title\]](#)

In releases prior to Cross Provisioning Platform Release 14.3R1, you can identify script-related issues only after you create a service. You cannot preview the XML configuration that is being pushed to the device.

With Cross Provisioning Platform Release 14.3R1, you can debug both the configuration script and the GUI script while you are still creating a service. This enables you to identify and rectify all script-related issues before you create a service. You can debug both Juniper Networks and Nokia scripts.

You can debug a Cross Provisioning Platform script by performing the following tasks:

Modifying a Cross Provisioning Platform Script

Step-by-Step Procedure

In releases prior to Cross Provisioning Platform Release 14.3R1, you need to upload the modified script from your local file system. In Cross Provisioning Platform Release 14.3R1, you can modify the script directly in the text area included in the Modify Script window. By default, the latest version of the script is populated in the text area.

To modify a Cross Provisioning Platform script, perform one of the following tasks:

- Browse the local file system to upload the script that you have modified in your local file system.
The uploaded script is displayed in the text area, included in the Modify Script window.
- Modify the script directly in the text area.

NOTE: In the text area in the Modify Script window, you can also modify the script that you have uploaded from your local file system. For more information about modifying an existing script, see [“Modifying Scripts Created for Cross Provisioning Platform” on page 779](#).

Use the **Preview** option in the Modify Script window to preview the script output. In the script output, use the **Verify** option to verify the script output.

Previewing a Cross Provisioning Platform Script

Step-by-Step Procedure

With Cross Provisioning Platform Release 14.3R1, you can preview the script output before you create a service.

To preview the output of a GUI script, perform one of the following tasks:

- On the **Scripts** inventory page, right-click a script and select **Preview**.
- In the Modify Script window, click the **Preview** option.

Verifying a Cross Provisioning Platform Script

Step-by-Step Procedure

Verify the script output to identify and troubleshoot issues, if any. The Cross Provisioning Platform application provides you with the option to specify real-time data while you preview the script output.

1. In the Modify Script window, click the **Preview** option.

You can preview the script output.

2. In the script output window, specify real-time data.

3. Click **Verify**.

NOTE: For the **Verify** option to appear in the script output window and to generate the required XML output, you must append the GUI script with the newly created script utility function, `scriptUtils.verifyForm(this,data)`.

Following is the code snippet to add the **Verify** option:

```
{
  xtype: 'button',
  handler: function(button, event) {
    var data = this.getDataJSON();
    this.scriptUtils.verifyForm(this,data)
  },
  scope: this,
  text: 'Verify'
}
```

All necessary information required for debugging the Cross Provisioning Platform script is displayed in a new window.

Provisioning the Services Using the Scripts

IN THIS SECTION

- [Configuring Nokia Devices | 1029](#)
- [Adding a Third-Party Device to the Cross Provisioning Platform System | 1031](#)
- [Adding Scripts Created for Cross Provisioning Platform | 1032](#)
- [Creating a Cross Provisioning Platform Service Definition | 1035](#)
- [Creating a Cross Provisioning Platform Service Order | 1038](#)
- [Deploying Services | 1043](#)

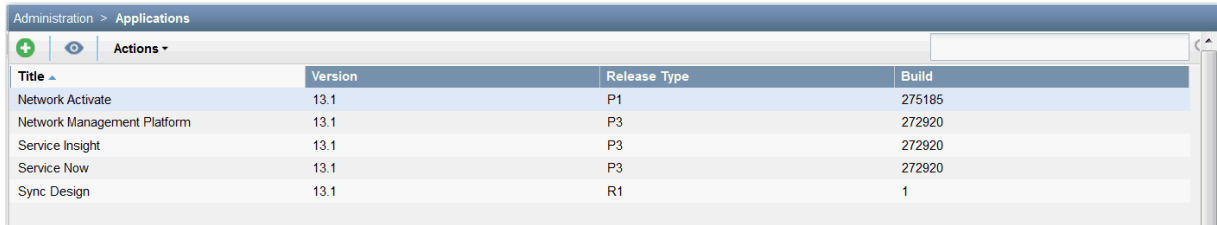
The following steps are involved in provisioning the services:

Configuring Nokia Devices

Step-by-Step Procedure

To preconfigure the third-party OSS device:

1. In the Network Management Platform, select **Administration > Applications**.



The screenshot shows the 'Administration > Applications' window. It features a table with the following data:

Title	Version	Release Type	Build
Network Activate	13.1	P1	275185
Network Management Platform	13.1	P3	272920
Service Insight	13.1	P3	272920
Service Now	13.1	P3	272920
Sync Design	13.1	R1	1

2. In the **Applications** window, select **Network Activate**.

3. From the **Actions** menu, select **Modify Application Settings**.



The screenshot shows the 'Modify Application Settings' window for 'Network Activate'. The left sidebar contains a list of settings categories: Deployment, Audit, UI, Monitoring, Logging, RouteTarget, VirtualCircuitID, PerformanceMonitoring, OSSConfigParameters, and ServiceDecommission. The main panel is titled 'Deployment' and contains the following settings:

- ☒ Deploy configuration to the device
- ☒ Enable service alarms
- ☒ Save configuration in XML format
- ☒ Show configuration in set format
- ☒ Use two phase commit for service provisioning
- ☐ Use vlanmaps for flexible tagged services

Buttons for 'Save' and 'Undo' are located in the top right corner of the main panel.

4. In the **Modify Application Settings** window, select **OSSConfigParameters**.

OSSConfigParameters		
OSSConfigParameters		
Alcatel Primary Server IP:	<input type="text" value="10.216.114.28"/>	
Alcatel Primary Server Port:	<input type="text" value="28443"/>	
Backup Server IP:	<input type="text"/>	
Backup Server Port:	<input type="text"/>	
HTTP Connection TimeOut (MilliSeconds):	<input type="text" value="25000"/>	[default]
Maximum API Requests:	<input type="text" value="5"/>	[default]
Number of devices for port sync request:	<input type="text" value="10"/>	[default]
OSS User Name:	<input type="text" value="SAM-CPP"/>	
OSS User Password:	<input type="password"/>	
Synchronize OSS Inventory daily at given time:	<input type="text" value="05:00 AM"/>	[default]
<input checked="" type="checkbox"/> Use HTTP protocol <input checked="" type="checkbox"/> Use primary server		
<div> <div>Modify</div> <div>Cancel</div> </div>		

5. Fill in the fields in the **OSSConfigParameters** panel as described in the following table.

OSS Parameter	Description
Primary Server IP	IP address of the primary server.
Primary Server Port	Port number of the primary server.
Backup Server IP	IP address of the backup server.
Backup Server Port:	Port number of the backup server.
HTTP Connection Timeout (milliseconds)	Duration of HTTP connection (in milliseconds) before the timeout elapses.
Maximum API Requests	Maximum number of simultaneous API requests permitted.
OSS Log Directory	Directory path of the OSS log directory.
OSS Log Filename	Filename of the OSS log.
OSS User Name	User name for accessing the OSS server.
OSS User Password	Hashed password for accessing the OSS server.

OSS Parameter	Description
Synchronize OSS Inventory daily at given time	<p>Sets the daily time at which the CPP system synchronizes third-party devices, added or deleted from the CPP system, with the OSS server.</p> <p>NOTE: The time at which the synchronization job runs is associated with the location of the browser in which you are using the Junos Space software. That is, the synchronization job runs according to the browser time where the job is scheduled, not according to the time where the Junos Space server is located.</p>
Use primary server	<p>If this check box is selected, the CPP system communicates with the primary OSS server. If the check box is not selected, the system interacts with the backup server.</p>

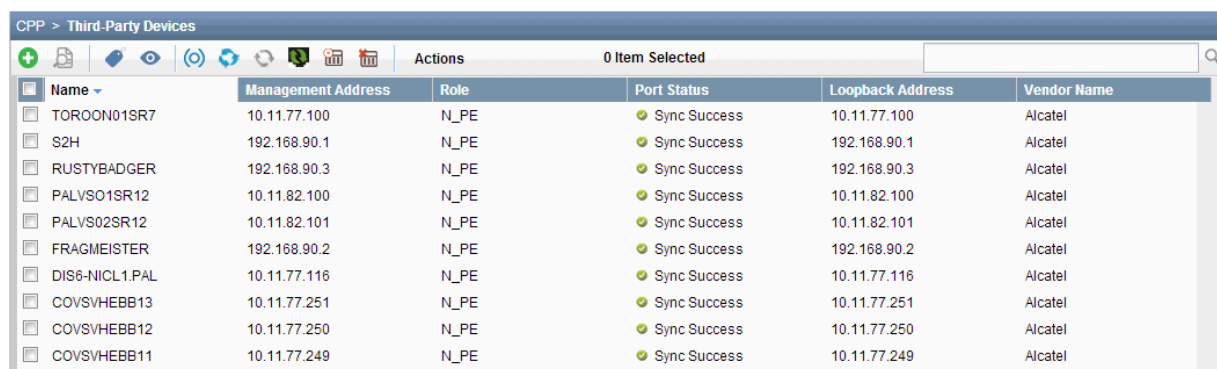
- When you are done entering information in the **OSSConfigParameters** fields, click **Modify**.

Adding a Third-Party Device to the Cross Provisioning Platform System

Step-by-Step Procedure

To add a third-party device to the Cross Provisioning Platform system:

- In the Network Activate task pane, select **CPP > Third-Party Devices**.



CPP > Third-Party Devices					
Actions 0 Item Selected					
Name	Management Address	Role	Port Status	Loopback Address	Vendor Name
TOROON01SR7	10.11.77.100	N_PE	Sync Success	10.11.77.100	Alcatel
S2H	192.168.90.1	N_PE	Sync Success	192.168.90.1	Alcatel
RUSTYBADGER	192.168.90.3	N_PE	Sync Success	192.168.90.3	Alcatel
PALVSO1SR12	10.11.82.100	N_PE	Sync Success	10.11.82.100	Alcatel
PALVSO2SR12	10.11.82.101	N_PE	Sync Success	10.11.82.101	Alcatel
FRAGMEISTER	192.168.90.2	N_PE	Sync Success	192.168.90.2	Alcatel
DIS6-NICL1.PAL	10.11.77.116	N_PE	Sync Success	10.11.77.116	Alcatel
COVSVHEBB13	10.11.77.251	N_PE	Sync Success	10.11.77.251	Alcatel
COVSVHEBB12	10.11.77.250	N_PE	Sync Success	10.11.77.250	Alcatel
COVSVHEBB11	10.11.77.249	N_PE	Sync Success	10.11.77.249	Alcatel

- In the **Third-Party Devices** window, click the **Add Third-Party Device** icon (+).



The image shows a dialog box titled "Add Third-Party Device". It contains two radio buttons: "Host Name" (selected) and "IP Address". Below the radio buttons, there are two input fields. The first is labeled "Host Name:" and contains the text "test". The second is labeled "Vendor:" and contains a dropdown menu with "Alcatel" selected. At the bottom of the dialog box, there are two buttons: "Add" and "Cancel".

3. In the **Add OSS Device** window, click the **Host Name** or **IP Address** button and then enter the hostname or IP address of the device.

4. Click **Add**.

The device is displayed in the **Third-Party Devices** window.

Adding Scripts Created for Cross Provisioning Platform

Step-by-Step Procedure

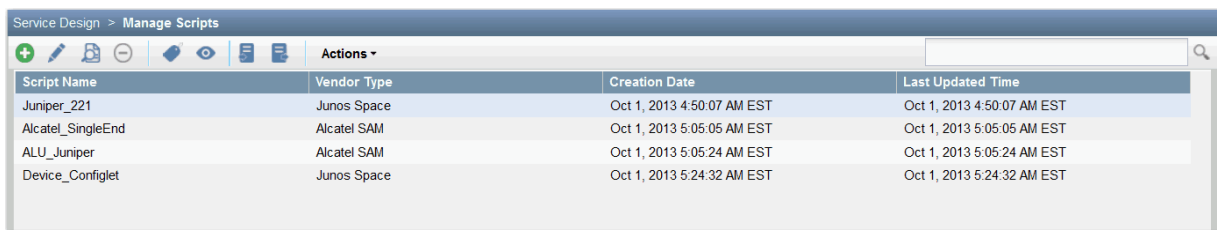
Before you can create a Cross Provisioning Platform service definition, you must add scripts to the system that enable management of the Juniper Networks devices and the devices of another vendor.

To enable Cross Provisioning Platform, you add three types of scripts:

- Junos XSLT—Provides the code that enables provisioning a particular Juniper Networks device.
- SAM XSLT—Provides the code that enables provisioning the device of another vendor.
- GUI JavaScript—Provides the code that renders the Network Activate GUI window required for provisioning a Juniper Networks device.

To view the scripts that have been loaded into the system:

1. In the Network Activate task pane, select **Service Design > Manage Scripts**.



The screenshot shows a web application window titled 'Service Design > Manage Scripts'. It features a command bar with various icons and an 'Actions' dropdown. Below the command bar is a table with four columns: 'Script Name', 'Vendor Type', 'Creation Date', and 'Last Updated Time'. The table contains five rows of data.

Script Name	Vendor Type	Creation Date	Last Updated Time
Juniper_221	Junos Space	Oct 1, 2013 4:50:07 AM EST	Oct 1, 2013 4:50:07 AM EST
Alcatel_SingleEnd	Alcatel SAM	Oct 1, 2013 5:05:05 AM EST	Oct 1, 2013 5:05:05 AM EST
ALU_Juniper	Alcatel SAM	Oct 1, 2013 5:05:24 AM EST	Oct 1, 2013 5:05:24 AM EST
Device_Configlet	Junos Space	Oct 1, 2013 5:24:32 AM EST	Oct 1, 2013 5:24:32 AM EST

2. In the **Manage Scripts** window, select the **Add Scripts** icon on the command bar (+).
3. In the **Add Script(s)** window, select a feature type and its corresponding vendor type from a list of features in the **Feature Type** drop-down list. These features require scripts in CPP.
4. In the **Add Script(s)** window, you can browse your local client file system for the scripts you want to be available to the Network Activate application. You can add scripts for Juniper Networks devices and for the devices of other vendors. If you select **Junos Space** in the **Vendor type** field, the window displays fields for selecting both **Configuration script** and **GUI script**.

NOTE: If you want to do service interface migration, you need to upload both **Configuration script** and the **GUI script**.

The screenshot shows the 'Add Script(s)' dialog box. The title bar is 'Add Script(s)'. Inside, there's a section titled 'Script Settings'. It contains the following fields: 'Name:' with an empty text box; 'Description:' with a larger empty text box; 'Version:' with a text box containing '1'; 'Vendor type:' with a dropdown menu showing 'Junos Space'; 'Configuration script:' with an empty text box and a 'Browse...' button to its right; and 'GUI script:' with an empty text box and a 'Browse...' button to its right. Below these fields is a note: 'Note: IE does not support uploading multiple files simultaneously'. At the bottom are 'Create' and 'Cancel' buttons.

If you select a third-party in the **Vendor type** field, the window displays a field for selecting a **Configuration script** only.

This screenshot shows the same 'Add Script(s)' dialog box, but the 'Vendor type' dropdown is now set to 'Alcatel SAM'. The 'Configuration script:' field is still empty with its 'Browse...' button. The 'GUI script:' field is no longer visible, indicating it is only shown for Junos Space. The 'Name:', 'Description:', and 'Version:' fields remain the same. The note and bottom buttons are also present.

NOTE: If you access the server on which the Junos Space software is installed as a remote client, you must copy the scripts you intend to add to the CPP system to your local client file system. That is, when you click on **Browse** to select a script, which you want to add, Junos Space opens the local client file system, not the file system of the server on which Junos Space is installed.

5. For each script, add the appropriate information for each field and click **Create**.

Creating a Cross Provisioning Platform Service Definition

Step-by-Step Procedure

Before you create a Cross Provisioning Platform service order, you must complete the following tasks:

- Import into the system the scripts that define the Juniper Networks devices.
- Import into the system the scripts that define the third-party devices.

