



M Series and MX Series Device Management with NSM



Published: 2013-01-02

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Copyright © 2013, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, 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.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

M Series and MX Series Device Management with NSM

Copyright © 2013, 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 <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	xxvii
	Documentation and Release Notes	xxvii
	Supported Platforms	xxvii
	Documentation Conventions	xxvii
	Documentation Feedback	xxix
	Requesting Technical Support	xxix
	Self-Help Online Tools and Resources	xxx
	Opening a Case with JTAC	xxx
Part 1	Overview	
Chapter 1	Getting Started	3
	Introduction to Network and Security Manager	3
	Installing NSM	3
	Role-Based Administration	4
Chapter 2	The Junos OS CLI and NSM	5
	NSM and Device Management Overview	5
	Understanding the CLI and NSM	6
	Comparing the CLI To the NSM UI	7
	NSM Services Supported for M Series and MX Series Devices	10
	How NSM Works with the CLI and Distributed Data Collection	11
	Device Schemas	12
	Communication Between a Device and NSM	13
Chapter 3	Before You Begin Adding Devices	15
	M Series and MX Series Devices Supported by NSM	15
	Considering the Device Status	16
	Configuring a Deployed M Series or MX Series Device for Importing to NSM	17
	Configure an IP Address and a User with Full Administrative Privileges for the Device	17
	Check Network Connectivity	18
	Check Connectivity to the NSM Server	18
	Configure a Static Route to the NSM Server	18
	Establish a Telnet or an SSHv2, and a NETCONF protocol over SSH Connection to the NSM Server	20
Part 2	Integration	
Chapter 4	Addition of M Series and MX Series Devices	25
	About Device Creation	25
	Supported Add Device Workflows for M Series and MX Series Devices	26

	Importing Devices Overview	27
	Modeling Devices Overview	28
	Adding Multiple Devices Using Automatic Discovery (Junos OS Devices Only)	29
	Adding Device Groups Overview	29
Chapter 5	M Series and MX Series Devices Update	31
	About Updating M Series and MX Series Devices	31
	How the Update Process Works	32
	Job Manager	33
	Tracking Updated Devices Using Job Manager	34
	Reviewing Job Information Displayed in Job Manager	35
	Device States Displayed in Job Manager During Update	36
	Understanding Updating Errors Displayed in the Job Manager	37
Part 3	Configuration	
Chapter 6	Configuration of M Series and MX Series Devices	43
	About Device Configuration	43
	M Series and MX Series Device Configuration Settings Supported in NSM	44
	Configuring Device Features	46
	Example: Configuration of Interfaces for MPLS in the CLI and NSM	47
Chapter 7	Configuration of Access	49
	Configuring Address-Assignment Pools (NSM Procedure)	49
	Configuring Access Address Pools (NSM Procedure)	52
	Configuring Access Group Profile (NSM Procedure)	53
	Configuring the LDAP Options (NSM Procedure)	54
	Configuring the LDAP Server (NSM Procedure)	55
	Configuring Access Profiles for L2TP or PPP Parameters (NSM Procedure)	56
	Configuring Access Profile (NSM Procedure)	57
	Configuring Accounting Parameters for Access Profiles (NSM Procedure)	57
	Configuring the Accounting Order (NSM Procedure)	58
	Configuring the Authentication Order (NSM Procedure)	59
	Configuring the Authorization Order (NSM Procedure)	59
	Configuring the L2TP Client (NSM Procedure)	60
	Configuring the Client Filter Name (NSM Procedure)	61
	Configuring the LDAP Options (NSM Procedure)	62
	Configuring the LDAP Server (NSM Procedure)	63
	Configuring the Provisioning Order (NSM Procedure)	64
	Configuring RADIUS Parameters for AAA Subscriber Management (NSM Procedure)	65
	Configuring the RADIUS Parameters (NSM Procedure)	68
	Configuring the RADIUS for Subscriber Access Management, L2TP, or PPP (NSM Procedure)	69
	Configuring Session Limit (NSM Procedure)	69
	Configuring the RADIUS Parameters (NSM Procedure)	70
	Configuring the RADIUS for Subscriber Access Management, L2TP, or PPP (NSM Procedure)	71

	Configuring the SecurID Server (NSM Procedure)	72
	Configuring the Access Profile (NSM Procedure)	73
Chapter 8	Configuration of Accounting Options	75
	Configuring Accounting Options (NSM Procedure)	75
	Configuring Class Usage Profiles (NSM Procedure)	75
	Configuring a Log File (NSM Procedure)	76
	Configuring the Filter Profile (NSM Procedure)	77
	Configuring the Interface Profile (NSM Procedure)	78
	Configuring the Policy Decision Statistics Profile (NSM Procedure)	79
	Configuring the MIB Profile (NSM Procedure)	80
	Configuring the Routing Engine Profile (NSM Procedure)	81
Chapter 9	Configuration of Application	83
	Configuring the Application and Application Set (NSM Procedure)	83
Chapter 10	Configuration of Bridge Domains	85
	Configuring Bridge Domains Properties (NSM Procedure)	85
	Configuring Logical Interfaces (NSM Procedure)	85
	Configuring Multicast Monitoring Options (NSM Procedure)	86
	Configuring VLAN ID (NSM Procedure)	89
Chapter 11	Configuration of Chassis	91
	Configuring Aggregated Devices (NSM Procedure)	91
	Configuring Chassis Alarms (NSM Procedure)	92
	Configuring Container Interfaces (NSM Procedure)	93
	Configuring Chassis FPC (NSM Procedure)	94
	Configuring a T640 Router on a Routing Matrix (NSM Procedure)	99
	Configuring Routing Engine Redundancy (NSM Procedure)	104
	Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors (NSM Procedure)	105
Chapter 12	Configuration of User Authentication	107
	Configuring RADIUS Authentication (NSM Procedure)	107
	Configuring TACACS+ Authentication (NSM Procedure)	108
	Configuring Authentication Order (NSM Procedure)	109
	Configuring User Access (NSM Procedure)	110
	Configuring Login Classes	110
	Configuring User Accounts	112
	Configuring Template Accounts (NSM Procedure)	113
	Creating a Remote Template Account	114
	Creating a Local Template Account	115
Chapter 13	Configuration of Class of Service Features	117
	Configuring CoS Classifiers (NSM Procedure)	118
	Configuring CoS Code Point Aliases (NSM Procedure)	120
	Configuring CoS Drop Profile (NSM Procedure)	121
	Configuring CoS Forwarding Classes (NSM Procedure)	123
	Configuring CoS Forwarding Policy (NSM Procedure)	125
	Configuring CoS Fragmentation Maps (NSM Procedure)	126
	Configuring CoS Host Outbound Traffic (NSM Procedure)	127

	Configuring CoS Interfaces (NSM Procedure)	128
	Configuring CoS Rewrite Rules (NSM Procedure)	134
	Configuring CoS Routing Instances (NSM Procedure)	137
	Configuring CoS Schedulers (NSM Procedure)	138
	Configuring CoS and Applying Scheduler Maps (NSM Procedure)	140
	Configuring CoS Restricted Queues (NSM Procedure)	141
	Configuring Tracing Operations (NSM Procedure)	142
	Configuring CoS Traffic Control Profiles (NSM Procedure)	143
	Configuring CoS Translation Table (NSM Procedure)	144
Chapter 14	Configuration of Event Options	149
	Configuring Destinations for File Archiving (NSM Procedure)	149
	Configuring Event Script (NSM Procedure)	150
	Generating Internal Events (NSM Procedure)	152
	Configuring Event Policy (NSM Procedure)	152
	Configuring Event Policy Tracing Operations (NSM Procedure)	155
Chapter 15	Configuration of Firewall	157
	Configuring the Firewall Filter for Any Family Type (NSM Procedure)	157
	Configuring the Firewall Filter for Bridge Family Type (NSM Procedure)	159
	Configuring the Firewall Filter for Ccc Family Type (NSM Procedure)	161
	Configuring Filters for inet Family Type (NSM Procedure)	163
	Configuring Firewall Filter for inet Family Type (NSM Procedure)	163
	Configuring Prefix-specific Actions (NSM Procedure)	165
	Configuring Service Filters (NSM Procedure)	166
	Configuring Simple Filters (NSM Procedure)	167
	Configuring Filters for inet6 Family Type (NSM Procedure)	168
	Configuring Firewall Filter for inet6 Family Type (NSM Procedure)	169
	Configuring Service Filters for inet6 (NSM Procedure)	171
	Configuring the Firewall Filter for MPLS Family Type (NSM Procedure)	172
	Configuring the Firewall Filter for VPLS Family Type (NSM Procedure)	175
	Configuring a Policier for a Firewall Filter	178
Chapter 16	Configuration of Forwarding Options	181
	Configuring Accounting Options (NSM Procedure)	181
	Configuring the Extended DHCP Agent (NSM Procedure)	183
	Configuring Authentication Support for the DHCP Relay Agent (NSM Procedure)	183
	Configuring Group (NSM Procedure)	184
	Overriding the Default Configuration Settings for the Extended DHCP Relay Agent (NSM Procedure)	185
	Configuring Relay Option 60 Information for Forwarding Client Traffic to Specific DHCP Servers (NSM Procedure)	187
	Configuring Relay Option 82 for a DHCP Server (NSM Procedure)	188
	Specifying the Name of a Group of DHCP Server Addresses for Use by the Extended DHCP Relay Agent (NSM Procedure)	189
	Configuring Operations for Extended DHCP Relay Agent Processes (NSM Procedure)	190
	Specifying Address Family for Filters (NSM Procedure)	191

	Configuring Load Balancing Using Hash Key (NSM Procedure)	192
	Configuring Helpers (NSM Procedure)	193
	Configuring a Router or Interface to Act as a Bootstrap Protocol Relay Agent	194
	Enabling DNS Request Packet Forwarding	197
	Configuring a Port for a DHCP or BOOTP Relay Agent	199
	Configuring Tracing Operations for BOOTP, DNS, and TFTP Packet Forwarding	201
	Configuring Per-Flow and Per-Prefix Load Balancing (NSM Procedure)	202
	Configuring Port Mirroring (NSM Procedure)	203
Chapter 17	Configuration of Interfaces	207
	Configuring Interfaces on the Routing Platform (NSM Procedure)	207
	Configuring Interface Properties (NSM Procedure)	207
	Damping Interface Transitions (NSM Procedure)	209
	Configuring Receive Bucket Properties on Interfaces (NSM Procedure)	210
	Configuring Tracing Operations of an Individual Router Interface (NSM Procedure)	210
	Configuring Transmit Leaky Bucket Properties (NSM Procedure)	211
	Configuring Logical Interface Properties (NSM Procedure)	212
	Configuring Logical Unit Properties (NSM Procedure)	212
	Configuring an IP Demux Underlying Interface (NSM Procedure)	213
	Configuring the Logical Demux Source Family Type on the IP Demux Underlying Interface (NSM Procedure)	214
	Configuring Epd Threshold for the Logical Interface (NSM Procedure)	214
	Configuring Protocol Family Information for the Logical Interface (NSM Procedure)	215
	Configuring Protocol Family (Ccc) Information for the Logical Interface (NSM Procedure)	216
	Configuring Protocol Family (Inet) Information for the Logical Interface (NSM Procedure)	217
	Configuring Protocol Family (Inet6) Information for the Logical Interface (NSM Procedure)	223
	Configuring Protocol Family (ISO) Information for the Logical Interface (NSM Procedure)	230
	Configuring Protocol Family (MPLS) Information for the Logical Interface (NSM Procedure)	231
	Configuring Protocol Family (TCC) Information for the Logical Interface (NSM Procedure)	233
	Configuring the Traffic Shaping Profile (NSM Procedure)	233
	Configuring Interface set on the Routing Platform (NSM Procedure)	235
	Configuring Trace Options on the Routing Platform (NSM Procedure)	236
Chapter 18	Configuration of Multicast Snooping Options	239
	Configuring Multicast Monitoring Options (NSM Procedure)	239
Chapter 19	Configuration of Policy Options	243
	Configuring an AS Path in a BGP Routing Policy (NSM Procedure)	243
	Configuring an AS Path Group in a BGP Routing Policy (NSM Procedure)	244

Chapter 20

Configuring a Community for use in BGP Routing Policy Conditions (NSM Procedure)	245
Configuring a BGP Export Policy Condition (NSM Procedure)	246
Configuring Flap Damping to Reduce the Number of BGP Update Messages(NSM Procedure)	247
Configuring a Routing Policy Statement (NSM Procedure)	249
Configuring Prefix List (NSM Procedure)	250
Configuration of Protocols	253
Configuring the BFD Protocol (NSM Procedure)	253
Configuring BGP (NSM Procedure)	254
Configuring the ILMI Protocol (NSM Procedure)	257
Configuring Layer 2 Address Learning and Forwarding Properties (NSM Procedure)	258
Configuring Layer 2 Circuit (NSM Procedure)	259
Configuring Local Interface Switching (NSM Procedure)	259
Configuring the Neighbor Interface for the Layer 2 Circuit (NSM Procedure)	260
Tracing Layer 2 Circuit Creation and Changes (NSM Procedure)	264
Configuring Layer 2 Protocol Tunneling and BPDU Protection (NSM Procedure)	265
Configuring Label Distribution Protocol (NSM Procedure)	267
Configuring Link Management Protocol (NSM Procedure)	278
Configuring MPLS Protocol (NSM Procedure)	282
Enabling MPLS on the Router (NSM Procedure)	282
Configuring Administrative Group (NSM Procedure)	285
Configuring Administrative Groups (NSM Procedure)	285
Configuring Bandwidth for the Reroute Path (NSM Procedure)	286
Configuring DiffServ-Aware Traffic Engineering (NSM Procedure)	287
Configuring MPLS on Interfaces (NSM Procedure)	288
Configure a Label Switched Path (LSP) to Use in Dynamic MPLS	290
Configuring Label Switched Path (NSM Procedure)	290
Configuring Administrative Group (NSM Procedure)	293
Configuring Automatic Bandwidth Allocation for LSPs (NSM Procedure)	294
Configuring Bandwidth for the Reroute Path (NSM Procedure)	295
Configuring Fast Reroute (NSM Procedure)	296
Adding LSP-Related Routes to the inet.3 Routing Table (NSM Procedure)	297
Configuring MPLS LSPs for GMPLS (NSM Procedure)	298
Configuring BFD for MPLS IPv4 LSPs (NSM Procedure)	299
Configuring the Primary Point-to-Multipoint LSP (NSM Procedure)	301
Configuring Policers for LSPs (NSM Procedure)	302
Configuring Primary Paths for an LSP (NSM Procedure)	303
Configuring Secondary Paths for an LSP (NSM Procedure)	308
Configuring System Log Messages and SNMP Traps for LSPs (NSM Procedure)	316
Configuring BFD for MPLS IPv4 LSPs (NSM Procedure)	317
Configuring Named Paths (NSM Procedure)	319

Configuring MTU Signaling in RSVPs (NSM Procedure)	320
Configuring static LSPs on the Ingress Router (NSM Procedure)	321
Configuring MPLS Statistics (NSM Procedure)	322
Tracing MPLS Packets and Operations (NSM Procedure)	323
Configuring MSDP Protocol (NSM Procedure)	324
Configuring MSDP on the Router (NSM Procedure)	324
Configuring the MSDP Active Source Limit (NSM Procedure)	325
Configuring Export Policy (NSM Procedure)	326
Configuring MSDP Peer Group	327
Configuring MSDP Peer Group (NSM Procedure)	327
Configuring MSDP Peers (NSM Procedure)	328
Configuring a Routing Table Group with MSDP (NSM Procedure)	330
Configuring Per-Source Active Source Limit (NSM Procedure)	331
Configuring MSDP Traceoptions (NSM Procedure)	332
Configuring MSTP (NSM Procedure)	332
Configuring OSPF (NSM Procedure)	334
Configuring RIP (NSM Procedure)	338
Configuring RIPng Protocol (NSM Procedure)	340
Configuring RIPng on the Router (NSM Procedure)	340
Configuring Graceful Restart for RIPng (NSM Procedure)	341
Configuring Group	342
Configuring Group-Specific RIPng Properties (NSM Procedure)	342
Applying Policies to Routes Exported by RIPng (NSM Procedure)	344
Applying Policies to Routes Imported by RIPng (NSM Procedure)	344
Configuring RIPng Neighbor Properties	345
Enable or Disable Receiving of Update Messages (NSM Procedure)	348
Configuring RIPng Send Update Messages (NSM Procedure)	348
Configuring RIPng Traceoptions (NSM Procedure)	349
Configuring Router Advertisement (NSM Procedure)	350
Configuring ICMP Router Discovery (NSM Procedure)	352
Configuring VRRP (NSM Procedure)	355
Configuring VSTP (NSM Procedure)	356
Configuring RSVP (NSM Procedure)	358
Chapter 21 Configuration of Routing Options	365
Configuring Confederation (NSM Procedure)	366
Configuring Dynamic Tunnels (NSM Procedure)	367
Configuring Fate Sharing (NSM Procedure)	368
Configuring Flow Route (NSM Procedure)	370
Configuring Forwarding Table (NSM Procedure)	372
Configuring Generated Routes (NSM Procedure)	373
Configuring Instance Export (NSM Procedure)	374
Configuring Instance Import (NSM Procedure)	375
Configuring Interface Routes (NSM Procedure)	376
Configuring Martian Addresses (NSM Procedure)	377
Configuring Maximum Paths (NSM Procedure)	378
Configuring Maximum Prefixes (NSM Procedure)	379
Configuring Multicast (NSM Procedure)	381
Configuring Options (NSM Procedure)	384

	Configuring Routing Tables (NSM Procedure)	385
	Configuring Routing Table Groups (NSM Procedure)	387
	Configuring Source Routing (NSM Procedure)	388
	Configuring Static Routes (NSM Procedure)	389
	Configuring Traceoptions (NSM Procedure)	390
	Configuring Topologies (NSM Procedure)	391
Chapter 22	Configuration of Security	393
	Configuring Topologies (NSM Procedure)	393
	Configuring Certificates (NSM Procedure)	394
	Configuring Certification Authority (NSM Procedure)	395
	Configuring the Local Certificate (NSM Procedure)	396
	Configuring Firewall Authentication (NSM Procedure)	396
	Configuring Pass-Through	397
	Configuring Traceoptions	398
	Configuring Web Authentication	399
	Configuring a Flow (NSM Procedure)	399
	Configuring a Bridge (NSM Procedure)	400
	Configuring the TCP MSS Option (NSM Procedure)	401
	Configuring the TCP Session Option (NSM Procedure)	402
	Configuring Traceoptions (NSM Procedure)	403
	Configuring File Options (NSM Procedure)	404
	Configuring Flag Options (NSM Procedure)	405
	Configuring Packet Filter Options (NSM Procedure)	405
	Configuring Forwarding Options (NSM Procedure)	406
	Configuring IKE (NSM Procedure)	407
	Configuring a Gateway (NSM Procedure)	408
	Configuring a Policy (NSM Procedure)	410
	Configuring a Respond Bad SPI (NSM Procedure)	412
	Configuring Traceoptions (NSM Procedure)	412
	Configuring the File Options (NSM Procedure)	413
	Configuring Flag Options (NSM Procedure)	414
	Configuring IPsec (NSM Procedure)	414
	Configuring a Policy (NSM Procedure)	415
	Configuring Traceoptions (NSM Procedure)	416
	Configuring a VPN (NSM Procedure)	416
	Configuring VPN Monitor Options (NSM Procedure)	419
	Configuring a PKI (NSM Procedure)	420
	Configuring Auto Re-enrollment (NSM Procedure)	420
	Configuring a CA Profile (NSM Procedure)	421
	Configuring Traceoptions (NSM Procedure)	423
	Configuring the File Options (NSM Procedure)	424
	Configuring Flag Options (NSM Procedure)	424
Chapter 23	Configuration of Services	427
	Configuring Adaptive Services PICs (NSM Procedure)	427
	Configuring Border Signaling Gateways (NSM Procedure)	428
	Configuring Gateway Properties (NSM Procedure)	428
	Configuring Gateway (NSM Procedure)	429
	Configuring an Admission Controller (NSM Procedure)	429

Configuring Session Policy Decision Function (NSM Procedure)	430
Configuring Service Point (NSM Procedure)	432
Configuring SIP Policies and Timers (NSM Procedure)	433
Configuring Traceoptions (NSM Procedure)	443
Configuring Class of Service (NSM Procedure)	447
Configuring Intrusion Detection Service (NSM Procedure)	450
Tracing Services PIC Operations (NSM Procedure)	454
Configuring Network Address Translation (NSM Procedure)	455
Configuring PGCP (NSM Procedure)	460
Configuring Gateway (NSM Procedure)	461
Configuring a Virtual Border Gateway Function on the Router (NSM Procedure)	461
Configuring Data Inactivity Detection (NSM Procedure)	462
Configuring Gateway Controller (NSM Procedure)	463
Configuring Graceful Restart (NSM Procedure)	464
Configuring H248 Options Properties (NSM Procedure)	465
Configuring H248 Options (NSM Procedure)	465
Changing Encoding Defaults (NSM Procedure)	466
Configuring Service Change (NSM Procedure)	466
Configuring H248 Properties (NSM Procedure)	471
Configuring Application Data Inactivity Detection (NSM Procedure)	472
Configuring Base Root (NSM Procedure)	472
Configuring Differentiated Services (NSM Procedure)	475
Configuring Event Timestamp Notification (NSM Procedure)	475
Hanging Termination Detection (NSM Procedure)	476
Configuring Inactivity Timer (NSM Procedure)	477
Configuring Notification Behavior (NSM Procedure)	478
Configuring Segmentation (NSM Procedure)	479
Configuring Traffic Management (NSM Procedure)	480
Configuring H248 Timers (NSM Procedure)	482
Configuring the Monitor (NSM Procedure)	483
Configuring Overload Control (NSM Procedure)	484
Configuring Session Mirroring (NSM Procedure)	485
Configuring Media Service (NSM Procedure)	485
Configuring a Rule (NSM Procedure)	486
Configuring Rule Set (NSM Procedure)	487
Configuring Session Mirroring (NSM Procedure)	487
Configuring Traceoptions (NSM Procedure)	488
Configuring Virtual Interface (NSM Procedure)	489
Configuring Service Interface Pools (NSM Procedure)	490
Configuring Stateful Firewall (NSM Procedure)	491
Configuring a Service Set (NSM Procedure)	493
Configuring Captive Portal (NSM Procedure)	497
Configuring Custom Options (NSM Procedure)	498
Configuring the Interface (NSM Procedure)	499
Configuring Traceoptions (NSM Procedure)	500
Configuring File Options (NSM Procedure)	500
Configuring Flag Options (NSM Procedure)	501