To create a Cross Provisioning Platform service definition:

1. In the Network Activate task pane, select **CPP > Service Definitions**.

CPP > Service Orders > Create CPP Service Order

Create CPP Service Order

General Settings

Select Service Definition

ID	Name	Type
	VPLS_SD	VPLS
	P2P_SD	PW-LDP
5678	Test_SD_123	PW-LDP
1234	Test_123_P2P	PW-LDP
4321	Test_123_VPLS	VPLS

Page 1 of 1 | Displaying 1 - 5 of 5 | Show 30 items

Description:

Next Cancel

2. In the **CPP > Service Definition** window, click on the + button. The **Create Service Definition** window appears.

Create CPP Service Definition

General

Name: SD-LDP Description:

ID: 10435

Type: PW-LDP

Service Script Selections

Operation Type: Please Select

Select Scripts

Name	Vendor Type	Version
<input type="checkbox"/> PD_P2P_LDP_Create_Script_JNPR	Juniper	1
<input type="checkbox"/> PD_P2P_LDP_Modify_Script_JNPR	Juniper	1
<input type="checkbox"/> PD_P2P_LDP_Create_Script_ALU	Alcatel	1
<input type="checkbox"/> PD_P2P_LDP_Modify_Script_ALU	Alcatel	1
<input type="checkbox"/> PD_L3VPN_Create_Script_JNPR	Juniper	1
<input type="checkbox"/> PD_L3VPN_Modify_Script_JNPR	Juniper	1
<input type="checkbox"/> PD_L3VPN_Create_Script_ALU	Alcatel	1

Page 1 of 1 Displaying 1 - 47 of 47

Add Script

Selected Scripts

Name	Vendor Type	Operation Type	Action
<input type="checkbox"/> PD_P2P_LDP_Create_Script_JNPR	Juniper	Create	
<input type="checkbox"/> PD_P2P_LDP_Create_Script_ALU	Alcatel	Create	

Create Cancel

3. Enter information in the **Create Service Definition** window according to the descriptions in the following table.

Parameter	Description
Name	Enter a name for the service.
Description	Enter a description of the service to distinguish its operation from others.
Type	<p>Select the service type from the list of available types:</p> <ul style="list-style-type: none"> • PW-LDP • VPLS • L3VPN • NPS • Device—If you select Device, the SAM Service Scripts parameter disappears. This type is for Juniper Networks devices only.

Parameter	Description
SAM Service Scripts	<p>This parameter provides two fields:</p> <ul style="list-style-type: none"> • Creation—One at a time, browse for the scripts you want to attach to the service definition. • Modification—Browse for a modified version of a script of the same name that was initially attached to the service definition. Junos Space compares the two scripts and generates a script that includes the new information.
Junos Space Service Scripts	<p>This parameter provides two fields:</p> <ul style="list-style-type: none"> • Creation—One at a time, browse for the scripts you want to attach to the service definition. • Modification—Browse for a modified version of a script of the same name that was initially attached to the service definition. Junos Space compares the two scripts and generates a script that includes the new information.

4. Click **Create**.
5. In the Network Activate task pane, select **CPP > Service Definitions**.
6. Select the service definition you just created and select **Action > Publish Service Definition**. The **State** column indicates when the service definition is published.

Creating a Cross Provisioning Platform Service Order

Step-by-Step Procedure

Before you create a Cross Provisioning Platform service order, you must complete the following tasks:

- Import into the system the scripts that define the Juniper Networks devices.
- Import into the system the scripts that define the third-party devices.
- Create the service definition upon which to base the service order.

To create a Cross Provisioning Platform service order:

1. In the Network Activate task pane, select **CPP > Service Orders**.
2. In the **CPP > Service Orders** window, click the + button. The **Create CPP Service Order** window appears.

CPP > Service Orders > Create CPP Service Order

Create CPP Service Order

General Settings

Select Service Definition

ID	Name	Type
	VPLS_SD	VPLS
	P2P_SD	PW-LDP
5678	Test_SD_123	PW-LDP
1234	Test_123_P2P	PW-LDP
4321	Test_123_VPLS	VPLS
7654	Test_SD_L3VPN	L3VPN
	L3VPN-SD	L3VPN

Page 1 of 1 | Displaying 1 - 7 of 7 | Show 30 items

Description:

Next Cancel

3. In the **Service definition** field, browse for the name of the published service definition upon which you want to base the service order.
4. In the **Order description** field, enter a description of the service that distinguishes its operation from others.
5. Click **Next**. The **Endpoint Settings** window appears.

NOTE: The following representation of an **Endpoint Settings** window is a sample only. The appearance of the **Endpoint Settings** window is based on the scripts that are associated with the service definition upon which the service is based.

6. Enter information for the parameters of the **Endpoint Settings** window according to the descriptions in the following table.

Parameter	Description
General	
Name	Enter a unique name for the service order to distinguish it from others that operate differently.
Jumbo	
Jumbo frame 3900	Sets the MTU frame size to 3900
Jumbo frame 9000	Sets the MTU frame size to 9000
	Default: 1596
Site B Selector	
Site B port type	Customer Facing Port
	Network Facing Port
Site A – Customer Facing Port	

Parameter	Description
Site name	Select the device from the list of devices displayed.
Resync now	Resyncs the interface on the selected device. NOTE: This parameter pertains to third-party devices only.
Port	Select a port from the list of ports displayed.
Service speed	Select the appropriate bandwidth for the selected site.
Canoga device?	If you select this check box, the software checks to determine whether the device is a Canoga device.
Anda untagged?	If you select this check box, the software checks to determine whether the device is an untagged Anda device.
Outer encapsulation	Enter an integer, or select the up or down arrow to select a value for the Outer encapsulation.
Validate	If this check box is selected, the system validates the encapsulation value with the specified site and port.
Untagged/802.1q?	If this check box is selected, the software checks to determine whether 802.1q was specified as the Ethernet option in UNI Settings.
Inner encapsulation	Enter an integer, or select the up or down arrow to select a value for the Inner encapsulation.

L2 Extension

Site name	Select the device from the list of devices displayed.
UNI port	Select a UNI port from the list of ports displayed.
Uplink port	Select a NNI port form the list of ports displayed.
UNI encapsulation	Enter an integer, or select the up or down arrow to select a value for the UNI encapsulation.
Validate	If this check box is selected, the system validates the encapsulation value with the specified site and port.

Site B – Customer Facing Port

Parameter	Description
Site name	Select the device from the list of devices displayed.
Resync now	Resyncs the interface on the selected device. NOTE: This parameter pertains to third-party devices only.
Port	Select a port from the list of ports displayed.
Service speed	Select the appropriate bandwidth for the selected site.
Canoga device?	If you select this check box, the software checks to determine whether the device is a Canoga device.
Anda untagged?	If you select this check box, the software checks to determine whether the device is an untagged Anda device.
Outer encapsulation	Enter an integer, or select the up or down arrow to select a value for the Outer encapsulation.
Validate	If this check box is selected, the system validates the encapsulation value with the specified site and port.
Untagged/802.1q?	If this check box is selected, the software checks to determine whether 802.1q was specified as the Ethernet option in UNI Settings.
Inner encapsulation	Enter an integer, or select the up or down arrow to select a value for the Inner encapsulation.
L2 Extension	
Site name	Select the device from the list of devices displayed.
UNI port	Select a UNI port from the list of ports displayed.
Uplink port	Select a NNI port from the list of ports displayed.
UNI encapsulation	Enter an integer, or select the up or down arrow to select a value for the UNI encapsulation.

Parameter	Description
Validate	If this check box is selected, the system validates the encapsulation value with the specified site and port.

7. Click **Create** or click **Create More** to provision additional endpoints.

Deploying Services

Step-by-Step Procedure

To schedule a service for deployment:

1. Select > **CPP** > **Service Orders**.

The **Service Orders** page displays the list of service orders.

2. Select the service order you want to deploy.

3. Open the **Actions** menu and click **Deploy Service Order**.

The **Deploy Service** window appears.

4. To deploy the service immediately, select **Deploy now**, and click **OK**.

To deploy the service at a later time, select **Deploy 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 deployment, the CPP software begins validating the service order.

33

CHAPTER

Statistics and Reports

[Viewing Service Design Statistics | 1045](#)

[Viewing Service Template Inventory | 1047](#)

[Search Techniques on the Cross Provisioning Platform Inventory Page | 1048](#)

[Managing Reports for Broadband Network Gateway Services in Cross Provisioning Platform | 1050](#)

[Viewing Service Provisioning Statistics | 1051](#)

Viewing Service Design Statistics

The following topics describe viewing statistics in the Service Design workspace:

- [Viewing Services Created from a Service Definition | 1045](#)
- [Viewing How Many Service Definitions Are in Each Service Definition State | 1046](#)

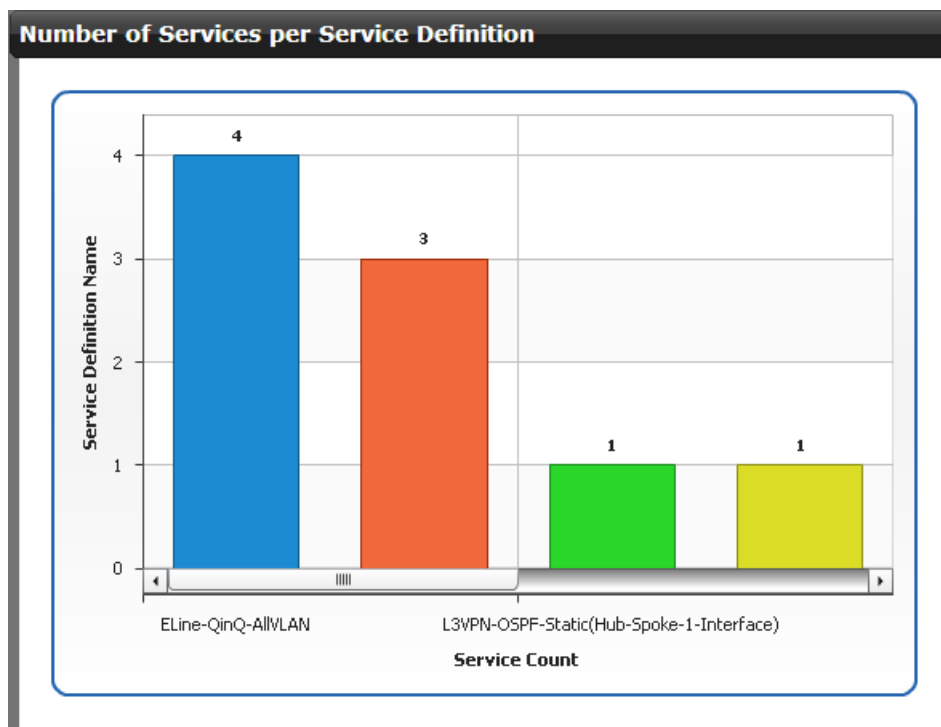
Viewing Services Created from a Service Definition

You can view the services that are associated with a service definition.

To view the number of services made from each service definition:

1. In the **Network Activate** task pane, select **Service Design**.

The Junos Space software displays the **Number of Services per Service Definition** chart.



Each vertical bar represents a service definition. The number of services is shown on the Y axis. Drag the slider across the bottom of the graph to display all service definitions. This example shows that 7 services have been created from the service definition named ELine-QinQ-AllVLAN, and 2 services have been created from the service definition name L3VPN-OSPF-Static(Hub-Spoke-1-Interface).

2. To see which services have been created from a specific service definition, click on the bar that represents the service definition.

The **Manage Services** page shows only the services created from that service definition.

SEE ALSO

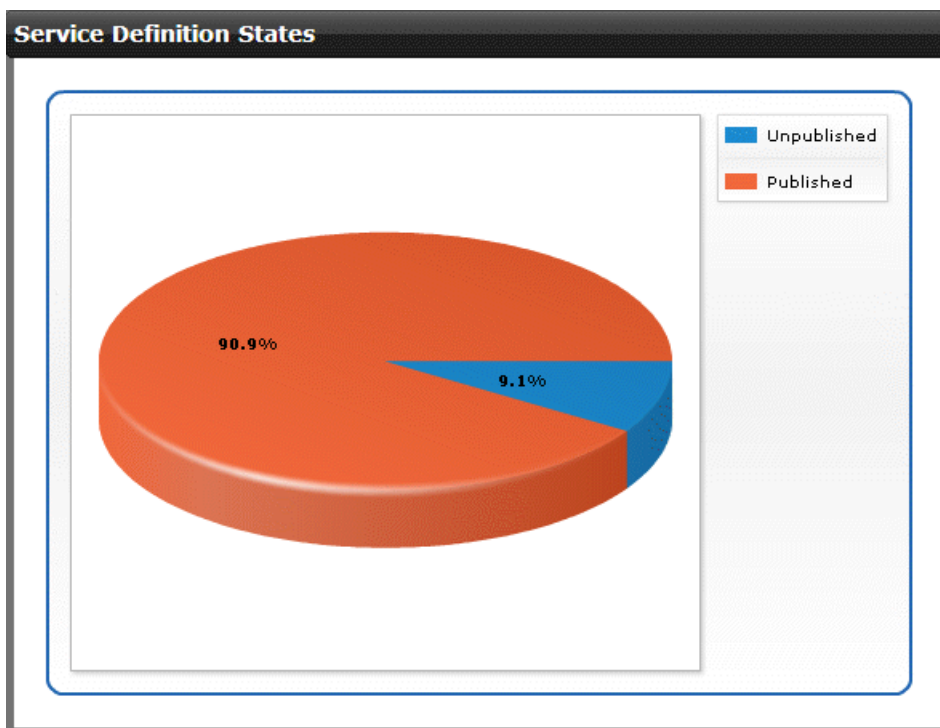
[Viewing How Many Service Definitions Are in Each Service Definition State](#) | 1046

Viewing How Many Service Definitions Are in Each Service Definition State

To view the percentage or number of service definitions that are in each service definition state:

1. In the **Network Activate** task pane, select **Service Design**.

The Junos Space software displays the **Service Definition States** chart.



Each segment of the pie chart represents the proportion of service definitions in the indicated state. In this example, 90.9 percent of all completed service definitions are in the Published state.

To view the number of service definitions in a state, move the mouse cursor over the segment.

2. To see which service definitions are in each state, click a segment in the pie chart.

The **Manage Service Definitions** page shows only those service definitions from the selected segment.

SEE ALSO

[Viewing Services Created from a Service Definition | 1045](#)

RELATED DOCUMENTATION

<i>Junos Space User Interface Overview</i>
Viewing Service Definitions 267
Viewing Services 832

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 Activate** 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 113
Modifying a Service Template 127
Deleting a Service Template 120
Exporting a Service Template 121

Tagging an Object

Viewing Tags for a Managed Object

Untagging Objects

Search Techniques on the Cross Provisioning Platform Inventory Page

In releases earlier than Cross Provisioning Platform Release 15.1R1, if you entered search criteria in the **Search** field on an inventory page, the matching entry in the **Name** column only is displayed.

With Cross Provisioning Platform Release 15.1R1, you can perform the following types of search on all the columns on an inventory page:

- **Column search by using a string**—In the **Search** field located at the top right of an inventory page, you can directly specify the search syntax in the form of a string. All columns that match the specified string are displayed.

For example, on the Service Orders inventory page, if you specify the search syntax as VPLS, all columns that include VPLS are listed in the search results.

- **Column search using the keywords**—In the **Search** field located at the top right of an inventory page, you can narrow down the search by using keywords and query expressions. The column that matches the search criteria is displayed.

For example, on the Service Orders inventory page, if you specify the search syntax along with the column name, *name:VPLS*, only the **Name** column that includes the string *VPLS* is listed in the search results.

NOTE: The column names are represented in camel case. For example, the keyword for the **Last Modified Date** column is *lastModifiedDate*.

A search syntax can include a column name and a query expression.

[Table 40 on page 1048](#) provides examples of query expressions that you can enter in the **Search** field.