	Configuring Mobile IP (NSM Procedure)	502
	Configuring Access Type (NSM Procedure)	502
	Configuring the Authenticate Mechanism (NSM Procedure)	503
	Configuring Dynamic Home Assignment (NSM Procedure)	504
	Configuring the Home Agent (NSM Procedure)	505
	Configuring Enable Service (NSM Procedure)	505
	Configuring Pool Match Order (NSM Procedure)	506
	Configuring the Virtual Network (NSM Procedure)	506
	Configuring the Peer (NSM Procedure)	507
	Configuring Traceoptions (NSM Procedure)	510
	Configuring File (NSM Procedure)	511
	Configuring Flag (NSM Procedure)	512
	Configuring RPM (NSM Procedure)	513
	Configuring BGP (NSM Procedure)	513
	Configuring Routing Instances (NSM Procedure)	514
	Configuring Probe (NSM Procedure)	515
	Configuring Probe Server (NSM Procedure)	518
	Configuring Unified Access Control (NSM Procedure)	519
	Configuring Infranet Controller (NSM Procedure)	520
	Configuring Traceoptions (NSM Procedure)	521
Chapter 24	Configuration of SNMP for Network Management	523
	Configuring Basic System Identification for SNMP (NSM Procedure)	523
	Configuring SNMP Communities (NSM Procedure)	524
	Configuring SNMP Trap Groups (NSM Procedure)	526
	Configuring SNMP Views (NSM Procedure)	528
Chapter 25	Configuration of System	531
	Configuring Accounting (NSM Procedure)	531
	Configuring Destination	532
	Configuring Events	534
	Configuring Traceoptions	534
	Configuring Archival (NSM Procedure)	535
	Configuring ARP (NSM Procedure)	536
	Configuring Auto Configuration (NSM Procedure)	537
	Configuring a Backup Router (NSM Procedure)	539
	Configuring a Commit (NSM Procedure)	540
	Configuring Diag Port Authentication (NSM Procedure)	540
	Configuring a Domain Search (NSM Procedure)	541
	Configuring Extensions (NSM Procedure)	541
	Configuring Providers	542
	Configuring Resource Limits	542
	Configuring an Inet6 Backup Router (NSM Procedure)	544
	Configuring Internet Options (NSM Procedure)	545
	Configuring Location (NSM Procedure)	548
	Configuring Login (NSM Procedure)	549
	Configuring Class	550
	Configuring Password	551
	Configuring Retry Options	552
	Configuring User	553

	Configuring a Name Server (NSM Procedure)	554
	Configuring PIC Console Authentication (NSM Procedure)	555
	Configuring Ports (NSM Procedure)	555
	Configuring RADIUS Options (NSM Procedure)	556
	Configuring RADIUS Server (NSM Procedure)	557
	Configuring Root Authentication (NSM Procedure)	558
	Configuring Static Host Mapping (NSM Procedure)	559
	Configuring TACACS+ Options (NSM Procedure)	560
	Configuring TACACS+ Server (NSM Procedure)	561
Part 4	Management	
Chapter 26	Management of M Series and MX Series Devices	565
	Managing M Series and MX Series Device Software Versions	565
Chapter 27	Device Inventory in NSM and the CLI	567
	Viewing and Reconciling Device Inventory	567
	Comparing Device Inventory in NSM and the CLI	568
	Viewing Device Inventory in NSM	568
	Viewing Device Inventory from the CLI	570
Chapter 28	Topology Manager	573
	Overview of the NSM Topology Manager	573
	Requisites for a Topology Discovery	573
	About the NSM Topology Manager Toolbar	574
Part 5	Monitor	
Chapter 29	Real Time Monitor	579
	About the Realtime Monitor	579
	Viewing Device Status	579
	Viewing Device Monitor Alarm Status	582
	Setting the Polling Interval For Device Alarm Status	583
Part 6	Index	
	Index	587

List of Figures

Part 1	Overview	
Chapter 2	The Junos OS CLI and NSM	5
	Figure 1: Overview of the User Interface	8
	Figure 2: NSM Network Architecture	12
Part 2	Integration	
Chapter 5	M Series and MX Series Devices Update	31
	Figure 3: Job Information Dialog Box	35
	Figure 4: Failed Update Job Information Dialog Box	38
Part 3	Configuration	
Chapter 6	Configuration of M Series and MX Series Devices	43
	Figure 5: MPLS Configuration in the CLI	47
	Figure 6: MPLS Configuration in NSM	48
Part 4	Management	
Chapter 27	Device Inventory in NSM and the CLI	567
	Figure 7: The Device Inventory Window	568
	Figure 8: Viewing the Hardware Inventory	569
	Figure 9: Viewing the Software Inventory	569

List of Tables

	About the Documentation	xxvii
	Table 1: Notice Icons	xxviii
	Table 2: Text and Syntax Conventions	xxviii
Part 1	Overview	
Chapter 3	Before You Begin Adding Devices	15
	Table 3: M Series Multiservice Edge Routers and MX Series Ethernet Services Routers	15
Part 2	Integration	
Chapter 5	M Series and MX Series Devices Update	31
	Table 4: Device States During Update	36
Part 3	Configuration	
Chapter 6	Configuration of M Series and MX Series Devices	43
	Table 5: The Junos OS Configuration Hierarchy and the NSM Configuration Tree	44
Chapter 7	Configuration of Access	49
	Table 6: Address Assignment Configuration Details	50
	Table 7: Access Address Pool Configuration Details	53
	Table 8: Access Group Profile Configuration Details	53
	Table 9: LDAP Options Configuration Details	55
	Table 10: LDAP Server Configuration Details	56
	Table 11: Access Profile Properties Configuration Details	57
	Table 12: Accounting Parameter Configuration Details	58
	Table 13: Accounting Order Configuration Details	59
	Table 14: Authentication Order Configuration Details	59
	Table 15: Authorization Order Configuration Details	60
	Table 16: Client Configuration Details	60
	Table 17: Client Filter Name Configuration Details	62
	Table 18: LDAP Options Configuration Details	62
	Table 19: LDAP Server Configuration Details	64
	Table 20: Provisioning Order Configuration Details	64
	Table 21: RADIUS Parameter Configuration Details	65
	Table 22: RADIUS Parameters Configuration Details	68
	Table 23: RADIUS Server Configuration Details	69
	Table 24: Session Limit Configuration Details	70
	Table 25: RADIUS Parameters Configuration Details	71

	Table 26: RADIUS Server Configuration Details	72
	Table 27: SecurID Server Configuration Details	73
	Table 28: Access Profile Configuration Details	73
Chapter 8	Configuration of Accounting Options	75
	Table 29: Class Usage Profile Configuration Details	76
	Table 30: Log File Configuration Details	77
	Table 31: Filter Profile Configuration Details	78
	Table 32: Interface Profile Configuration Details	79
	Table 33: Policy Decision Statistics Profile Configuration Details	80
	Table 34: MIB Profile Configuration Details	81
	Table 35: Routing Engine Profile Configuration Details	82
Chapter 9	Configuration of Application	83
	Table 36: Applications Configuration Details	84
Chapter 10	Configuration of Bridge Domains	85
	Table 37: Logical Interface Configuration Details	86
	Table 38: Multicast Monitoring Options Configuration Details	87
	Table 39: VLAN ID Configuration Details	89
Chapter 11	Configuration of Chassis	91
	Table 40: Aggregated Devices Configuration Details	92
	Table 41: Chassis Alarms Configuration Details	93
	Table 42: Container Interfaces Configuration Details	93
	Table 43: FPC Configuration Details	94
	Table 44: Lcc Configuration Details	99
	Table 45: Chassis Redundancy Configuration Details	104
	Table 46: Chassis Routing Engine Configuration Details	105
Chapter 12	Configuration of User Authentication	107
	Table 47: RADIUS Authentication Configuration Details	107
	Table 48: TACACS+ Authentication Configuration Details	108
	Table 49: Login Class Authentication Configuration Details	110
	Table 50: User Authentication Configuration Details	112
	Table 51: Remote Template Account Details	114
	Table 52: Local Template Account Details	115
Chapter 13	Configuration of Class of Service Features	117
	Table 53: Configuring and Applying Behavior Aggregate Classifiers	118
	Table 54: Configuring Code Point Aliases	121
	Table 55: Drop Profile Configuration Fields	122
	Table 56: Assigning Forwarding Classes to Output Queues	124
	Table 57: Forwarding Policy Configuration Details	125
	Table 58: Fragmentation Maps Configuration Details	127
	Table 59: Host Outbound Traffic Configuration Details	128
	Table 60: Interfaces Configuration Fields	129
	Table 61: Configuring and Applying Rewrite Rules	134
	Table 62: Routing Instances Configuration Details	137
	Table 63: Configuring Schedulers	139
	Table 64: Assigning Forwarding Classes to Output Queues	140

	Table 65: Restricted Queue Configuration Details	142
	Table 66: Traceoptions Configuration Details	142
	Table 67: Traffic Control profile Configuration Details	144
	Table 68: Translation Table Configuration Details	145
Chapter 14	Configuration of Event Options	149
	Table 69: Destination Configuration Details	149
	Table 70: Event Script Configuration Details	151
	Table 71: Generate Event Details	152
	Table 72: Configure Event Policy Details	153
	Table 73: Event Options Traceoptions Configuration Details	156
Chapter 15	Configuration of Firewall	157
	Table 74: Firewall Filter Configuration Details	158
	Table 75: Bridge Filter Configuration Details	159
	Table 76: Ccc Filter Configuration Details	161
	Table 77: Firewall Filter Configuration Details	163
	Table 78: Prefix Actions Details	166
	Table 79: Service Filter Configuration Details	166
	Table 80: Simple Filter Details	168
	Table 81: Inet6 Firewall Filter Configuration Details	169
	Table 82: inet6 Service Filter Configuration Details	171
	Table 83: MPLS Firewall Filter Configuration Details	173
	Table 84: VPLS Firewall Filter Configuration Details	176
	Table 85: Configuring a Policar for a Firewall Filter	178
Chapter 16	Configuration of Forwarding Options	181
	Table 86: Accounting Options Configuration Details	181
	Table 87: Authentication Configuration Details	184
	Table 88: Group Configuration Details	185
	Table 89: Overrides Configuration Details	186
	Table 90: Relay Option 60 Configuration Details	187
	Table 91: Relay option 82 Configuration Details	189
	Table 92: Sever Group Configuration Details	190
	Table 93: DHCP Relay Traceoptions Configuration Details	190
	Table 94: Address Family Details	191
	Table 95: Load Balance Configuration Details	193
	Table 96: BOOTP Configuration Details	194
	Table 97: DNS and TFTP Configuration Details	199
	Table 98: Port Configuration Details	200
	Table 99: Traceoptions Configuration Details	201
	Table 100: Load Balancing Configuration Details	202
	Table 101: Port Mirroring Configuration Details	204
Chapter 17	Configuration of Interfaces	207
	Table 102: Interface Properties Configuration Details	208
	Table 103: Hold Time Configuration Details	209
	Table 104: Receive Bucket Configuration Details	210
	Table 105: Trace Options Configuration Details	211
	Table 106: Transmit Bucket Configuration Details	212

	Table 107: Logical Unit Configuration Details	213
	Table 108: IP Demux Configuration Details	214
	Table 109: IP Demux Source Configuration Details	214
	Table 110: Epd Threshold Configuration Details	215
	Table 111: Ccc Family Configuration Details	216
	Table 112: Inet Family Configuration Details	218
	Table 113: Inet6 Family Configuration Details	224
	Table 114: Iso Family Configuration Details	231
	Table 115: MPLS Family Configuration Details	232
	Table 116: TCC Family Configuration Details	233
	Table 117: Traffic Shaping Configuration Details	234
	Table 118: Interface Set Configuration Details	235
	Table 119: Traceoption Configuration Details	236
Chapter 18	Configuration of Multicast Snooping Options	239
	Table 120: Multicast Monitoring Options Configuration Details	240
Chapter 19	Configuration of Policy Options	243
	Table 121: AS Path Configuration Details	244
	Table 122: AS Path Group Configuration Details	245
	Table 123: Community Configuration Details	246
	Table 124: Condition Configuration Details	247
	Table 125: Damping Configuration Details	248
	Table 126: Configuring Policy Statement Fields	249
	Table 127: Configuring Prefix List Fields	251
Chapter 20	Configuration of Protocols	253
	Table 128: Configuring Bfd Fields	254
	Table 129: BGP Configuration Fields	255
	Table 130: Trace Options Configuration Details	257
	Table 131: L2 Learning Configuration Details	259
	Table 132: Local Switching Configuration Details	260
	Table 133: Neighbor Interface Configuration Details	261
	Table 134: Layer2 Circuit Traceoption Configuration Details	264
	Table 135: Layer2 Circuit Configuration Details	265
	Table 136: LDP Configuration Details	268
	Table 137: Link Management Protocol Configuration Details	279
	Table 138: MPLS Configuration Details	283
	Table 139: Administrative Group Configuration Details	285
	Table 140: Administrative Groups Configuration Details	286
	Table 141: Automatic Policers Configuration Details	287
	Table 142: DiffServ-Aware Traffic Engineering Configuration Details	288
	Table 143: Interface Configuration Details	289
	Table 144: LSP Configuration Details	291
	Table 145: Administrative Group Configuration Details	294
	Table 146: Automatic Bandwidth Configuration Details	295
	Table 147: Bandwidth Configuration Details	296
	Table 148: Fast Reroute Configuration Details	296
	Table 149: Install Configuration Details	298
	Table 150: Lsp Attributes Configuration Details	299

Table 151: Oam Configuration Details	300
Table 152: Point-to-Multipoint Configuration Details	302
Table 153: Policer Configuration Details	302
Table 154: Primary Paths Configuration Details	303
Table 155: Administrative Group Configuration Details	305
Table 156: Bandwidth Configuration Details	306
Table 157: Oam Configuration Details	306
Table 158: Secondary Paths Configuration Details	309
Table 159: Administrative Group Configuration Details	311
Table 160: Bandwidth Configuration Details	312
Table 161: Oam Configuration Details	312
Table 162: Egress Router Address Configuration Details	315
Table 163: LSP Traceoptions Configuration Details	315
Table 164: Log Updown Configuration Details	316
Table 165: Oam Configuration Details	317
Table 166: Named Path Configuration Details	320
Table 167: Path MTU Configuration Details	320
Table 168: Static Path Configuration Details	321
Table 169: MPLS Statistics Configuration Details	323
Table 170: Traceoptions Configuration Details	324
Table 171: MSDP Configuration Details	325
Table 172: Active Source Limit Configuration Details	326
Table 173: Export Policy Configuration Details	326
Table 174: Peer Group Configuration Details	327
Table 175: MSDP Peer Configuration Details	329
Table 176: Rib Group Configuration Details	331
Table 177: Active Source Limit Configuration Details	331
Table 178: MSDP Traceoption Configuration Details	332
Table 179: MSTP Configuration Fields	333
Table 180: OSPF Configuration Fields	335
Table 181: RIP Configuration Fields	338
Table 182: RIPng Configuration Details	341
Table 183: Graceful Restart Configuration Details	342
Table 184: Group Configuration Details	343
Table 185: RIPng Export Policy Configuration Details	344
Table 186: Import Policy Configuration Details	345
Table 187: Neighbor Properties Configuration Details	346
Table 188: Import Policy Configuration Details	346
Table 189: Receive Message Update Configuration Details	347
Table 190: Send Update Message Configuration Details	348
Table 191: Receive Message Update Configuration Details	348
Table 192: RIPng Send Configuration Details	349
Table 193: RIPng Traceoption Configuration Details	350
Table 194: Router Advertisement Configuration Details	351
Table 195: Router Discovery Configuration Details	353
Table 196: VRRP Configuration Fields	355
Table 197: VSTP Configuration Fields	357
Table 198: RSVP Configuration Details	358

Chapter 21

Configuration of Routing Options 365

	Table 199: Confederation Fields	366
	Table 200: Dynamic Tunnels Configuration Details	367
	Table 201: Fate Sharing Fields	369
	Table 202: Flow Route Fields	371
	Table 203: Forwarding Table Fields	373
	Table 204: Generated Routes Fields	374
	Table 205: Interface Routes Fields	376
	Table 206: Configuring Martian Address Fields	378
	Table 207: Configuring Maximum Paths Fields	379
	Table 208: Configuring Maximum Prefixes Fields	380
	Table 209: Configuring Multicast Fields	381
	Table 210: Configuring Options Fields	385
	Table 211: Rib Fields	386
	Table 212: Rib Group Fields	388
	Table 213: Source Routing Fields	389
	Table 214: Static Fields	390
	Table 215: Traceoption Fields	391
	Table 216: Topology Configuration Details	392
Chapter 22	Configuration of Security	393
	Table 217: Topology Configuration Details	394
	Table 218: Certificates Configuration Details	394
	Table 219: Certification Authority Configuration Details	395
	Table 220: Local Configuration Details	396
	Table 221: Pass-Through Configuration Details	397
	Table 222: Traceoptions Configuration Details	398
	Table 223: Web Authentication Configuration Details	399
	Table 224: Flow Configuration Details	400
	Table 225: Bridge Configuration Details	401
	Table 226: TCP MSS Configuration Details	401
	Table 227: TCP Session Configuration Details	403
	Table 228: Traceoptions Configuration Details	404
	Table 229: File Configuration Details	404
	Table 230: Flag Configuration Details	405
	Table 231: Packet Filter Configuration Details	406
	Table 232: Forwarding Options Configuration Details	407
	Table 233: Gateway Configuration Details	408
	Table 234: Policy Configuration Details	410
	Table 235: Respond Bad SPI Configuration Details	412
	Table 236: Traceoptions Configuration Details	413
	Table 237: File Configuration Details	413
	Table 238: Flag Configuration Details	414
	Table 239: Policy Configuration Details	415
	Table 240: Traceoptions Configuration Details	416
	Table 241: VPN Configuration Details	417
	Table 242: VPN Monitor Options Configuration Details	419
	Table 243: Auto Re-enrollment Configuration Details	421
	Table 244: CA Profile Configuration Details	421
	Table 245: Traceoptions Configuration Details	423

Chapter 23

Table 246: File Configuration Details	424
Table 247: Flag Configuration Details	425
Configuration of Services	427
Table 248: Adaptive Services Pics Configuration Details	428
Table 249: Gateway Configuration Details	429
Table 250: Admission Controller Configuration Details	430
Table 251: Session Policy Decision Configuration Details	431
Table 252: Service Point Configuration Details	433
Table 253: Message Manipulate Rules Configuration Details	434
Table 254: New Call Usage Policy Configuration Details	436
Table 255: New Call Usage Policy Set Configuration Details	439
Table 256: Transaction Policy Configuration Details	440
Table 257: Transaction Policy Set Configuration Details	442
Table 258: Timers Configuration Details	443
Table 259: Traceoption BSG Configuration Details	444
Table 260: CoS Configuration Details	448
Table 261: IDS Configuration Details	451
Table 262: Traceoptions Configuration Details	455
Table 263: NAT Configuration Details	457
Table 264: Virtual BGF Configuration Details	461
Table 265: Data Inactivity Detection Configuration Details	463
Table 266: Gateway Controller Configuration Details	464
Table 267: Graceful Restart Configuration Details	465
Table 268: H248 Configuration Details	466
Table 269: Encoding Defaults Configuration Details	466
Table 270: Context indication Configuration Details	467
Table 271: Control Association Configuration Details	469
Table 272: Virtual Interface Indications Configuration Details	471
Table 273: Data Inactivity Detection Configuration Details	472
Table 274: Base Root Package Configuration Details	474
Table 275: DiffServ Configuration Details	475
Table 276: Event Timestamp Notification Configuration Details	476
Table 277: Hanging Termination Detection Configuration Details	477
Table 278: Inactivity Timer Configuration Details	478
Table 279: Notification Behavior Configuration Details	479
Table 280: Segmentation Package Configuration Details	480
Table 281: Traffic Management Configuration Details	481
Table 282: H248 Timers Configuration Details	483
Table 283: Monitor Configuration Details	484
Table 284: Overload Control Configuration Details	484
Table 285: Session Mirroring Configuring Details	485
Table 286: Media Service Configuration Details	486
Table 287: Configuring Rule	486
Table 288: Configuring Rule Set	487
Table 289: Session Mirroring Configuration Details	488
Table 290: Traceoptions Configuration Details	489
Table 291: Virtual Interface Configuration Details	490
Table 292: Service Interface Pools Configuration Details	490