Table 40: Query Expressions in the Search Field

Query Expression	Matching Contents
snmp	snmp

Table 40: Query Expressions in the Search Field (*continued*)

Query Expression	Matching Contents
snmp OR ntp	<i>snmp</i> or <i>ntp</i>
snmp AND ntp	<i>snmp</i> and <i>ntp</i>
name:snmp	<i>snmp</i> in the Name column
name:snmp AND NOT externalId:snmp	<i>snmp</i> in the Name column but not in the External ID column
(snmp OR ntp) AND http	<i>http</i> as well as <i>snmp</i> or <i>ntp</i>
description:"http server"	Exact phrase <i>http server</i> in the Description column
description: "http server"~5	<i>http</i> and <i>server</i> within five positions of one another in the Description column (that is, <i>http</i> and <i>server</i> need to have no more than five words between them)
ge-*	Terms that begin with <i>ge-</i> , such as <i>ge-0/0/1</i> or <i>ge-0/0/1.4</i>
s??p	Terms such as <i>sntp</i> or <i>snmp</i>
lastModified:[1/1/2012 TO 12/31/2012]	Last modified column values between the dates January 1, 2012 and December 31, 2012
port:(80 8080 8888)	<i>80</i> , <i>8080</i> , or <i>8888</i> in the Port field
IPAddress:10.1.1.1	<i>10.1.1.1</i> or <i>10.1.1.0/24</i> in the IPAddress field

NOTE: While specifying the keyword in the **Search** field, you can use the down arrow to view the search hint string.

In the query expression, the following special characters must be suffixed with a backslash (\):

+ ~ & || ! () { } [] ^ " ~ * ? : \

RELATED DOCUMENTATION

[Creating a Cross Provisioning Platform Service Definition](#) | 305

Managing Reports for Broadband Network Gateway Services in Cross Provisioning Platform

The report management functionality is used to query live data from a device by using RPC commands. The output of the RPC commands can be represented in the following ways:

- Chart
- HTML
- Text

This data is used to troubleshoot configurations and view device statistics. The script designers determine the format in which the output of the RPC calls is represented. One of the major features of the report management functionality is the generation of live reports.

To activate this functionality, you need to upload the report-based parser XSLT and the GUI script by using the script management functionality. Also, create a service definition of the **Report** type by combining the GUI script and the XSLT parsing script.

The report management functionality is supported only on Juniper Networks devices.

To generate live reports:

1. In the **Cross Provisioning Platform** task pane, select **CPP > Report Management**.

The **Report Management** page that appears consists of the following tab:

- **Generate Live Reports**

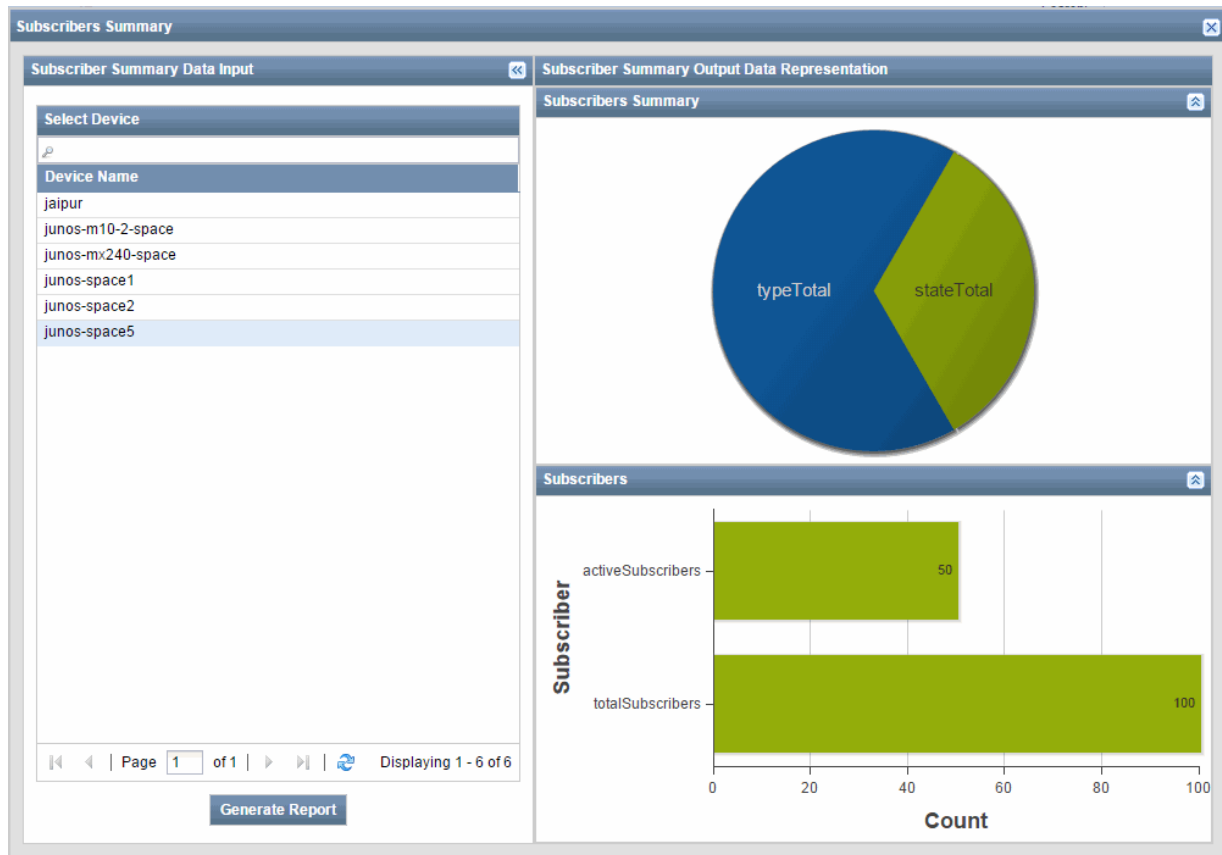
NOTE: The **Generate Live Reports** tab is pre-selected and displays a list of existing report definitions.

2. Right-click any report definition and select **Run Report**.

The GUI scripts of the associated service definitions appear. For example, the **getsubscriberinfo** script is attached to display the subscriber information on the **Subscribers Summary** page.

3. Select any device by clicking the corresponding checkbox and click the **Generate Report** link.

The adjacent sections of the page displays **Subscribers Summary** and the **Subscribers Count** details in any of the following formats: graph, HTML or text.



You can also add a new report definition from the **Cross Provisioning Platform > CPP** task pane on the **Scripts** page.

RELATED DOCUMENTATION

Providing Broadband Network Gateway Service Support in Cross Provisioning Platform

Viewing Service Provisioning Statistics

The Service Provisioning workspace provides a visual overview of customers and service orders on your network, and enables you to quickly access related and commonly needed information.

The following topics describe viewing statistics in the Service Provisioning workspace:

- [Viewing Service Orders by Customer | 1052](#)
- [Viewing the Percentage of Service Orders in Each Service Order State | 1053](#)

Viewing Service Orders by Customer

To view the number of service orders created for each customer:

1. In the **Network Activate** task pane, select **Service Provisioning**.

The system displays the chart named Services by Customer.



Each vertical bar represents a customer. The number of service orders is shown on the Y axis. In this example, three service orders has been issued on behalf of Best Customer.

2. To list the service orders created for a specific customer, click on the bar that represents the customer.

The **Manage Service Orders** page shows only those service orders made on behalf of the selected customer.

SEE ALSO

[Viewing the Percentage of Service Orders in Each Service Order State | 1053](#)

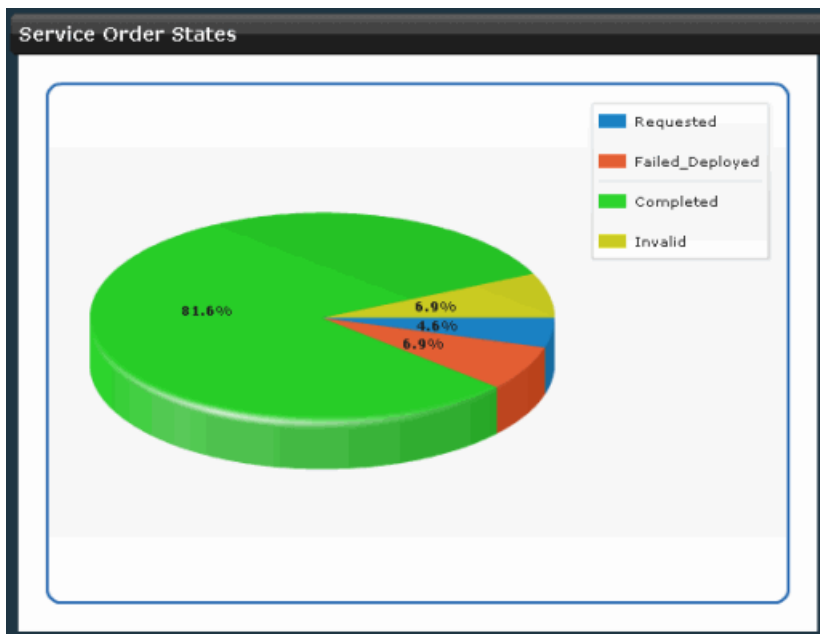
Viewing the Percentage of Service Orders in Each Service Order State

You can view service orders in a specific state. For example, you can check for failed service orders and then access a list of failed requests so you can begin to take corrective action.

To view service orders by service order state:

1. In the **Network Activate** task pane, select **Service Provisioning**.

The system displays the chart named Service Order States.



Each segment of the pie chart represents the proportion of service orders in a specific service order state:

- **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 Network Activate software 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.

2. To list the service orders in a specific state, click on the state's segment of the pie chart.

The **Manage Service Orders** page shows only those services in the specified state.

SEE ALSO

[Creating a Point-to-Point ATM or TDM Pseudowire Service Order | 578](#)

[Creating a Point-to-Point Service Order | 586](#)

[Viewing Service Orders by Customer | 1052](#)

RELATED DOCUMENTATION

[*Junos Space User Interface Overview*](#)

[Viewing Services | 832](#)

[Viewing Service Orders | 620](#)

34

CHAPTER

Customer Operations

[Adding a New Customer | 1056](#)

[Deleting Customers | 1057](#)

[Editing an Existing Customer | 1058](#)

[Viewing Customers | 1059](#)

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. In the **Network Activate** task pane, select **Service Provisioning > Manage Customers > Create Customer**.
2. On the **Create Customer** window, provide the information requested for the customer, similar to the following example.

Service Provisioning > Manage Customers > Create Customer

Create Customer

Name:

Account number:

Contact name:

Contact email:

Contact information:

Image File:

Fill out the fields in the form.

The **Name** and **Account number** fields are required. All other fields are optional.

3. Optionally, use the **Image File** field to upload a graphical image of the customer. This image will represent the customer in Junos Space windows to easily identify information about that customer. For example, the image might use the customer's corporate logo.

To upload an image file for the customer:

4. Click **Create**.

The **Manage Customers** page shows the new customer.

To upload an image file for the customer:

1. In the **Image File** field, click **Browse**.
2. Select the file that contains the image you want to use for this customer.
3. Click **Upload**.
4. Click **Create**.

The **Manage Customers** page shows the new customer.

RELATED DOCUMENTATION

[Viewing Customers | 1059](#)

[Editing an Existing Customer | 1058](#)

[Deleting Customers | 1057](#)

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. In the **Network Activate** task pane, select **Service Provisioning > Manage Customers**.

The **Manage Customers** page shows the customers in the database.

2. Select the customer you need to delete. To delete several customers at the same time, use the multiple selection capability in the quick-look panel.
3. Open the **Actions** menu and click **Delete Customer**.

If the **Delete Customer** option is dimmed, drag your mouse over **Delete Customer** to display a tool tip that lists customers that must be cleared for the operation to succeed.

After successfully selecting the **Delete Customer** action, a pop-up window appears requesting confirmation.

4. Click **Delete**.

The **Manage Customers** page no longer lists the deleted customer.

RELATED DOCUMENTATION

[Viewing Customers | 1059](#)

[Adding a New Customer | 1056](#)

[Editing an Existing Customer | 1058](#)

[Decommissioning a Service | 834](#)

Editing an Existing Customer

To edit the information about an existing customer:

1. In the **Network Activate** task pane, select **Service Provisioning > Manage Customers > Service Provisioning**.

The **Manage Customers** page shows the customers already added to the system.

2. In the **Manage Customers** page, select the customer whose information you want to edit.
3. Open the **Actions** menu and click **Modify Customer**.
4. Make the required changes to the customer information.
5. Click **Modify**.

The **Manage Customers** page shows the modified information.

RELATED DOCUMENTATION

[Viewing Customers | 1059](#)

[Adding a New Customer | 1056](#)

[Deleting Customers | 1057](#)

Viewing Customers

The following topics describe how to view customer information either as graphics or in a table.

- [Viewing Customers as Graphics | 1059](#)

- [Viewing Customers in a Table | 1059](#)

Viewing Customers as Graphics

To view your customers:

1. In the **Network Activate** task pane, select **Service Provisioning > Manage Customers**.
2. 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.
3. For details about a specific customer, double-click the listed customer.

The **Details** window displays the customer name, account number, contact name, contact e-mail address, and contact information.

SEE ALSO

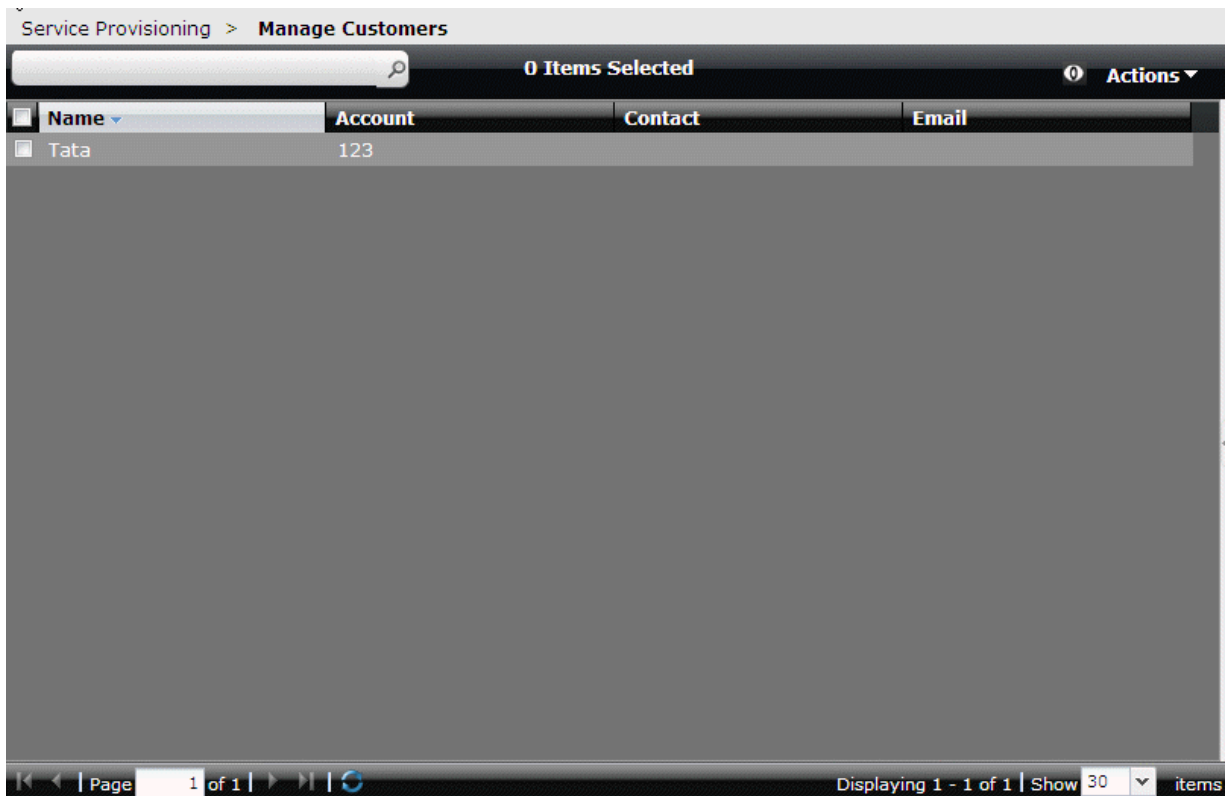
[Viewing Customers in a Table | 1059](#)

Viewing Customers in a Table

To view a list of your customers in a table:

1. In the **Network Activate** task pane, select **Service Provisioning > Manage Customers**.

A list of customers appears in a table in the main display area of the page. The table includes the customer name, account number, contact name, and e-mail address.



The screenshot shows a web application interface for 'Manage Customers'. At the top, there is a breadcrumb 'Service Provisioning > Manage Customers' and a search bar. Below the search bar, a status bar indicates '0 Items Selected' and an 'Actions' dropdown. The main area contains a table with the following data:

<input type="checkbox"/>	Name	Account	Contact	Email
<input type="checkbox"/>	Tata	123		

At the bottom, a pagination bar shows 'Page 1 of 1' and 'Displaying 1 - 1 of 1 | Show 30 items'.