	Table 293: Stateful Firewall Configuration Details	492
	Table 294: Service Set Configuration Details	494
	Table 295: Captive Portal Configuration Details	497
	Table 296: Custom Options Configuration Details	498
	Table 297: Interface Configuration Details	499
	Table 298: File Configuration Details	501
	Table 299: Flag Configuration Details	502
	Table 300: Access Type Configuration Details	503
	Table 301: Authenticate Configuration Details	504
	Table 302: Dynamic Home Assignment Configuration Details	504
	Table 303: Enable Service Configuration Details	506
	Table 304: Pool Match Order Configuration Details	506
	Table 305: Virtual Network Configuration Details	507
	Table 306: Peer Configuration Details	508
	Table 307: Traceoptions Configuration Details	511
	Table 308: File Configuration Details	512
	Table 309: Flag Configuration Details	512
	Table 310: RPM Configuration Options	513
	Table 311: BGP Configuration Options	514
	Table 312: Routing Instance Configuration Options	515
	Table 313: Probe Configuration Options	515
	Table 314: Probe Server Configuration Details	518
	Table 315: UAC Configuration Details	519
	Table 316: Infranet Controller Configuration Details	520
	Table 317: Traceoptions Configuration Details	521
Chapter 24	Configuration of SNMP for Network Management	523
	Table 318: Basic System Identification Details	523
	Table 319: Configuring Community Fields	525
	Table 320: Configuring SNMP Trap Group Fields	527
	Table 321: Configuring SNMP View Fields	528
Chapter 25	Configuration of System	531
	Table 322: Destination Configuration Details	532
	Table 323: File and Flag Configuration Details	535
	Table 324: Archival Configuration Details	536
	Table 325: Arp Configuration Details	537
	Table 326: Auto Configuration Traceoptions Details	538
	Table 327: Provider Configuration Details	542
	Table 328: Resource Limits Configuration Details	543
	Table 329: Inet6 Backup Router Configuration Details	545
	Table 330: Internet Options Configuration Details	545
	Table 331: Location Details	548
	Table 332: Class Configuration Details	550
	Table 333: Password Configuration Details	551
	Table 334: Retry Options Configuration Details	552
	Table 335: User Configuration Details	553
	Table 336: Port Configuration Details	556
	Table 337: Radius Option Configuration Details	557
	Table 338: RADIUS Server Configuration Details	557

Table 339: Root Authentication Configuration Details	559
Table 340: Static Host Mapping Configuration Details	559
Table 341: TACACS+ Options Configuration Details	560
Table 342: TACACS+ Server Configuration Details	561

Part 5

Chapter 29

Monitor

Real Time Monitor	579
Table 343: Device Status Information	580

About the Documentation

- Documentation and Release Notes on page xxvii
- Supported Platforms on page xxvii
- Documentation Conventions on page xxvii
- Documentation Feedback on page xxix
- Requesting Technical Support on page xxix

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 <http://www.juniper.net/techpubs/>.

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 <http://www.juniper.net/books>.

Supported Platforms

For the features described in this document, the following platforms are supported:

- NSMXpress Series II
- NSMXpress
- NSM3000
- MX Series
- M Series

Documentation Conventions

Table 1 on page xxviii 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.

Table 2 on page xxviii 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 book 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 System Basics Configuration Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
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)	Enclose optional keywords or variables.	stub <default-metric <i>metric</i> >;

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

Convention	Description	Examples
(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 string2 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)	Enclose a variable for which you can substitute one or more values.	community name members [community-ids]
Indentation and braces ({ })	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop address; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web 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 J-Web selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release 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 J-Care or JNASC 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 <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://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: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- 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 <http://www.juniper.net/support/requesting-support.html>.

PART 1

Overview

- [Getting Started on page 3](#)
- [The Junos OS CLI and NSM on page 5](#)
- [Before You Begin Adding Devices on page 15](#)

CHAPTER 1

Getting Started

- [Introduction to Network and Security Manager on page 3](#)
- [Installing NSM on page 3](#)
- [Role-Based Administration on page 4](#)

Introduction to Network and Security Manager

Juniper Networks Network and Security Manager (NSM) gives you complete control over your network. Using NSM, you can configure all your Juniper Networks devices from one location, at one time.

NSM works with networks of all sizes and complexity. You can add a single device, or create device templates to help you deploy multiple devices. You can create new policies, or edit existing policies for security devices. The management system tracks and logs each administrative change in real time, providing you with a complete administrative record and helping you perform fault management.

NSM also simplifies control of your network with a straightforward user interface. Making all changes to your devices from a single, easy-to-use interface can reduce deployment costs, simplify network complexity, speed configuration, and minimize troubleshooting time.

For more detailed information about NSM, including a technical overview, working in the NSM user interface (UI), and new features in NSM 2010.1, see the section on getting started with NSM in the *Network and Security Manager Administration Guide*.

Related Documentation

- [Installing NSM on page 3](#)
- [Role-Based Administration on page 4](#)
- [NSM and Device Management Overview on page 5](#)

Installing NSM

NSM is a software application that enables you to integrate and centralize management of your Juniper Networks environment. You need to install two main software components to run NSM: the NSM management system and the NSM user interface (UI).

The overall process for installing NSM is as follows:

- Management System Installation Process
- User Interface Installation Process

Refer to the *Network Security Manager Installation Guide* for details on the steps to install the NSM management system on a single server or on separate servers. It also includes information about how to install and run the NSM user interface. The *Network Security Manager Installation Guide* is intended for IT administrators responsible for the installation of or upgrade to NSM.

**Related
Documentation**

- [Introduction to Network and Security Manager on page 3](#)
- [Role-Based Administration on page 4](#)
- [NSM and Device Management Overview on page 5](#)

Role-Based Administration

The NSM role-based administration (RBA) feature enables you to define strategic roles for your administrators, delegate management tasks, and enhance existing permission structures using task-based functions.

Use NSM to create a secure environment that reflects your current administrator roles and responsibilities. By specifying the exact tasks your NSM administrators can perform within a domain, you minimize the probability of errors and security violations and enable a clear audit trail for every management event.

For more detailed information about role-based administration, including using role-based administration more effectively and configuring role-based administration, see “Configuring Role-Based Administration” in the *Network and Security Manager Administration Guide*.

**Related
Documentation**

- [Introduction to Network and Security Manager on page 3](#)
- [Installing NSM on page 3](#)
- [NSM and Device Management Overview on page 5](#)

CHAPTER 2

The Junos OS CLI and NSM

- [NSM and Device Management Overview on page 5](#)
- [Understanding the CLI and NSM on page 6](#)
- [Comparing the CLI To the NSM UI on page 7](#)
- [NSM Services Supported for M Series and MX Series Devices on page 10](#)
- [How NSM Works with the CLI and Distributed Data Collection on page 11](#)
- [Device Schemas on page 12](#)
- [Communication Between a Device and NSM on page 13](#)

NSM and Device Management Overview

NSM is the Juniper Networks network management tool that allows distributed administration of network appliances like the M Series and MX Series routers. You can use the NSM application to centralize status monitoring, logging, and reporting, and to administer device configurations. The term *device* is used in NSM to describe a router or platform.

With NSM you can manage and administer a device from a single management interface.

In addition, NSM lets you manage most of the parameters that you can configure through the command-line interface (CLI). Although the configuration screens rendered in NSM look different, the top-level configuration elements essentially correspond to commands in the CLI.

NSM incorporates a broad configuration management framework that allows comanagement using other methods. To manage the device configuration, you can also use the XML files import and export feature, or you can manage from the device's admin console.

Related Documentation

- [Understanding the CLI and NSM on page 6](#)
- [Comparing the CLI To the NSM UI on page 7](#)
- [NSM Services Supported for M Series and MX Series Devices on page 10](#)
- [How NSM Works with the CLI and Distributed Data Collection on page 11](#)
- [Device Schemas on page 12](#)

- [Communication Between a Device and NSM on page 13](#)

Understanding the CLI and NSM

M Series and MX Series devices are routers that have the Junos OS installed as the operating system. With the Junos OS you use the command-line interface (CLI) to access an individual router (which is called a device in NSM)—whether from the console or through a network connection. The CLI is a Junos OS-specific command shell that runs on top of a UNIX-based operating system kernel. The CLI is a straightforward command interface you can use to monitor and configure a router. You type commands on a single line, and the commands are executed when you press the Enter key. For more information about the CLI, see the *Junos OS CLI User Guide*.

Network and Security Manager (NSM) is a software application that centralizes control and management of your Juniper Networks devices. NSM is a three-tier management system made up of the following:

- A user interface (UI)
- Management system
- Managed devices

The devices process your network traffic and are the enforcement points that implement your policies. The UI and management system tiers are software-based so you can deploy them quickly and easily. Because the management system uses internal databases for storage and authentication, you do not need LDAP or an external database. For more information about NSM architecture, see the technical overview in the *Network Security Manager Administration Guide*.

With NSM you can manage most of the parameters that you can configure through the CLI. Although the configuration screens rendered in NSM look different, the top-level configuration elements essentially correspond to commands in the CLI.

Typically, M Series and MX Series devices are managed individually using the CLI. The advantage of using NSM is that you can centralize status monitoring and administration of the configurations of a network of M Series and MX Series devices.

Related Documentation

- [NSM and Device Management Overview on page 5](#)
- [Comparing the CLI To the NSM UI on page 7](#)
- [NSM Services Supported for M Series and MX Series Devices on page 10](#)
- [How NSM Works with the CLI and Distributed Data Collection on page 11](#)
- [Device Schemas on page 12](#)
- [Communication Between a Device and NSM on page 13](#)

Comparing the CLI To the NSM UI

Because NSM is a UI and the CLI is a command-line interface, the way you access configuration, monitoring, and management information is different in each interface. The CLI has two modes: operational mode and configuration mode.

- Operational mode—This mode displays the current router status. In operational mode, you enter commands to monitor and troubleshoot the software, network connectivity, and router.
- Configuration mode—A router configuration is stored as a hierarchy of statements. In configuration mode, you enter these statements to define all properties of the Junos OS, including interfaces, general routing information, routing protocols, user access, and several system hardware properties.