2. 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.

SEE ALSO

[Viewing Customers as Graphics | 1059](#)

RELATED DOCUMENTATION

[Adding a New Customer | 1056](#)

[Editing an Existing Customer | 1058](#)

[Deleting Customers | 1057](#)

35

CHAPTER

Auditing

Performing a Configuration Audit | **1062**

Performing a Functional Audit | **1064**

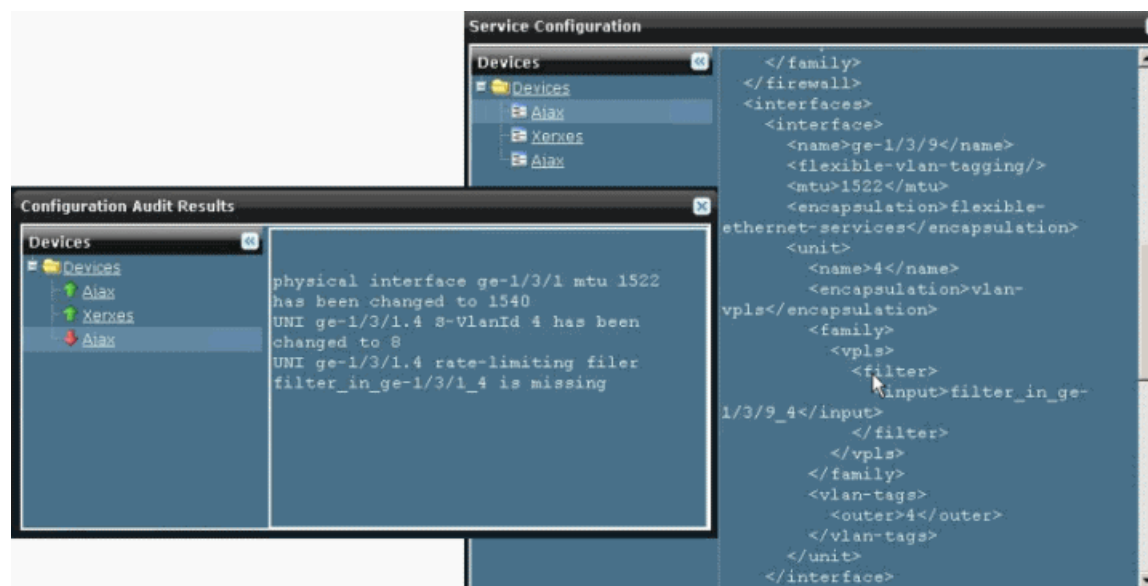
Viewing Configuration Audit Results | **1078**

Viewing Functional Audit Results | **1081**

Viewing Functional Audit Results for an Inverse Multiplexing for ATM Service | **1086**

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. In the **Network Activate** task pane, select **Service Provisioning > Manage Services**.
2. In the **Manage Services** page, select the service you want to investigate.
3. Open the **Actions** menu and select **Perform Configuration Audit**.
4. In the **Schedule Configuration Audit** window, either:
 - Select **Audit Now**, then click **OK**.
An **Audit Information** window appears, providing a link to details about the audit in the **Job Management** workspace, and an **OK** button.
 - Select **Audit Later**, enter a date and time, then click **OK**.
5. 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 functional audit job.
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. In the **Network Activate** task pane, 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.
6. 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.

Job Management > Manage Jobs										
<input type="text"/> Actions										
ID	Name	Per...	State	Job T...	Summary	Sche...	Act...	End...	User	R...
1545607	VPLS_SO_withST ConfigAudit	100.0	 SUC...	Confi... Audit	Audited [VPLS_S... -10-30 20:08:28... Success on Device [junos- mx80-1- space] Success on Device [junos- mx80-1- space] Success on Device [junos- mx80-2- space]	Oct 30, 2012 4:08:... PM EDT	Oct 30, 2012 4:0... PM EDT	Oct 30, 2012 4:0... PM EDT	super	

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*.

7. In the **State** 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.

For details about using the **Job Management** workspace, see *Viewing Jobs* in the *Junos Space Network Application Platform User Guide*.

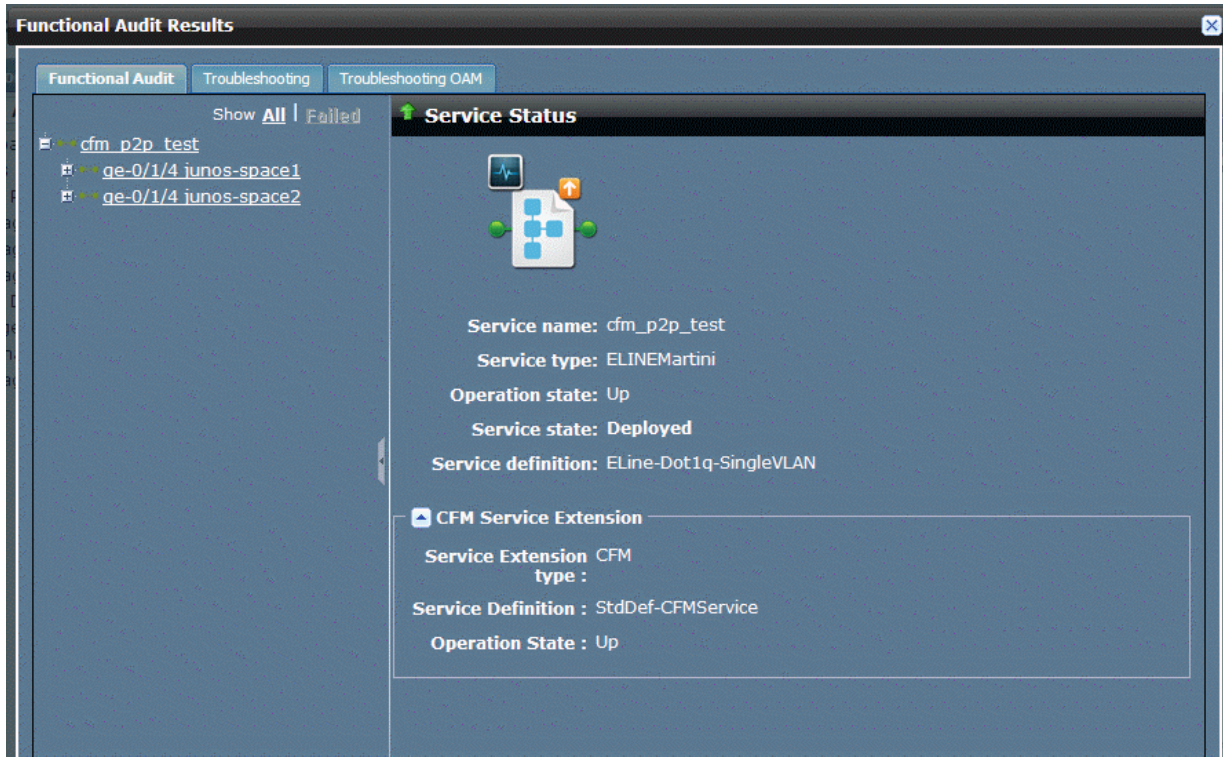
RELATED DOCUMENTATION

Viewing Configuration Audit Results 1078
Performing a Functional Audit 1064
Viewing Functional Audit Results 1081
Canceling a Job

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** tab on the **Functional Audit Results** window displays information about the service statistics for the link you are monitoring. The **Troubleshooting** tab displays status of the interfaces, LDP sessions, neighbor links, and endpoints.



Performing the Functional Audit

To perform a functional audit:

1. In the **Network Activate** task pane, select **Service Provisioning > Manage Services** to display the **Manage Services** inventory page.
2. On the **Manage Services** page, select the service you want to audit.
3. Right-click a service or open the **Actions** menu to display the list of possible functions.

Service Provisioning > **Manage Services**

Name	Customer	State	FA Status	Fault State	
VPLS_SO_withST	October	✓ Deployed	Pending	Up	
SO_ELine-BGP-Dot1q-SingleVLAN_bulk_2	October	✓ Deployed	Pending	None	
SO_ELine-BGP-Dot1q-SingleVLAN_bulk_1	October	✓ Deployed	Pending	Down	
LVPN_SO1	October	✓ Deployed	Pending	Up	
VPLSSO_1	October	✓ Deployed	Down	Up	
P2P_QinQ_ALL_V...	October	✓ Deployed	Down	None	
cfm_p2p_test	October	✓ Deployed	Up	Up	

Actions

- Service
- Audit
- View Results
- PM Statistics
- View Service Alarms
- Tag It
- View Tags
- UnTag It

Page 1 of 1 | Displaying 1 - 7 of 7 | Show 30 items

Select **Perform Functional Audit**. From the **Monitoring** window you may choose either the functional audit or troubleshooting.

4. In the **Schedule Functional Audit** dialog box, do one of the following:

- 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.

- 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:

- In the **Network Activate** task pane, select **Jobs**.
- 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.

- 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.

5. Click the Job ID link in the **Audit Information** window. The **Job Management** page shows information about the functional audit job.

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.

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 1081](#).

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.

Service Type/ Device Type	XML Commands		CLI Commands	
	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>			

Service Type/ Device Type	XML Commands		CLI Commands	
	Control Plane	Data Plane	Control Plane	Data Plane
BX Series	Not supported.	<pre><get-l2circuit-information> <l2circuit-name> <i>name</i></l2circuit-name> <brief/> </get-l2circuit-information></pre>	Not supported.	<pre>show l2circuit <i>name</i> brief</pre>
	<p>Where:</p> <p>Name = name of the l2 circuit ID</p>			
VPLS/ M Series	<pre><get-vpls-connection-information> <instance> <i>routing_instance_name</i> </instance> <local-site> <i>local-siteID</i> </local-site> <remote-site> <i>remote-siteID</i> </remote-site> </get-vpls-connection-information></pre>	<pre><request-ping-vpls-instance> <instance-name> <i>routing_instance_name</i> </instance-name> <destination-mac> <i>destMacValue</i> </destination-mac> <source-ip> <i>sourceIP</i> </source-ip> <learning-vlan-id> <i>learning-vlan-id</i> </learning-vlan-id> </request-ping-vpls-instance></pre>	<pre>show vpls connections instance <i>routing_instance_name</i> local-site <i>local-siteID</i> remote-site <i>remote-siteID</i></pre>	<pre>ping vpls instance <i>routing_instance_name</i> destination-mac <i>destMacValue</i> source-ip <i>sourceIPValue</i> learning-vlan-id <i>learningVlanID</i></pre>
	<p>Where:</p> <p><i>routing_instance_name</i> = Routing instance name</p> <p><i>destMacValue</i> = Destination MAC address</p> <p><i>sourceIP</i> = Source IP address</p> <p><i>local-SiteID</i> = Name or ID of VPLS local site</p> <p><i>remote-SiteID</i> = ID of VPLS remote site</p> <p><i>learning-vlan-id</i> = Learning VLAN identifier</p>			
L3VPN/ Junos	<pre><get-route-information> <table> bgp.l3vpn.0</table> <rd-prefix><i>destinationRDprefix</i></rd-prefix> </get-route-information></pre>	<pre><ping><routing-instance> <i>routingInstanceValue</i> </routing-instance> <count>5 </count></pre>	<pre>show route table bgp.l3vpn.0 rd-prefix <i>destinationRDprefix</i></pre>	<pre>ping routing-instance <i>routingInstanceValue</i> count</pre>

Service Type/ Device Type	XML Commands		CLI Commands	
	Control Plane	Data Plane	Control Plane	Data Plane
	<div>Where:</div> <div><i>routingInstanceValue</i> = Routing instance name</div> <div><i>destinationRDprefix</i> = Route Distinguisher: remote UNI IP address</div> <div><i>destinationUniInterfaceIP</i> = Destination UNI IP address</div>			

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:

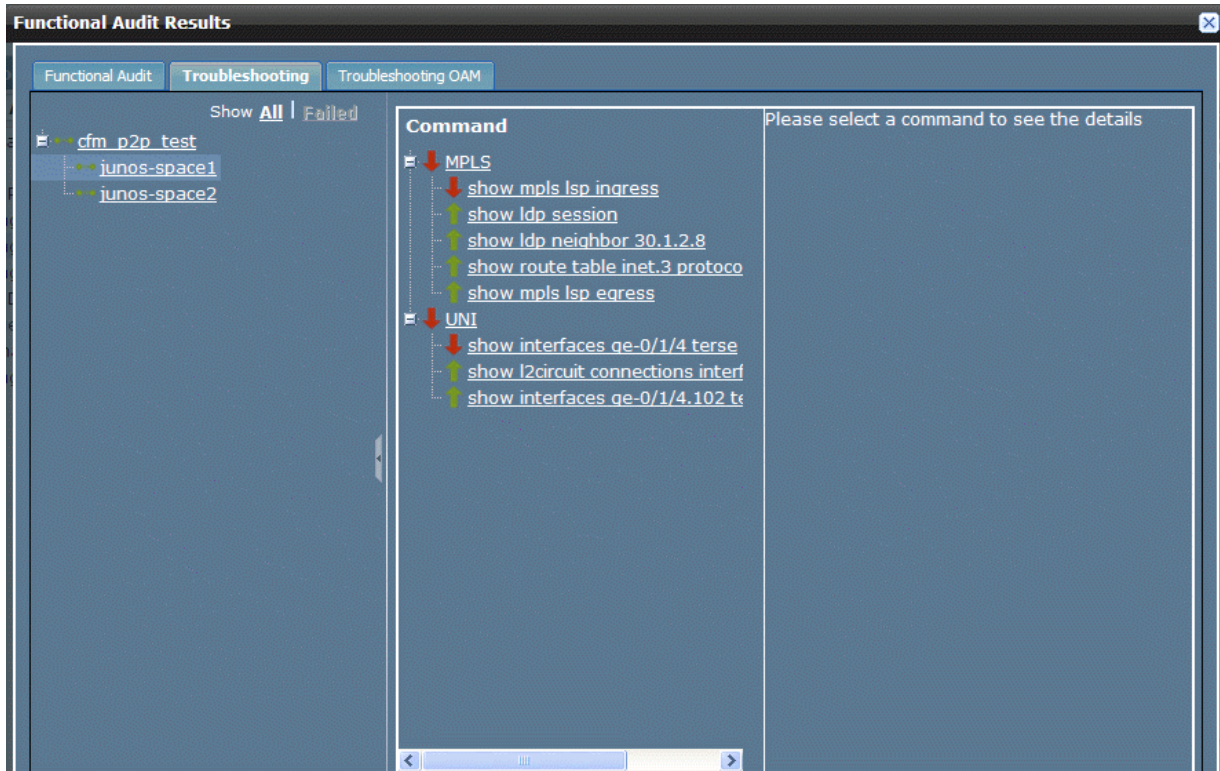
Service Type	Device Family	XML Commands	CLI Commands	Category
--------------	---------------	--------------	--------------	----------

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>instancevalue</interface-name> </get-interface-information>	show interfaces instancevalue.initvalue terse	Route
		<get-forwarding-table-information> <vpn>instance </vpn> </get-forwarding-table-information>	show route forwarding-table vpn instance	Route
		<get-rsvp-session-information> </get-rsvp-session-information>	show rsvp session	Route
		<get-interface-information> <statistics/> <interface-name>instance</interface-name> </get-interface-information>	show interfaces instance 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>bgp.l3vpn.0 </table> <rd-prefix>destinationRDprefix</rd-prefix> </get-route-information>	show route table bgp.l3vpn.0	Route
		<get-lacp-interface-information> <interface-name> lagInterface </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

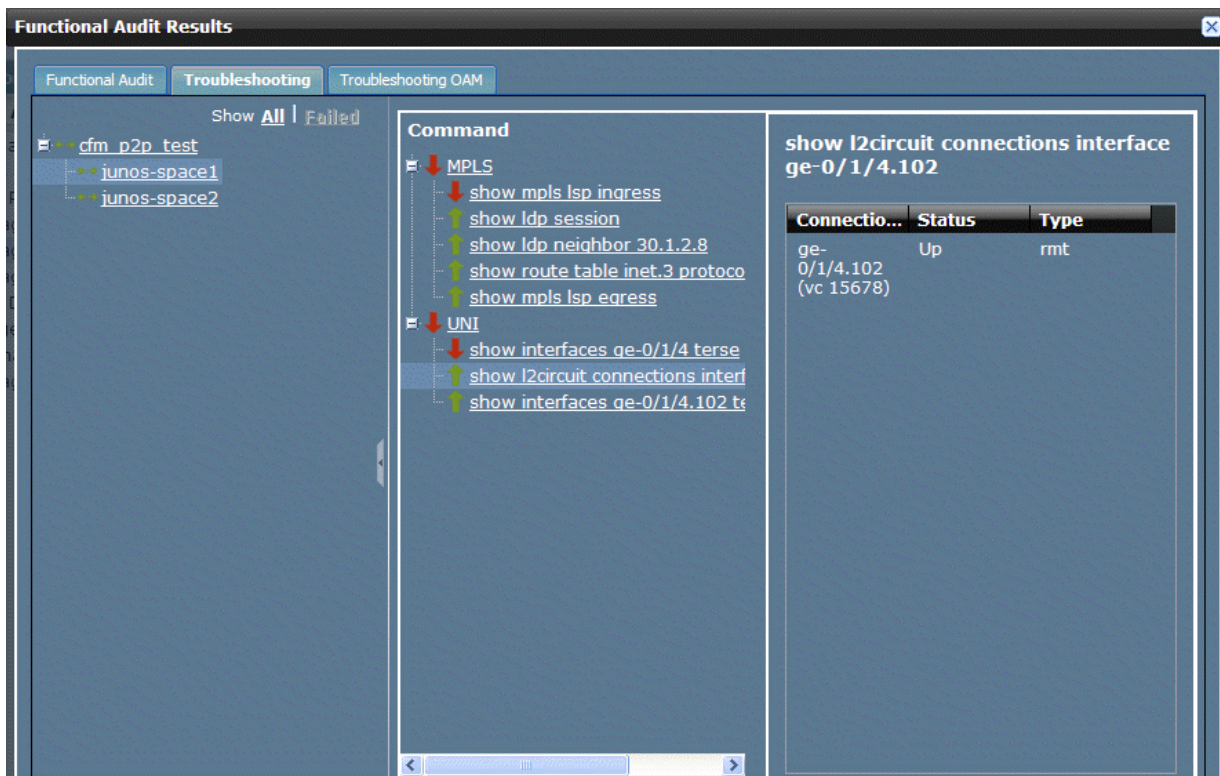
<div><get-isis-control-protocol-information> </get-isis-control-protocol-information></div>	show iscp	UNI
<div><get-vrrp-interface-information> <interface-name> Interface </interface-name> </get-vrrp-interface-information></div>	Show vrrp <i>interfaceName</i>	UNI
<div><get-bridge-instance-information> <bridge-domain-name> <i>domainName</i> </bridge-domain-name> </get-bridge-instance-information></div>	Show bridge domain <i>domainName</i>	UNI
<div>Where: <i>instanceValue</i>= Name of the service <i>neighborIP</i>= Address of the remote neighbor <i>interfaceValue</i>= Name of the interface</div>		

Troubleshooting Point-to-Point Service

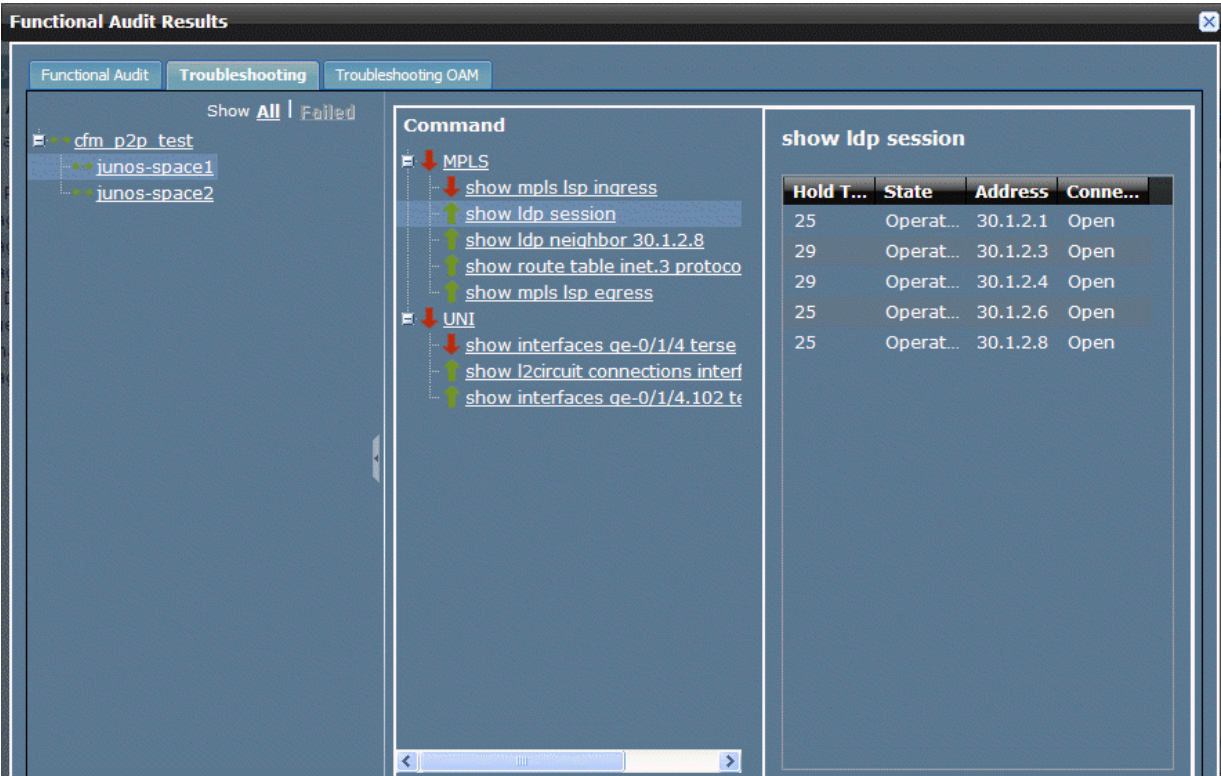
From the **Troubleshooting** tab you can check status of the interfaces, LDP sessions, neighbor links, and endpoints of a point-to-point service. To select the status you want to check, click on the device from the device list on the left, and select the show command from the **Command** list. This figure shows the routing table for the selected device in the Point-to-Point service.



The following figure shows the interface status window. The status shows that the interface is up.



The following figure shows the status of the LDP session for the selected device.



The following figure shows the LDP neighbor status.

Functional Audit Results

Functional Audit Troubleshooting Troubleshooting OAM

Show All Failed

cfm p2p test

- junos-space1
- junos-space2

Command

MPLS

- show mpls lsp ingress
- show ldp session
- show ldp neighbor 30.1.2.8
- show route table inet.3 proto
- show mpls lsp egress

UNI

- show interfaces ge-0/1/4 terse
- show l2circuit connections interf
- show interfaces ge-0/1/4.102 t

show ldp neighbor 30.1.2.8

Interface	Label	Neighbor...
lo0.0	30.1.2.8:0	30.1.2.8

Troubleshooting VPLS Service

From the **Troubleshooting** tab 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 routing table for the selected device in the VPLS service.

Functional Audit Results

Functional Audit Troubleshooting

Last Audited: 2012-10-31 05:57:00.0

- VPLS_SO_31
 - junos-mx80-2-space
 - junos-mx80-1-space

Command

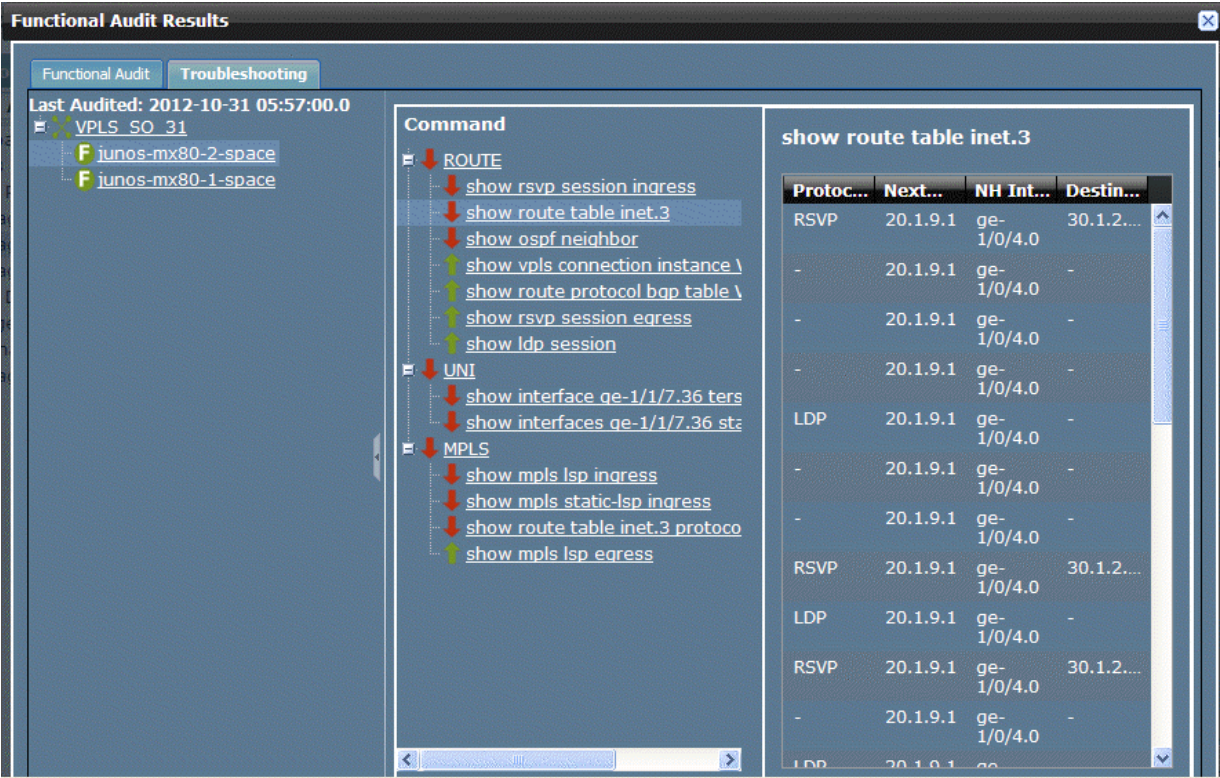
- ROUTE
 - show rsvp session ingress
 - show route table inet.3
 - show ospf neighbor
 - show vpls connection instance \
 - show route protocol bgp table \
 - show rsvp session egress
 - show ldp session
- UNI
 - show interface ge-1/1/7.36 ters
 - show interfaces ge-1/1/7.36 stz
- MPLS
 - show mpls lsp ingress
 - show mpls static-lsp ingress
 - show route table inet.3 protoco
 - show mpls lsp egress

show vpls connection instance VPLS_SO_31

Connectio...	Status	Type
1	Up	rmt

Troubleshooting L3VPN Service

From the **Troubleshooting** tab 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 routing table for the selected device in the L3VPN service.



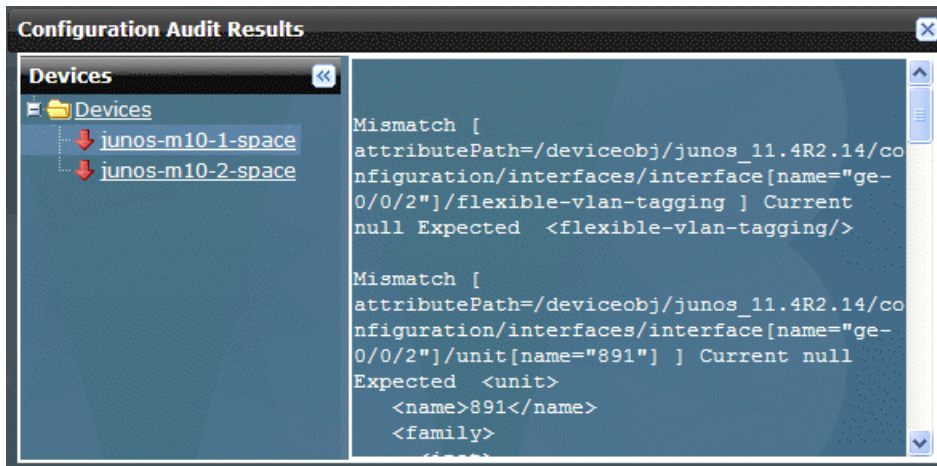
RELATED DOCUMENTATION

- [Viewing Functional Audit Results | 1081](#)
- [Performing a Configuration Audit | 1062](#)
- [Viewing Configuration Audit Results | 1078](#)

Viewing Configuration Audit Results

After performing a configuration audit, check the detailed results of the audit:

1. a. In the **Network Activate** task pane, select **Service Provisioning > Manage Services**.
- b. In the **Manage Services** page view, select the service you are investigating.
- c. Open the **Actions** menu and select **View Configuration Audit Results**.



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).

2. To view the service configuration in the Junos Space database, double click the service icon in the **Manage Services** 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.

RELATED DOCUMENTATION

[Performing a Configuration Audit | 1062](#)

[Performing a Functional Audit | 1064](#)

[Viewing Functional Audit Results | 1081](#)

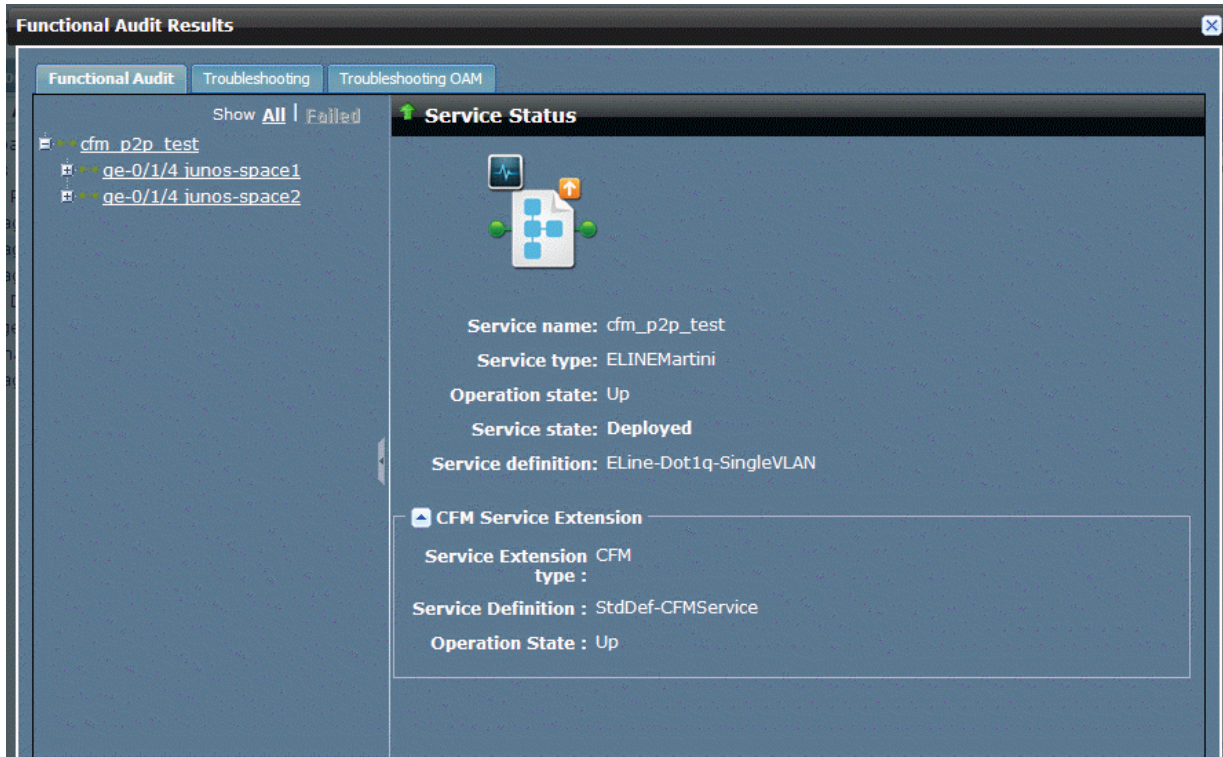
Viewing Functional Audit Results

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 1064), look at the functional audit results:

1. In the Network Activate task pane, select **Service Provisioning > Manage Services**.
2. In the Manage Services screen, select the service for which you want to view the functional audit results.
3. Either open the **Actions** drawer and select **View Functional Audit Results**, or select the same command from the right mouse-click menu.