The following sample output shows the operational mode commands available at the top level of the CLI operational mode:

```
user@host> ?
Possible completions:
clear          Clear information in the system
configure      Manipulate software configuration information
file           Perform file operations
help           Provide help information
monitor        Show real-time debugging information
mtrace         Trace multicast path from source to receiver
op             Invoke an operation script
ping           Ping remote target
quit           Exit the management session
request        Make system-level requests
restart        Restart software process
set            Set CLI properties, date/time, craft interface message
show           Show system information
ssh            Start secure shell on another host
start          Start shell
telnet         Telnet to another host
test           Perform diagnostic debugging
traceroute     Trace route to remote host
```

The following sample output shows the protocols configuration of an M Series device:

```
[edit]
user@host# show protocols
mpls {
    interface ge-1/3/3.0;
    interface fe-0/1/2.0;
    interface fe-0/1/1.0;
}
ospf {
    traffic-engineering;
    area 0.0.0.1 {
        interface lo0.0 {
            passive;
        }
        interface ge-1/3/3.0;
        interface fe-0/1/2.0;
        interface fe-0/1/1.0;
```

```

    }
}

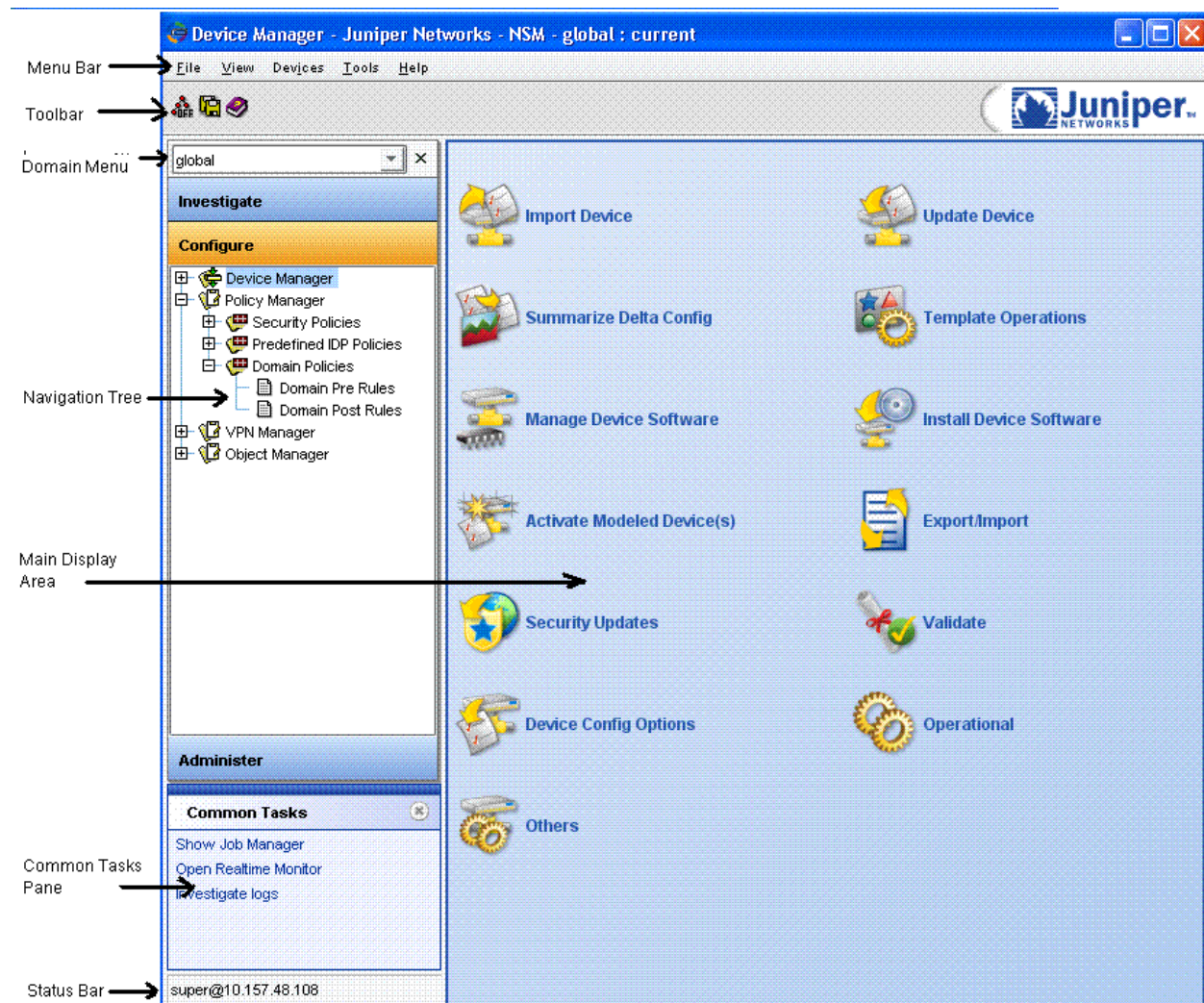
```

For more information about operational and configuration mode, see the *Junos OS CLI User Guide*.

In contrast, the NSM UI displays a set of menus, toolbar icons at the top of the UI window, and a navigation tree that includes an Investigate panel, a Configure panel, and an Administer panel. For some components, right-click menus are available to perform tasks.

Figure 1 on page 8 shows the NSM UI with the Configure navigation tree expanded and the main display area containing the services available from the Configure panel. Different services display when you select the Investigate or Administer panels.

Figure 1: Overview of the User Interface



- Menu bar—Contains clickable commands. You can access many menu bar commands using keyboard shortcuts. For a complete list of keyboards shortcuts, see the *Network and Security Manager Online Help*.
- Toolbar—Contains buttons for common tasks. The buttons displayed in the toolbar are determined by the selected module.
- Domain menu—Contains a pull-down menu above the navigation tree where domains and subdomains are selected. The domains and subdomains displayed are those to which the current user has access.
- Navigation Tree—The navigation tree displays the 11 NSM modules in the left pane of the NSM window.
- Investigate panel—Provides NSM modules with tree structures for monitoring your network.
- Configure panel—Provides NSM modules with tree structures for configuring devices, policies, virtual private networks (VPNs), and other objects.
- Administer panel—Provides NSM modules with tree structures for managing the NSM servers, ongoing jobs, and other actions.
- Main display area—Displays the content for the currently selected module or module contents.
- Common tasks pane—Provides links to commonly accessed tasks throughout the UI. These common tasks change depending on what tasks are often selected in the UI.
- Status bar—Displays additional information for a selected module.

For details about the Investigate, Configure, and Administer panels, see “NSM Modules” in the *Network Security Manager Administration Guide*.

**Related
Documentation**

- [NSM and Device Management Overview on page 5](#)
- [Understanding the CLI and NSM on page 6](#)
- [NSM Services Supported for M Series and MX Series Devices on page 10](#)
- [How NSM Works with the CLI and Distributed Data Collection on page 11](#)
- [Device Schemas on page 12](#)
- [Communication Between a Device and NSM on page 13](#)

NSM Services Supported for M Series and MX Series Devices

NSM supports the following services for the M Series and MX Series devices:

- Device management—Enables addition of new devices, editing and deletion of existing devices, software version update, reconfiguration of existing devices, activation of modeled devices, and master Routing Engine switchover with synchronized commits. In addition, Return Merchandise Authorization (RMA) updates enable failed device replacement without a serial number or connection statistics.
- Device discovery—Uses sets of rules to find, add, and import multiple devices into NSM. In addition, configure and run rules to search a network and find devices in a specified subnet, or within a specified range of IP addresses. M Series and MX Series devices must be configured with static IP addresses to be found by device discovery rules.
- Topology management—Provides discovery and management of the physical topology of a network of devices connected to a Juniper Networks EX-series switch. These include networking devices such as the J-series, M Series, MX Series and EX-series as well as ScreenOS and Intrusion Detection and Prevention (IDP) devices, IP phones, desktops, printers, and servers. The Topology Manager also provides details about connections between a device and the EX-series switch.
- Inventory and license management—Displays device inventory and licensing details. In a dual Routing Engine system, the inventory data is collected from the master Routing Engine.
- Upgrading software for single and dual Routing Engines.
- Configuration management—Enables in-device configuration and editing, configuration groups, and template configuration.
- Status monitoring—Displays a list of all managed devices, including status, name, domain, OS version, synchronization status, connection details, and current alarms.
- Job management—Displays details of the update process in a dedicated information window and includes the update's success or failure and the errors involved in a failed update.

Below is a summary of the services that are not supported for the M Series and MX Series devices:

- Adding, deleting, or editing licensing information, (though licenses can be viewed).
- Downgrading software.
- Configuration of cluster objects, policy manager, VPN manager, and shared objects.
- Junos Redundancy Protocol (JSRP), VPN, and IDP cluster monitor.

Related Documentation

- [NSM and Device Management Overview on page 5](#)
- [Understanding the CLI and NSM on page 6](#)
- [Comparing the CLI To the NSM UI on page 7](#)

- [How NSM Works with the CLI and Distributed Data Collection on page 11](#)
- [Device Schemas on page 12](#)
- [Communication Between a Device and NSM on page 13](#)

How NSM Works with the CLI and Distributed Data Collection

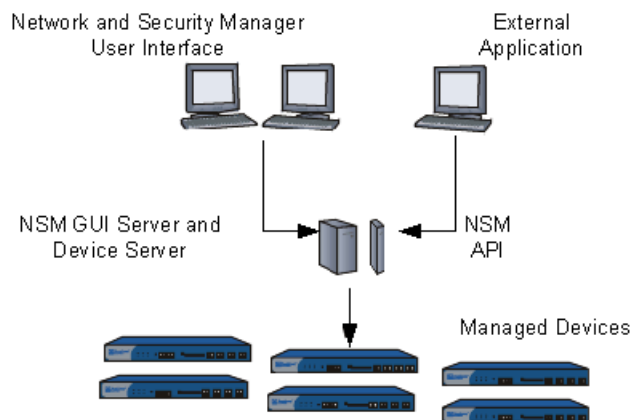
Before we can discuss how NSM works with the CLI, the following terms need to be defined:

- *ADM (Abstract Data Model)*—The Abstract Data Model is an XML file that contains all the configuration information for a domain.
- *configlet*—A configlet is a small, static configuration file that contains information about how a device can connect to NSM.
- *Device Server*—The Device Server is the component of the NSM management system that handles communication between the GUI Server and the device, collects data from the managed devices on your network, formats configuration information sent to your managed device, and consolidates log and event data.
- *DM (Data Model)*—A Data Model is an XML file that contains configuration data for an individual device. The DM is stored in the Device Server; when you create, update, or import a device, the GUI Server edits the Abstract Data Model (ADM) to reflect the changes, then translates that information to the DM
- *GUI Server*—The GUI Server manages the system resources and data that drives NSM functionality. The GUI Server contains the NSM databases and centralizes information for devices and their configurations, attack and server objects, and policies.

NSM and the CLI communicate through the GUI and Device Servers that translate objects and object attributes in both directions. Device configuration information is translated into Data Model (DM) objects or Abstract Data Model (ADM) object attributes, and conversely DM objects and ADM object attributes are translated into XML configlets and documents.

NSM uses a distributed data collection system. Each device is described by a unique DM. The DM is stored in the Device Server which communicates with the GUI Server and the device.

When you create, update, or import a device into NSM, the GUI Server edits the ADM to reflect the changes, then translates that information to the DM. The ADM contains configuration data for all objects in a specific domain. When you use the UI to interface with your managed devices, the ADM and DMs work together.

Figure 2: NSM Network Architecture

- When you update a device configuration, the GUI Server translates the objects and object attributes in the ADM domain into device configuration information in a DM. For DMI based devices which include the M Series and MX Series, the Device Server converts the DM into an XML configlet and sends the configlet through NetConf protocol to the device.
- When you import a device configuration, the device sends the configuration through the NetConf protocol as an XML document to the Device Server, which translates the XML document into a DM with device configuration information. The GUI Server then translates the device configuration in the DM into objects and object attributes in the ADM, and uses the ADM to display current information in the UI.

For more details on the ADM and DMs, see “Managing Devices” in the *Network Security Manager Administration Guide*.

The management system also provides an application programming interface (API) for integrating NSM into larger enterprise business systems. This NSM API provides an alternative interface to that provided by the UI. For details, see the *Network and Security Manager API Guide*.