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 Network Activate and CFM service.



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 41 on page 1083](#) describes these icons for a point-to-multipoint service.



Table 41: 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
4. 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.
 5. 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.
 6. 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 42 on page 1084](#) describes these icons.

Table 42: 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.

7. 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 43 on page 1084](#) describes icons and the textual information provided in the box beside the icon.

Table 43: 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.

Table 43: Multipoint-to-Multipoint Service Control Plane and Data Plane Validation Icons (continued)

Icon	Meaning	Explanation
	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, open the **Troubleshooting** tab. 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 44 on page 1085](#) describes these icons.

Table 44: 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.

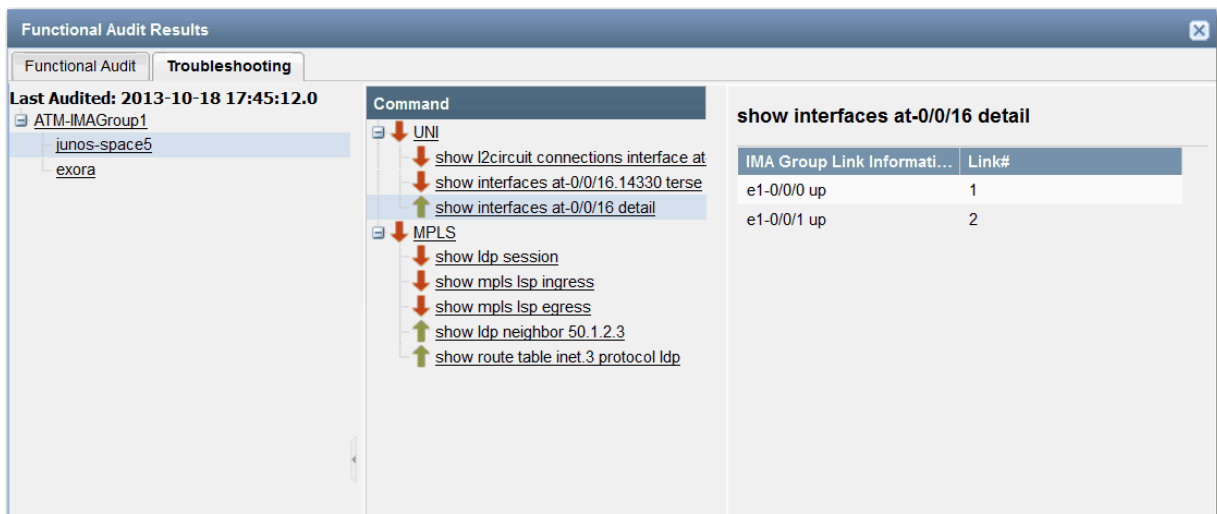
RELATED DOCUMENTATION

[Performing a Functional Audit | 1064](#)
[Performing a Configuration Audit | 1062](#)
[Viewing Configuration Audit Results | 1078](#)

Viewing Functional Audit Results for an Inverse Multiplexing for ATM Service

To view functional audit results for an Inverse Multiplexing for ATM Service:

1. In the Network Activate task pane, select **Service Provisioning > Manage Services**.
2. In the **Manage Services** screen, select the service for which you want to view the functional audit results.
3. Right-click the service, or click the **Actions** menu, and select **View Functional Audit Results**.
4. In the **Functional Audit Results** window, click the **Troubleshooting** tab.



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

[Inverse Multiplexing for ATM Overview | 612](#)

[Creating an Inverse Multiplexing for ATM Service Order | 613](#)

36

CHAPTER

Performance Management and Statistics

Performance Management Overview | **1089**

Monitoring Performance Management Statistics | **1091**

Viewing Performance Management Statistics | **1094**

Monitoring Performance Statistics Derived from MIB Objects | **1100**

Viewing Performance Statistics Collected According to SLAX Scripts | **1103**

Performance Management Overview

In performance management (PM), the Network Activate 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 Network Activate 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 Network Activate 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

[Viewing Performance Management Statistics | 1094](#)[Monitoring Performance Management Statistics | 1091](#)

Monitoring Performance Management Statistics

IN THIS SECTION

- [Monitoring Statistics for Point-to-Point Service | 1091](#)
- [Monitoring Statistics for VPLS Service | 1093](#)

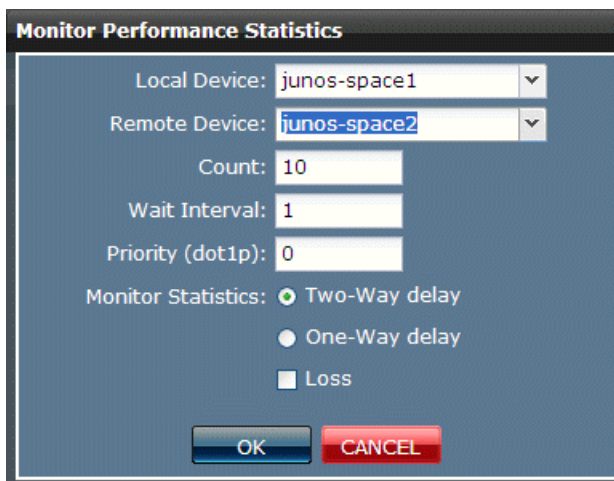
The following topics show how to monitor the performance statistics for point-to-point and VPLS services:

Monitoring Statistics for Point-to-Point Service

In the **Network Activate** task pane, select **Service Provisioning > Manage Services**.

To monitor the statistics for the point-to-point service:

1. Right-click a point-to-point service and select **Start PM Statistics**. The **Monitor Performance Statistics** window is displayed.



The **Monitor Performance Statistics** dialog box is shown. It contains the following fields and options:

- Local Device:** junos-space1 (dropdown menu)
- Remote Device:** junos-space2 (dropdown menu)
- Count:** 10 (text input)
- Wait Interval:** 1 (text input)
- Priority (dot1p):** 0 (text input)
- Monitor Statistics:**
 - ☒ Two-Way delay
 - ☐ One-Way delay
 - ☐ Loss
- Buttons:** OK and 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.

2. Fill in the fields as indicated in the table.

Field	Action
Local Device	Select a local device from the list.
Remote Device	Select a remote device from the list.
Count	Specify the number of frames to be sent to a specific peer MEP. Range: 1 through 65,535 frames Default: 10 frames
Wait Interval	Specify the wait interval for the frame transfer. Range: 1 through 255 seconds Default: 1 second
Priority (dot1p)	Select the 802.1p priority of continuity-check and link-trace packet. Range: 0 through 7 Default: 0
Monitor Statistics	Select one of the following: <ul style="list-style-type: none"> • Two-Way delay • One-Way delay • Loss

3. Click **OK**.

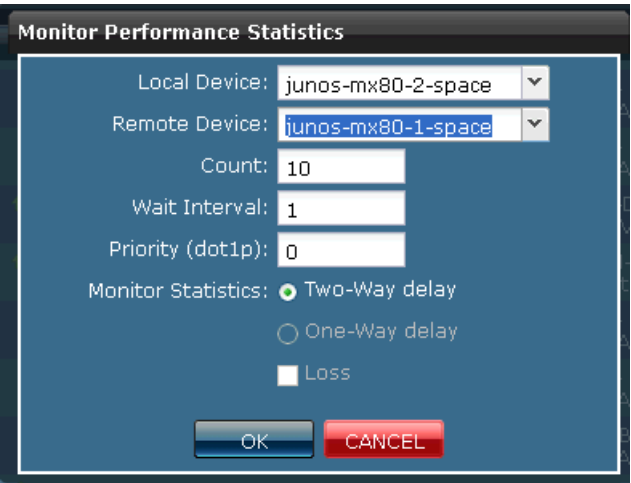
This action initiates a statistics collection on the endpoint device. The **View PM Statistics** action is enabled on successful initiation of the statistics.

Monitoring Statistics for VPLS Service

In the **Network Activate** task pane, select **Service Provisioning > Manage Services**.

To monitor the statistics for the VPLS Service:

1. Right-click a VPLS service and select **Start PM Statistics**. The **Monitor Performance Statistics** window is displayed.



The screenshot shows a dialog box titled "Monitor Performance Statistics". It contains several input fields and radio buttons. The "Local Device" dropdown is set to "junos-mx80-2-space". The "Remote Device" dropdown is set to "junos-mx80-1-space". The "Count" field is set to "10". The "Wait Interval" field is set to "1". The "Priority (dot1p)" field is set to "0". Under "Monitor Statistics", the "Two-Way delay" radio button is selected, with "One-Way delay" and "Loss" as unselected options. At the bottom, there are "OK" and "CANCEL" buttons.

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.

2. Fill in the fields as indicated in the table.

Field	Action
Local Device	Select a local device from the list.
Remote Device	Select a remote device from the list.
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
Wait Interval	Specify the wait interval for the frame transfer. Range: 1 through 255 seconds Default: 1 second
Priority (dot1p)	Select the 802.1p priority of continuity-check and link-trace packet. Range: 0 through 7 Default: 0
Monitor Statistics	Select Two-Way delay.

3. 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.

RELATED DOCUMENTATION

[Performance Management Overview | 1089](#)

[Viewing Performance Management Statistics | 1094](#)

Viewing Performance Management Statistics

IN THIS SECTION

- [Viewing Statistics for Point-to-Point Service | 1095](#)
- [Viewing Statistics for VPLS Service | 1097](#)

The following topics show how to view the performance statistics for point-to-point and VPLS services:

Viewing Statistics for Point-to-Point Service

In the **Network Activate** task pane, select **Service Provisioning** > **Manage Services**.

To view the statistics for the point-to-point service:

1. Right-click a point-to-point service and select **View PM Statistics**.

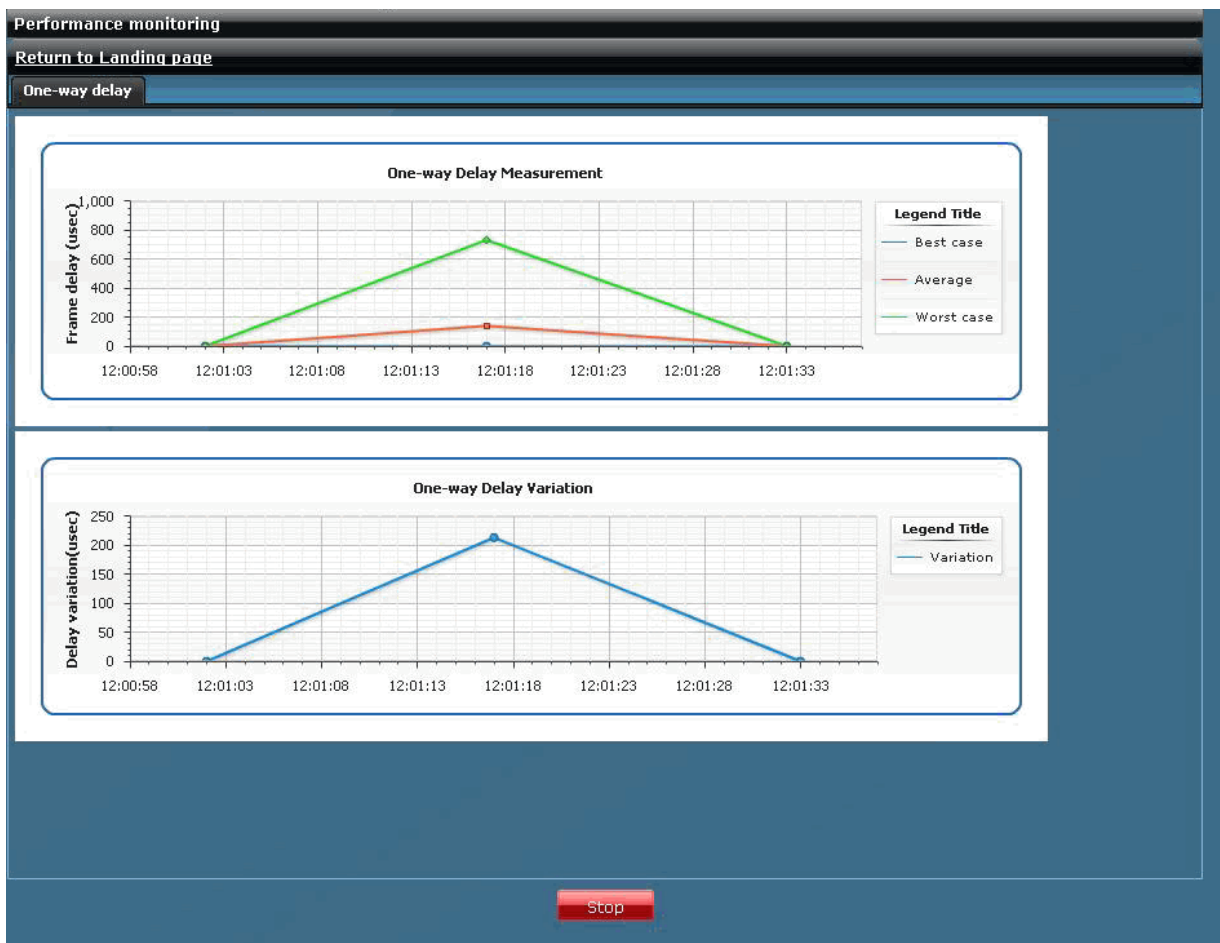
NOTE: The View PM Statistics action is enabled only after performing the Start PM Statistics.

2. View and analyze the respective graph.

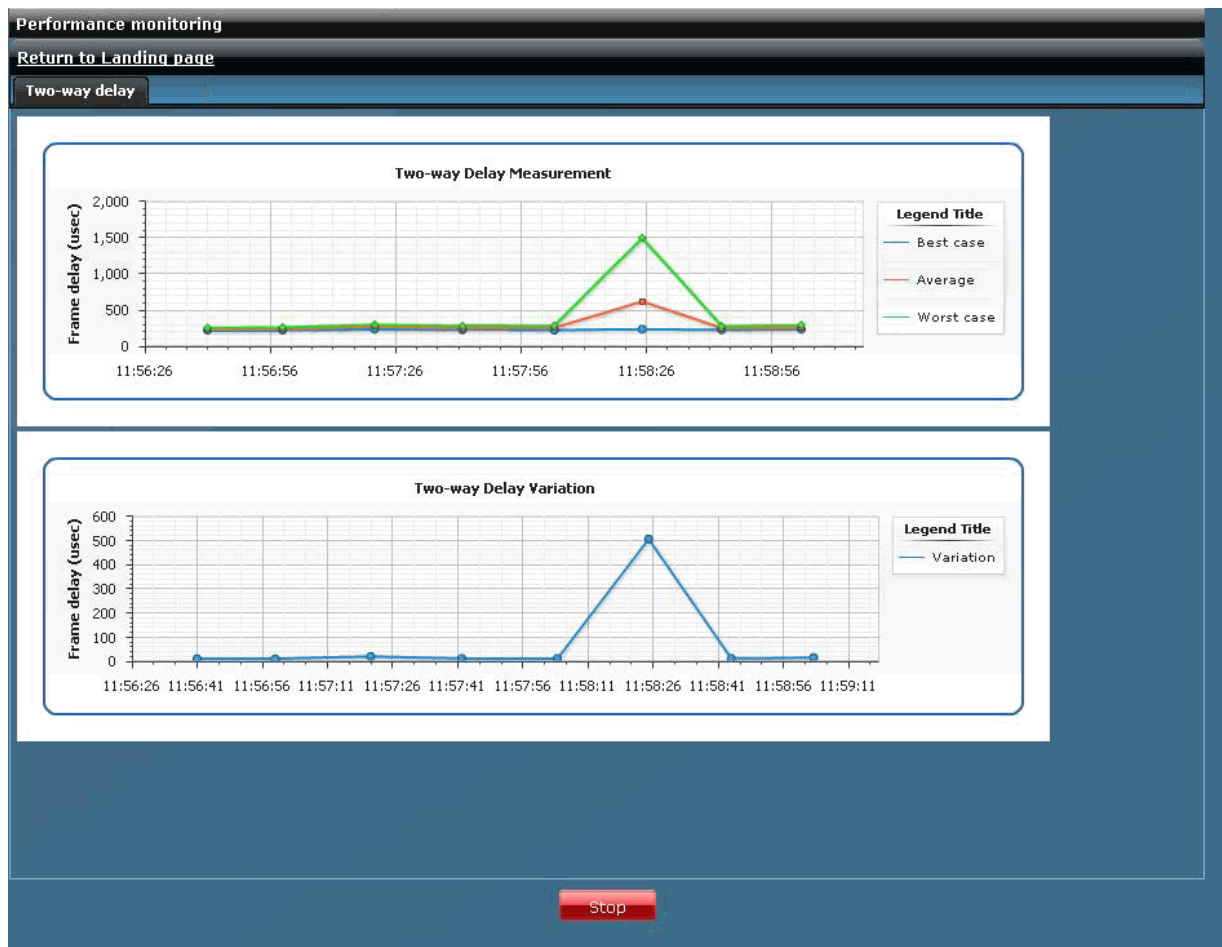
The Delay Measurement graph displays a real-time linear plot of delay value with respect to the time. The x-axis represents the time and the y-axis represent frame delay in microseconds.

The Delay Variation graph displays the difference between the consecutive frame delay values. The x-axis represents the time and the y-axis represent delay variation in microseconds.

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 tab is displayed only if you have selected the **Loss** check box. It 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. To stop the data collection, click **Stop**.

To return to the **Manage Services Landing** page, click **Return to Landing page**.

Viewing Statistics for VPLS Service

In the **Network Activate** task pane, select **Service Provisioning > Manage Services**.

To view the statistics for the VPLS Service:

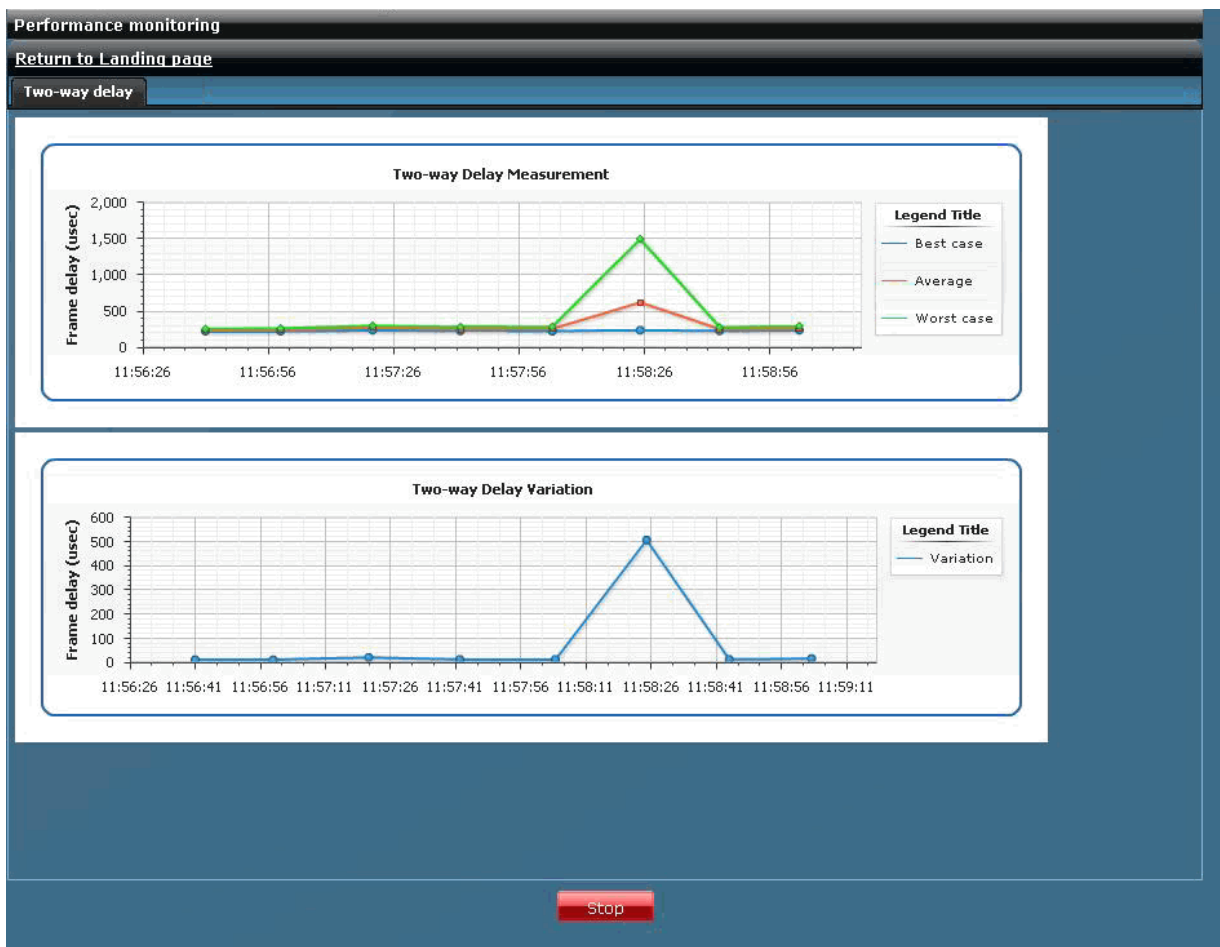
1. Right-click a VPLS service and select **View PM Statistics**. The **Monitor Performance Statistics** window appears.

NOTE: The **View PM Statistics** action is enabled only after performing the Start PM Statistics.

2. View and analyze the graphs.

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 represent frame delay in microseconds.

The Delay Variation graph displays the difference between the consecutive frame delay values. The x-axis represents the time and the y-axis represent delay variation in microseconds.



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. To stop the data collection, click **Stop**.

To return to the **Manage Services Landing** page, click **Return to Landing page**.

RELATED DOCUMENTATION

Performance Management Overview 1089
Monitoring Performance Management Statistics 1091

Monitoring Performance Statistics Derived from MIB Objects

Junos Space Release 13.1P1 enables you to collect and display performance data derived from MIB objects. The instructions for deriving the MIB data are contained in a Stylesheet Language Alternative Syntax (SLAX) script. The Network Activate application automatically edits a predefined SLAX script to detect policies that are specific to different point-to-point pseudowire or VPLS services.

To configure Junos Space to monitor service performance based on an SLAX script, you perform tasks in both the Network Management Platform application and Network Activate application.

Before you can view performance statistics collected according to SLAX scripts, you must complete some preparatory tasks. On the server on which you are running the Junos Space software, modify files in the existing directories as described in the following list:

- In the directory `/home/admin/opennmsspatch`, copy the file `collectd-configuration.xml` and replace the existing version of the file in the directory `/opt/opennms/etc/`.
- In the directory `/home/admin/opennmsspatch`, copy the file `datacollection-config.xml` and replace the existing version of the file in the directory `/opt/opennms/etc/`.
- In the directory `/home/admin/opennmsspatch`, copy the file `JNX-Util.xml` and add it to the directory `/opt/opennms/etc/datacollection/`.
- In the directory `/home/admin/opennmsspatch`, copy the file `jnxutil-graph.properties` and replace the existing version of the file in the directory `/opt/opennms/etc/snmp-graph.properties.d/`.
- In the directory `/home/admin/opennmsspatch`, copy the file `eventconf.xml` and replace the existing version of the file in the directory `/opt/opennms/etc/`.
- In the directory `/home/admin/opennmsspatch`, copy the file `JNX-Util-TCA.xml` and add it to the directory `/opt/opennms/etc/events/JuniperEvents/`.
- In the directory `/home/admin/opennmsspatch`, copy the file `threshd-configuration.xml` and replace the existing version of the file in the directory `/opt/opennms/etc/`.
- In the directory `/home/admin/opennmsspatch`, copy the file `thresholds.xml` and replace the existing version of the file in the directory `/opt/opennms/etc/`.

To collect performance data based on an SLAX script:

1. In the Network Management Platform task pane, select **Images and Scripts > Scripts**.
2. In the **Scripts** window, click the **Import Script** icon in the command bar.
3. In the **Import Script** window, click the **+** button.

4. In the **Add Device Scripts** window, browse your local file system for the SLAX script **PM.slax**.

NOTE: If you access the server on which the Junos Space software is installed as a remote client, you must copy the **PM.slax** script from the directory **/home/admin/opennmsspatch/** to your local client file system. That is, when you click on **Browse** to select the **PM.slax** script, which you want to import, Junos Space opens the local client file system, not the file system of the server on which Junos Space is installed.

5. When the script is added successfully, in the **Scripts** window, right-click the script and select **Stage Scripts on Devices**.
6. In the **Stage Scripts on Devices** window, select the device on which you want the script to manage the collection of performance data.
7. Click the **Enable Scripts on Device** check box.
8. When you complete staging scripts, in the Network Management Platform task pane, select **Administration**.
9. In the **Administration** window, right-click **Network Activate** and select **Modify Application Settings**.
10. In the **Modify Application Settings** panel, select **Performance Monitoring**.

In the **Performance Monitoring** window, the **Enable performance monitoring through scripts** check box should be enabled.

NOTE: By default, the **Enable performance monitoring through scripts** check box is disabled.

When the check box is enabled, the performance data is collected according to the SLAX scripts. If the check box is disabled, the performance data is collected according to the Y.1731 OAM method.

After you configure Junos Space to collect performance data according to SLAX scripts:

1. In the Network Activate application, create a point-to-point or VPLS service on which you attach a CFM profile.
2. Perform a Functional Audit on the service.

3. After the Functional Audit completes successfully, select **PM statistics > Start**.

At this point, the system checks to determine whether the statistics will be collected according to scripts or by the Y.1731 OAM method.

If data collection by script is enabled, the system pushes a policy to the device upon which the performance will be monitored. The script runs every 5 minutes to collect data from updated MIB objects. To see graphs for the collected performance data, to see graphs select **Network Management Platform > Network Monitoring > Reports** and select the node.

If data collection by script is disabled, to see graphs for the collected performance data, see [“Viewing Performance Management Statistics” on page 1094](#).

RELATED DOCUMENTATION

[Performing a Functional Audit | 1064](#)

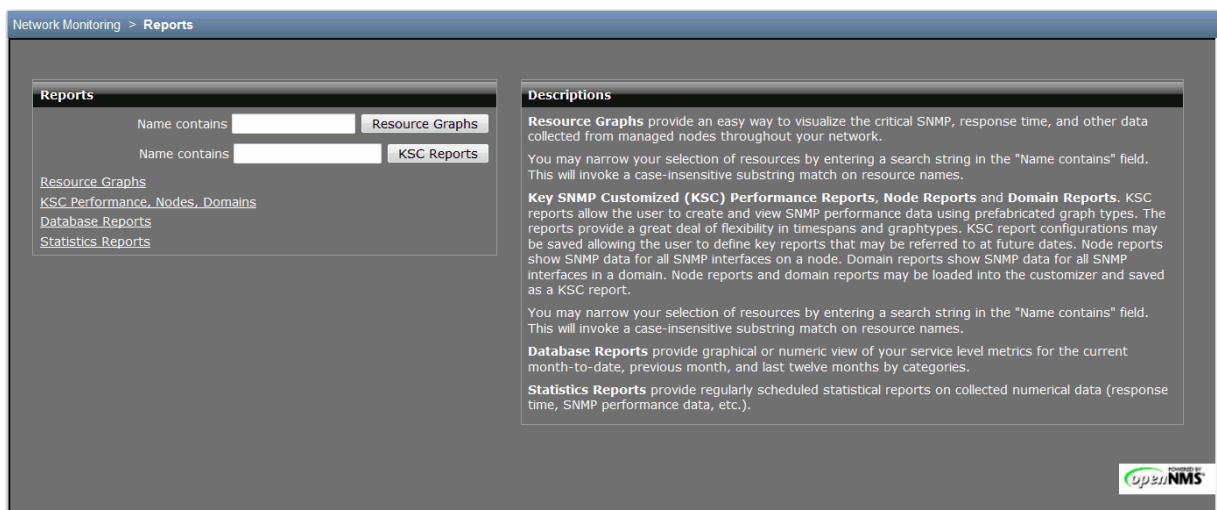
[Viewing Performance Statistics Collected According to SLAX Scripts | 1103](#)

Viewing Performance Statistics Collected According to SLAX Scripts

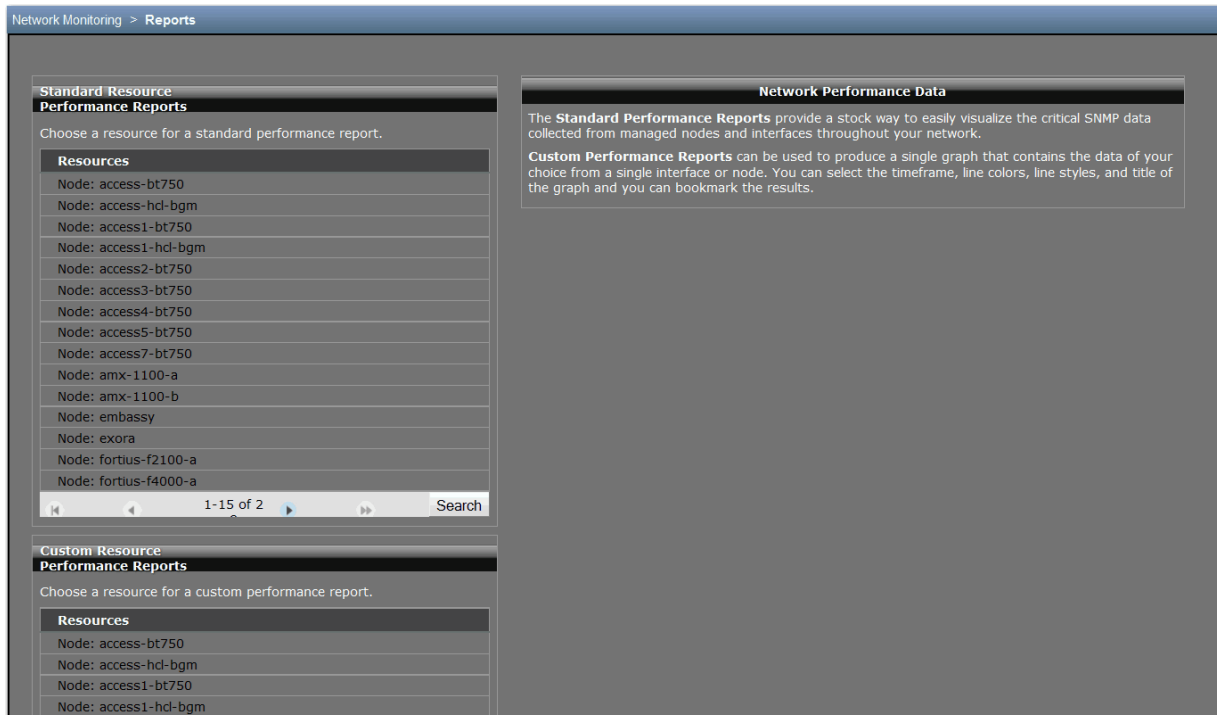
Junos Space Release 13.1P1 enables you to display performance statistics derived from MIB objects. The performance statistics are collected according to instructions contained in SLAX scripts. By default, data collection occurs once every 5 minutes (300 seconds).