Related Documentation

- [NSM and Device Management Overview on page 5](#)
- [Understanding the CLI and NSM on page 6](#)
- [Comparing the CLI To the NSM UI on page 7](#)
- [NSM Services Supported for M Series and MX Series Devices on page 10](#)
- [Device Schemas on page 12](#)
- [Communication Between a Device and NSM on page 13](#)

Device Schemas

The structure of the ADM and the DMs is defined by a DM schema, which lists all the possible fields and attributes for a type of object or device. The DM schema reads from a capability file, which lists the fields and attributes that a specific operating system version supports, to determine the supported features for the operating system version

that is running on the managed devices. NSM uses capability files to enable Junos OS upgrades without changing the device configuration in NSM.

The M Series and MX Series device families are described by schemas that are maintained on a schema repository owned by Juniper Networks. These schemas can be added dynamically to NSM.

**Related
Documentation**

- [NSM and Device Management Overview on page 5](#)
- [Understanding the CLI and NSM on page 6](#)
- [Comparing the CLI To the NSM UI on page 7](#)
- [NSM Services Supported for M Series and MX Series Devices on page 10](#)
- [How NSM Works with the CLI and Distributed Data Collection on page 11](#)
- [Communication Between a Device and NSM on page 13](#)

Communication Between a Device and NSM

The M Series and MX Series devices and the NSM application communicate through the Device Management Interface (DMI). DMI is a collection of schema-driven protocols that run on a common transport (TCP). DMI is designed to work with routers running the Junos OS to make device management consistent across all administrative realms. The DMI protocols that are supported include NetConf (for inventory management, XML-based configuration, text-based configuration, alarm monitoring, and device-specific commands), structured system log, and threat flow for network profiling. DMI supports third-party network management systems that incorporate the DMI standard; however, only one DMI-based agent per device is supported.

The configuration of the M Series and MX Series device is represented as a hierarchical tree of configuration items. This structure is expressed in XML that can be manipulated with NetConf. NetConf is a network management protocol that uses XML. DMI uses NetConf's generic configuration management capability and applies it to allow remote configuration of the device.

The schema repository enables access to XSD and XML files defined for each device, model, and software version.

**Related
Documentation**

- [NSM and Device Management Overview on page 5](#)
- [Understanding the CLI and NSM on page 6](#)
- [Comparing the CLI To the NSM UI on page 7](#)
- [NSM Services Supported for M Series and MX Series Devices on page 10](#)
- [How NSM Works with the CLI and Distributed Data Collection on page 11](#)
- [Device Schemas on page 12](#)

CHAPTER 3

Before You Begin Adding Devices

- [M Series and MX Series Devices Supported by NSM on page 15](#)
- [Considering the Device Status on page 16](#)
- [Configuring a Deployed M Series or MX Series Device for Importing to NSM on page 17](#)

M Series and MX Series Devices Supported by NSM

[Table 3 on page 15](#) lists the M Series and MX Series Routers, and the versions of Junos OS that NSM supports.

Table 3: M Series Multiservice Edge Routers and MX Series Ethernet Services Routers

Device	Versions of Junos OS
Juniper Networks M7i	Junos OS Release 9.3, 9.4, 9.5, 9.6, 10.0, 10.1, 10.2 (via schema update)
Juniper Networks M10i	Junos OS Release 9.3, 9.4, 9.5, 9.6, 10.0, 10.1, 10.2 (via schema update)
Juniper Networks M40e	Junos OS Release 9.3, 9.4, 9.5, 9.6, 10.0, 10.1, 10.2 (via schema update)
Juniper Networks M120	Junos OS Release 9.3, 9.4, 9.5, 9.6, 10.0, 10.1, 10.2 (via schema update)
Juniper Networks M320	Junos OS Release 9.3, 9.4, 9.5, 9.6, 10.0, 10.1, 10.2 (via schema update)
Juniper Networks MX240	Junos OS Release 9.3, 9.4, 9.5, 9.6, 10.0, 10.1, 10.2 (via schema update)
Juniper Networks MX240 with MS-DPC PIC	Junos OS Release 9.4, 9.5, 9.6, 10.0, 10.1, 10.2 (via schema update)
Juniper Networks MX240 with IDP services	Junos OS Release 9.4, 9.5, 9.6, 10.0, 10.1

Table 3: M Series Multiservice Edge Routers and MX Series Ethernet Services Routers (*continued*)

Device	Versions of Junos OS
Juniper Networks MX480	Junos OS Release 9.3, 9.4, 9.5, 9.6, 10.0, 10.1, 10.2 (via schema update)
Juniper Networks MX480 with MS-DPC PIC	Junos OS Release 9.4, 9.5, 9.6, 10.0, 10.1, 10.2 (via schema update)
Juniper Networks MX480 with IDP services	Junos OS Release 9.4, 9.5, 9.6, 10.0, 10.1
Juniper Networks MX960	Junos OS Release 9.3, 9.4, 9.5, 9.6, 10.0, 10.1, 10.2 (via schema update)
Juniper Networks MX960 with MS-DPC PIC	Junos OS Release 9.4, 9.5, 9.6, 10.0, 10.1, 10.2 (via schema update)
Juniper Networks MX960 with IDP services	Junos OS Release 9.4, 9.5, 9.6, 10.0, 10.1

- Related Documentation**
- [Considering the Device Status on page 16](#)
 - [Configuring a Deployed M Series or MX Series Device for Importing to NSM on page 17](#)

Considering the Device Status

The network status of your device influences the preliminary configuration required before you can add the device to NSM and the method you use to add the device to NSM. Devices can be deployed in your network or undeployed. Deployed devices can be configured with a static or dynamic IP address, which influences the method you use to add them to NSM. Also, undeployed devices are treated differently from deployed devices.

- **Deployed devices**—Deployed devices are the devices you are currently using in your existing network. These devices have already been configured with a static or dynamic IP address and other basic information. You can import a device with a static or dynamic IP address to NSM, so long as it has the following enabled:
 - The management interface (fxp0) with the IP address of the device and a user with full administrative privileges for the NSM administrator.
 - A physical connection to your network with access to network resources.
 - Connectivity to the NSM device server, which can be with a static IP address.
 - Telnet or SSHv2, and NETCONF protocol over SSH.

The NSM process of importing a deployed device differs depending on whether your device is configured with a static or dynamic IP address. For information about importing a device with a static IP address or about importing a device with a dynamic IP address, see the *Network Security Manager Administration Guide*.



NOTE: To import device configurations, the connection between NSM and the managed device must be at least 28.8 Kbps. For details on installing NSM on your network, refer to the *Network and Security Manager Installation Guide*.

- **Undeployed devices**—Undeployed devices are devices that you are not currently using in your network and, typically, for which you do not have IP addresses, zones, or other basic network information. For undeployed devices, you can model a new device configuration and later install that configuration on the device. For more information about adding undeployed devices, see “Modeling a Device” in the *Network Security Manager Administration Guide*.

Related Documentation

- [M Series and MX Series Devices Supported by NSM on page 15](#)
- [Configuring a Deployed M Series or MX Series Device for Importing to NSM on page 17](#)

Configuring a Deployed M Series or MX Series Device for Importing to NSM

A deployed device is a device you are currently using in your network. Before you can add a deployed device to NSM, you must configure the following parameters on the device, regardless of the static or dynamic nature of the IP address:

- The management interface (fxp0) with the IP address of the device
- A user with full administrative privileges for the NSM administrator
- A physical connection to your network with access to network resources
- Connectivity to the NSM device server, which can be with a static IP address
- Telnet or SSHv2, and NETCONF protocol over SSH

To configure these parameters, perform the following tasks:

- [Configure an IP Address and a User with Full Administrative Privileges for the Device on page 17](#)
- [Check Network Connectivity on page 18](#)
- [Check Connectivity to the NSM Server on page 18](#)
- [Configure a Static Route to the NSM Server on page 18](#)
- [Establish a Telnet or an SSHv2, and a NETCONF protocol over SSH Connection to the NSM Server on page 20](#)

Configure an IP Address and a User with Full Administrative Privileges for the Device

Purpose Before you can add an M Series or MX Series device to NSM, you must have an IP address configured on the management interface (fxp0) and a user with full administrative privileges for the NSM administrator.

Action Generally when you install the Junos OS, you configure the router from scratch and at that point you configure the management interface (fxp0) with the IP address and a user with full administrative privileges.

For information about configuring the router from scratch, see the *Junos OS System Basics Configuration Guide*.

For step-by-step instructions on reconfiguring names, addresses, and the root password after reinstalling the Junos OS, see “Configure Names and Addresses” and “Example: Configuring the Root Password.”

Check Network Connectivity

Purpose Establish that the M Series or MX Series device has a connection to your network.

Action To check that the device has a connection to your network, log on to the M Series or MX Series device and issue a **ping** command to a system on your network:

```
root@> ping address
```

If there is no response, verify that there is a route to the **address** using the **show route** command. If the address is outside your **fxp0** subnet, add a static route.

Check Connectivity to the NSM Server

Purpose Establish that the M Series or MX Series device has a connection to the NSM server.

Action To check that the device has a connection to the NSM server, log on to the M Series or MX Series device and issue a **ping** command to the IP address of the NSM server:

```
root@> ping address
```

If there is no response, verify that there is a route to the **address** using the **show route** command. If the address is outside your **fxp0** subnet, add a static route to the NSM server.

Configure a Static Route to the NSM Server

Purpose When your M Series or MX Series device and the NSM server are in different subnets, you can install a static route on the device to connect to the NSM server. The static route is installed in the routing table only when the route is active; that is, the list of next-hop routers configured for that route contains at least one next hop on an operational interface.

Action To configure a static route, follow these steps:

1. Log on to the M Series or MX Series device and, in configuration mode, go to the following hierarchy level:

```
[edit]  
user@host# edit routing-options
```

2. Configure a static route to the NSM server with the **retain** option so that the static route remains in the forwarding table when the routing protocol process shuts down normally:

```
[edit routing-options]
user@host# set static route destination-prefix next-hop address retain
```

3. Configure the **no-readvertise** option so that the route is not eligible for readvertisement by dynamic routing protocols:

```
[edit routing-options]
user@host# set static route destination-prefix next-hop address no-readvertise
```

4. Verify the configuration:

```
user@host# show
```

5. Commit the configuration:

```
user@host# commit
```

6. Verify the connection to the NSM server:

```
user@host# run ping destination
```

Sample Output

```
user@host> edit
Entering configuration mode

[edit]
user@host# edit routing-options

[edit routing-options]
user@host# set static route 192.193.60.181/32 next-hop 192.193.76.254

[edit routing-options]
user@host# set static route 192.193.60.181/32 retain

[edit routing-options]
user@host# set static route 192.193.60.181/32 no-readvertise

[edit routing-options]
user@host# show
static {
}
  route 192.193.60.181/32 {
    next-hop 192.193.76.254;
    retain;
    no-readvertise;
  }
}

[edit routing-options]
user@host# commit
commit complete

[edit routing-options]
user@host# run ping 192.193.60.181
PING 192.193.60.181 (192.193.60.181): 56 data bytes
64 bytes from 192.193.60.181: icmp_seq=0 ttl=64 time=23.050 ms
64 bytes from 192.193.60.181: icmp_seq=1 ttl=64 time=18.129 ms
```

```
64 bytes from 192.193.60.181: icmp_seq=2 ttl=64 time=0.304 ms
^C
--- 192.193.60.181 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.304/13.828/23.050/9.771 ms
```

Meaning The sample output shows that a static route (192.193.60.181/32) to the NSM server is configured and committed, and that there is a connection between the router and the server because the **ping** command shows that three packets were transmitted and received.