To view the graphs for the collected data:

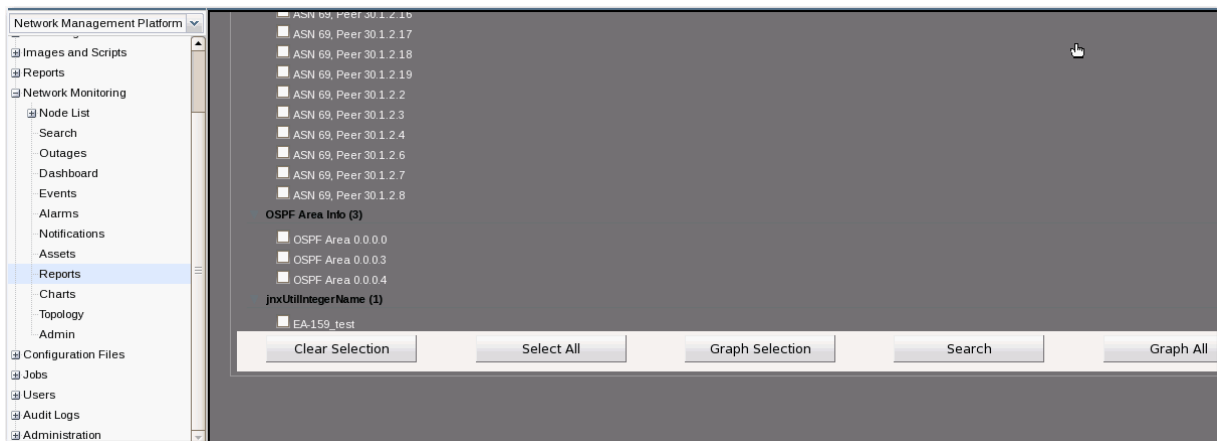
1. In the Network Management Platform task pane, select **Network Monitoring > Reports**.



2. In the **Reports** window, select **Resource Graphs**.



3. Select the node (local device) on which you have deployed a service.



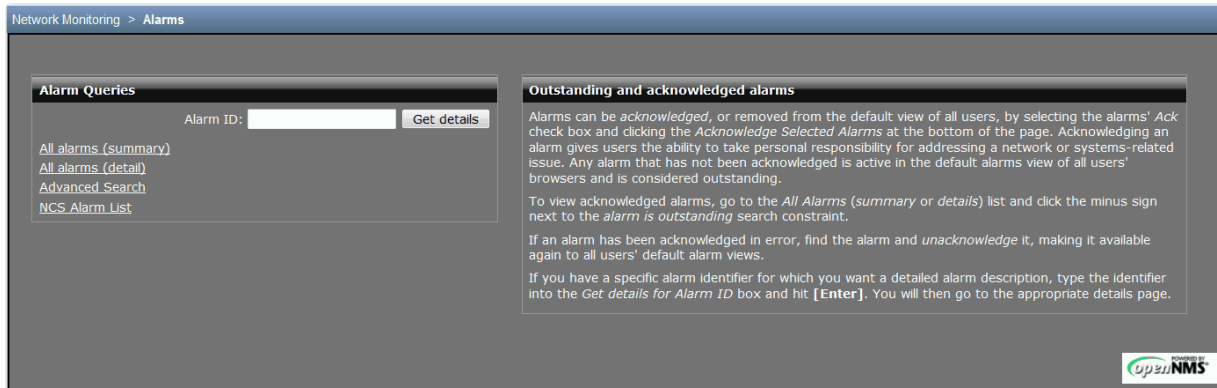
4. Select jnxUtilIntegerName, under which instances are displayed. Each instance is the service name.

5. Select the instance (that is, the service name) for which you want to view the graph.



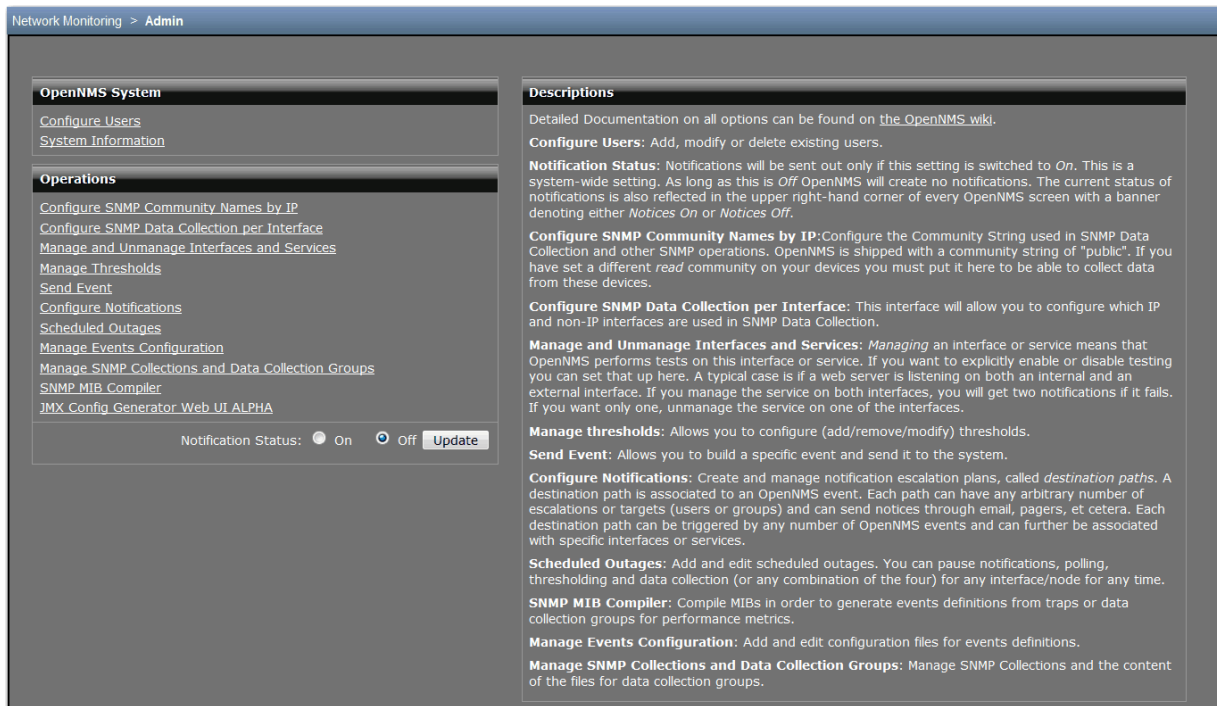
6. To stop the gathering of performance statistics, right-click the service and select **PM Stats > Stop**.

Threshold crossing alarms are generated when the value of collected data exceeds the specified threshold value. To view threshold crossing alarms, in the Network Management task pane, select **Network Monitoring > Alarms**.



You can edit the specified values for the various threshold performance parameters such as TwoWayDelayAvg, TwoWayDelayBest, TwoWayDelayWorst, and so on. To modify a threshold performance parameter value:

1. In the Network Management Platform task pane, select **Network Monitoring > Admin**.



2. Select **Manage Thresholds**.

Threshold Configuration		
Name	RRD Repository	
JNX-Util	/home/gsaranya123patch/build/opennms/share/rrd/snmp/	Edit
cisco	/home/gsaranya123patch/build/opennms/share/rrd/snmp/	Edit
coffee	/home/gsaranya123patch/build/opennms/share/rrd/snmp/	Edit
hrstorage	/home/gsaranya123patch/build/opennms/share/rrd/snmp/	Edit
mib2	/home/gsaranya123patch/build/opennms/share/rrd/snmp/	Edit
netsnmp	/home/gsaranya123patch/build/opennms/share/rrd/snmp/	Edit
netsnmp-memory-linux	/home/gsaranya123patch/build/opennms/share/rrd/snmp/	Edit
netsnmp-memory-nonlinux	/home/gsaranya123patch/build/opennms/share/rrd/snmp/	Edit
Request a reload threshold packages configuration		

3. Select JNX-Util > Edit.

Edit group JNX-Util

Type	Description	Datasource	Datasource type	Datasource label	Value	Re-arm	Trigger	Triggered UEI	Re-armed UEI		
Create New Threshold											
Type	Description	Expression	Datasource type	Datasource label	Value	Re-arm	Trigger	Triggered UEI	Re-armed UEI		
high	TwoWayDelay Avg	JnxUtilInteger Name	TwoWayDelay Avg	100.0	0.0	2	uei.opennms.org/juniper/twowaydelayavghigh	uei.opennms.org/juniper/twowaydelayavgrearm	Edit	Delete	
high	TwoWayDelay Best	JnxUtilInteger Name	TwoWayDelay Best	100.0	0.0	2	uei.opennms.org/juniper/twowaydelaybesthigh	uei.opennms.org/juniper/twowaydelaybestrearm	Edit	Delete	
high	TwoWayDelay Worst	JnxUtilInteger Name	TwoWayDelay Worst	100.0	0.0	2	uei.opennms.org/juniper/twowaydelayworsthigh	uei.opennms.org/juniper/twowaydelayworstrearm	Edit	Delete	
high	TwoWayDelay Var	JnxUtilInteger Name	TwoWayDelay Var	10.0	0.0	2	uei.opennms.org/juniper/twowaydelayvariationhigh	uei.opennms.org/juniper/twowaydelayvariationrearm	Edit	Delete	
high	OneWayDelay Avg	JnxUtilInteger Name	OneWayDelay Avg	100.0	0.0	2	uei.opennms.org/juniper/onewaydelayavghigh	uei.opennms.org/juniper/onewaydelayavgrearm	Edit	Delete	
high	OneWayDelay Best	JnxUtilInteger Name	OneWayDelay Best	100.0	0.0	2	uei.opennms.org/juniper/onewaydelaybesthigh	uei.opennms.org/juniper/onewaydelaybestrearm	Edit	Delete	
high	OneWayDelay Worst	JnxUtilInteger Name	OneWayDelay Worst	100.0	0.0	2	uei.opennms.org/juniper/onewaydelayworsthigh	uei.opennms.org/juniper/onewaydelayworstrearm	Edit	Delete	
high	OneWayDelay Var	JnxUtilInteger Name	OneWayDelay Var	10.0	0.0	2	uei.opennms.org/juniper/onewaydelayvariationhigh	uei.opennms.org/juniper/onewaydelayvariationrearm	Edit	Delete	
high	FrameLossFEAvg	JnxUtilInteger Name	FrameLossFEAvg	10.0	0.0	2	uei.opennms.org/juniper/framelossfarndavghigh	uei.opennms.org/juniper/framelossfarndavgrearm	Edit	Delete	
high	FrameLossFEBest	JnxUtilInteger Name	FrameLossFEBest	10.0	0.0	2	uei.opennms.org/juniper/framelossfarndbesthigh	uei.opennms.org/juniper/framelossfarndbestrearm	Edit	Delete	
high	FrameLossFEWorst	JnxUtilInteger Name	FrameLossFEWorst	10.0	0.0	2	uei.opennms.org/juniper/framelossfarndworsthigh	uei.opennms.org/juniper/framelossfarndworstrearm	Edit	Delete	
high	FrameLossNEA	JnxUtilInteger Name	FrameLossNEA	10.0	0.0	2	uei.opennms.org/juniper/framelossnear	uei.opennms.org/juniper/framelossnear	Edit	Delete	

4. Click the **Edit** column for the threshold expression you want to modify.

Network Monitoring > Admin

Edit expression threshold

Type	Expression	Datasource type	Datasource label	Value	Re-arm
high	TwoWayDelayVar	Node	TwoWayDelayVar	10.0	0.0
Description	Triggered UEI	Re-armed UEI			
	uei.opennms.org/juniper/twowaydelayvariationhigh	uei.opennms.org/juniper/twowaydelayvariationrearm			

[Save](#) [Cancel](#)

5. Modify the threshold **Expression** and **Re-armed UEI** values according to your requirements.

6. Click **Save**.

RELATED DOCUMENTATION

| [Monitoring Performance Statistics Derived from MIB Objects](#) | 1100

37

CHAPTER

Collection of Log Files

[Downloading the Collection of Cross Provisioning Platform Log Files](#) | **1110**

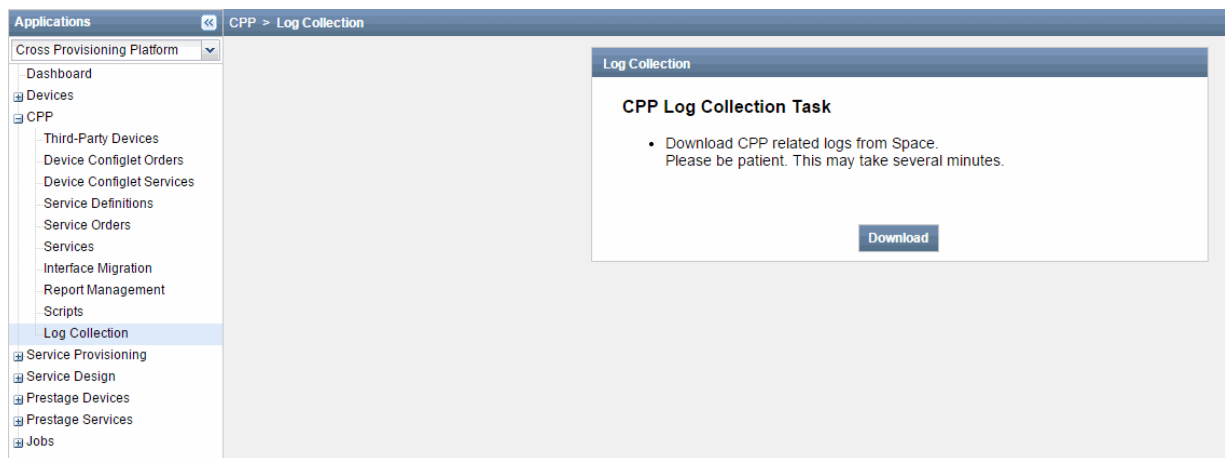
Downloading the Collection of Cross Provisioning Platform Log Files

You can download the collection of Cross Provisioning Platform log files with a single link. The collection of log files is packaged into a single zip file that can be downloaded and saved to your local machine. This feature proves beneficial especially, for troubleshooting purposes.

To download the collection of log files related to Cross Provisioning Platform:

1. In the **Cross Provisioning Platform** task pane, select **CPP > Log Collection**.

The **Log Collection** dialog box that appears the **Download** button.



2. Click the **Download** button.

The **Download Troubleshooting** dialog box that appears shows a progress bar.

NOTE: In a multinode setup, all log files related to different nodes are present in the same zip file. However, they are available within their respective directories along with their specific node names.

3. After the download process is completed, you can save the zip file to your local machine.

The following files are packaged, zipped, and downloaded as part of the collection of log files:

File/Folder	Location (by default)
All Deployment Files under FLEX directory	<p>/var/tmp/jboss/debug/FLEX/*</p> <p>The Application Settings determine the location of the debug folder. You can navigate to ApplicationSettings by selecting Network Management Platform > Administration > Applications > Cross Provisioning Platform > Modify Application Settings > Logging > Log Directory.</p>
OSS log file (includes requests and responses to and from the Service Aware Manager server)	<p>/var/tmp/jboss/oss.log</p> <p>The logger setting specific to the OSS log determines the location of the debug folder.</p>
Server logs	/var/log/jboss/servers/*

The Role-Based Access Control option is provided along with this feature to control access to the collection of log files. For more information about Role-Based Access Control, see the *Junos Space Network Management Platform User Guide*.

38

CHAPTER

Application Settings

[Modifying Application Settings](#) | **1113**

Modifying Application Settings

In Network Management platform, you can modify the configuration settings for the Network Activate application.

To modify the configuration settings of Network Activate, 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** or **Cross Provisioning Platform** 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 respective application or click **Cancel** to retain the original settings.

To understand the parameters of the Network Activate or Cross Provisioning Platform application settings, refer to [Table 45 on page 1113](#).

Table 45: Parameters in Network Activate Application Settings

FIELDS	DESCRIPTION
DEPLOYMENT	
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 Network Activate 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.

Table 45: Parameters in Network Activate Application Settings (*continued*)

FIELDS	DESCRIPTION
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 vlanmaps for flexible tagged services	Select this check box to use vlanmaps for flexible tagged services, instead of normalization. VLAN mapping refers to the swapping of the incoming VLAN ID to a new VLAN ID.
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.
UI	
Allow template modification for service	Select this check box to allow the templates to be changed during the service modification.
Bandwidth Combo Items Count	Specify the bandwidth combo items count. 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. The default value is 100.
MONITORING	

Table 45: Parameters in Network Activate Application Settings (*continued*)

FIELDS	DESCRIPTION
Perform Monitoring on Failed Functional Audit	Select this check box to perform monitoring if the functional audit fails.
Pseudo-wire 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>
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>
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>

Table 45: Parameters in Network Activate 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:10.1.1.1:2. 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>

Table 45: Parameters in Network Activate Application Settings (*continued*)

FIELDS	DESCRIPTION
Enable Performance Monitoring through scripts	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.
OSSCONFIGPARAMETERS	
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.
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	<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>

Table 45: Parameters in Network Activate Application Settings *(continued)*

FIELDS	DESCRIPTION
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.