Establish a Telnet or an SSHv2, and a NETCONF protocol over SSH Connection to the NSM Server

To configure an M Series or MX Series device before adding it to NSM, take the following steps:

1. Log on to the M Series or MX Series device.
2. In configuration mode, go to the following hierarchy level:
[edit system services]
3. At the [edit system services] hierarchy level, enter the following commands:
user@host# set ftp
user@host# set ssh protocol-version v2
user@host# set telnet
user@host# set netconf ssh
4. Verify the configuration:
user@host# show
5. Commit the configuration:
user@host# commit

Sample Output

```
[edit]
user@host# edit system services

[edit system services]
user@host# set ftp

[edit system services]
user@host# set ssh protocol-version v2

[edit system services]
user@host# set telnet

[edit system services]
user@host# set netconf ssh

[edit system services]
user@host# show
ftp;
ssh {
    protocol-version v2;
}
telnet;
netconf {
    ssh;
}

[edit system services]
user@host# commit
commit complete
```


PART 2

Integration

- [Addition of M Series and MX Series Devices on page 25](#)
- [M Series and MX Series Devices Update on page 31](#)

CHAPTER 4

Addition of M Series and MX Series Devices

- [About Device Creation on page 25](#)
- [Supported Add Device Workflows for M Series and MX Series Devices on page 26](#)
- [Importing Devices Overview on page 27](#)
- [Modeling Devices Overview on page 28](#)
- [Adding Multiple Devices Using Automatic Discovery \(Junos OS Devices Only\) on page 29](#)
- [Adding Device Groups Overview on page 29](#)

About Device Creation

Before Network and Security Manager (NSM) can manage devices, you must first add those devices to the management system using the NSM user interface (UI). To add a device, you create an object in the UI that represents the physical device, and then create a connection between the UI object and the physical device so that their information is linked. When you make a change to the UI device object, you can push that information to the real device so the two remain synchronized. You can add a single device at a time or add multiple devices all at once.



NOTE: The connection between a managed device and the NSM Device Server must be at least 28.8 Kbps.

How you add your devices to the management system depends on the network status of the device. You can import deployed devices, or you can model devices that have not yet been deployed:

- **Import deployed devices**—Deployed devices are the devices you are currently using in your existing network. These devices have already been configured with a static or dynamic IP address and other basic information. For deployed devices, you can import the existing device configuration information into NSM.



NOTE: To import device configurations, the connection between NSM and the managed device must be at least 28.8 Kbps. For details on installing NSM on your network, refer to the *Network and Security Manager Installation Guide*.

- Model undeployed devices—Undeployed devices are devices that you are not currently using in your network and, typically for which, you do not have IP addresses, zones, or other basic network information. For undeployed devices, you can model a new device configuration and later install that configuration on the device.

To help you add a device, the UI contains an Add Device wizard that walks you through each step of the device creation process. The Add Device wizard prompts you to first choose a workflow from the given options. **Device is reachable** is the default option. The wizard then prompts you for specific device information, such as the device platform name, OS name and version, IP address, and device administrator name, and then uses that information to detect the device. You can then choose to modify the displayed name of the device and assign a color to the device. If the host name is not unique within NSM or is undetected, the Add Device wizard generates a validation error, forcing you to add a valid device name in order to proceed with adding the physical device to the Device Server.

After the physical device connects, it is considered to be a *managed device*, meaning it is now under the control of NSM.

For more detailed information about verifying and managing a device, see “About Device Creation” in the *Network and Security Manager Administration Guide*.

Related Documentation

- [Supported Add Device Workflows for M Series and MX Series Devices on page 26](#)
- [Importing Devices Overview on page 27](#)
- [Modeling Devices Overview on page 28](#)
- [Adding Multiple Devices Using Automatic Discovery \(Junos OS Devices Only\) on page 29](#)
- [Adding Device Groups Overview on page 29](#)

Supported Add Device Workflows for M Series and MX Series Devices

An M Series or MX Series device can be added using the following methods or workflows:

- Import device with static IP address
- Import device with dynamic IP address
- Model and activate device
- Rapid deployment (configlets)
- Device discovery

- Import many devices (CSV file) with static IP addresses
- Import many devices (CSV file) with dynamic IP addresses

The model many devices (CSV file) workflow is not supported.

**Related
Documentation**

- [About Device Creation on page 25](#)
- [Importing Devices Overview on page 27](#)
- [Modeling Devices Overview on page 28](#)
- [Adding Multiple Devices Using Automatic Discovery \(Junos OS Devices Only\) on page 29](#)
- [Adding Device Groups Overview on page 29](#)

Importing Devices Overview

NSM can import device configurations from M Series and MX Series devices running Junos OS 9.3 or later.

When importing from a device, the management system connects to the device and imports Data Model (DM) information that contains details of the device configuration. The connection is secured using Secure Server Protocol (SSP), a proprietary encryption method; an always-on connection exists between the management system and the device.

For details about adding multiple devices at one time, see the *Network and Security Manager Administration Guide*.

Requirements To import a single device, you must have available the following requirements:

- A management interface (fxp0) with the IP address of the device
- A user with full administrative privileges for the NSM administrator
- Device connection information (IP address, connection method) and the device administrator's name and password



NOTE: All passwords handled by NSM are case-sensitive.

- A physical connection to your network with access to network resources
- Connectivity to the NSM Device Server, which can be with a static IP address
- A Telnet or an SSHv2, and a NETCONF protocol over SSH connection



NOTE: After importing a device configuration, log entries from that device begin to appear in the Log Viewer. However, until you update the device from NSM, the following log fields display 0 (or unknown):

- domain
- rulebase
- policy
- rule number
- source zone
- destination zone

After you update the imported device configuration using NSM, the appropriate values are displayed for log entries from the device.

When you import a device configuration, the Log Viewer displays the appropriate values for the device's log entries. This feature eliminates the need to update the device after importing it.

For more detailed information about adding and importing devices with static and dynamic IP addresses and verifying imported device configurations, see “Adding Devices” in the *Network and Security Manager Administration Guide*.

**Related
Documentation**

- [About Device Creation on page 25](#)
- [Supported Add Device Workflows for M Series and MX Series Devices on page 26](#)
- [Modeling Devices Overview on page 28](#)
- [Adding Multiple Devices Using Automatic Discovery \(Junos OS Devices Only\) on page 29](#)
- [Adding Device Groups Overview on page 29](#)

Modeling Devices Overview

For an undeployed M Series or MX Series device, you can create a device configuration in NSM, and then install that device configuration on the physical device.

Adding a single undeployed device to NSM is a four-stage process:

1. Model the device in the UI.
2. Create the device object configuration.
3. Activate the device.
4. Update the device configuration.

For more detailed information and steps about modeling a device, see “Modeling Devices” in the *Network and Security Manager Administration Guide*.

**Related
Documentation**

- [About Device Creation on page 25](#)
- [Supported Add Device Workflows for M Series and MX Series Devices on page 26](#)
- [Importing Devices Overview on page 27](#)
- [Adding Multiple Devices Using Automatic Discovery \(Junos OS Devices Only\) on page 29](#)
- [Adding Device Groups Overview on page 29](#)

Adding Multiple Devices Using Automatic Discovery (Junos OS Devices Only)

You can use automatic discovery to add and import multiple Junos OS devices into NSM. You do so by configuring and running discovery rules. For a Junos OS device to be discovered by this mechanism, it must be configured with a static IP address.

By configuring and running a discovery rule, you can search a network to discover devices in a specified subnet or within a range of IP addresses. Authentication of the devices is through administrator login SSHv2 credentials and SNMP community settings, which you also configure as part of the rule. Devices that match the rules for discovery also present an SSH key for your verification before the device is added to NSM.

For more detailed information and steps about adding multiple M Series and MX Series devices using automatic discovery, see “Adding a Device Discovery Rule” and “Running a Device Discovery Rule” in the *Network and Security Manager Administration Guide*.

**Related
Documentation**

- [About Device Creation on page 25](#)
- [Supported Add Device Workflows for M Series and MX Series Devices on page 26](#)
- [Importing Devices Overview on page 27](#)
- [Modeling Devices Overview on page 28](#)
- [Adding Device Groups Overview on page 29](#)

Adding Device Groups Overview

You can create groups of devices to manage multiple devices at one time. Use device groups to organize your managed devices, making it easier for you to configure and manage devices within a domain. You can group devices by type (such as all the M Series in a domain), by physical location (such as all the devices in the San Jose office), or logically (such as all the devices in sales offices throughout western Europe).

Use the groups to:

- Deploy new or updated device configurations to the entire device group.
- Deploy new or updated policies to the entire device group.

The devices that you add to a device group must exist; that is, you must have previously added or modeled the devices in the domain. You can group devices before configuring them. You can add a device to more than one device group. You can also add a device group to another device group.



.....

NOTE: You cannot apply a template to a device group. You must apply templates to individual devices in a device group. If you need to apply the same set of templates to multiple devices, you can create a single template that includes all the templates that are to be applied to a device, and then apply the combined template to each device.

.....

For an example of creating a device group, see “Adding Device Groups” in the *Network and Security Manager Administration Guide*.

**Related
Documentation**

- [About Device Creation on page 25](#)
- [Supported Add Device Workflows for M Series and MX Series Devices on page 26](#)
- [Importing Devices Overview on page 27](#)
- [Modeling Devices Overview on page 28](#)
- [Adding Multiple Devices Using Automatic Discovery \(Junos OS Devices Only\) on page 29](#)

CHAPTER 5

M Series and MX Series Devices Update

- [About Updating M Series and MX Series Devices on page 31](#)
- [How the Update Process Works on page 32](#)
- [Job Manager on page 33](#)
- [Tracking Updated Devices Using Job Manager on page 34](#)
- [Reviewing Job Information Displayed in Job Manager on page 35](#)
- [Device States Displayed in Job Manager During Update on page 36](#)
- [Understanding Updating Errors Displayed in the Job Manager on page 37](#)

About Updating M Series and MX Series Devices

When you update a managed device, you modify the running device configuration (the configuration currently installed on the physical device) with the modeled device configuration (the configuration currently modeled in Network and Security Manager (NSM)).

You can update a single device, multiple devices, or device groups simultaneously. For example, if you have created a device group that includes only M Series devices, you can update the entire device group in a single update procedure. During the update, NSM displays the progress of the update on each individual device so you can see exactly what is happening. Simultaneous updating also reduces downtime to unaffected devices and areas of your network.

Updating a device is a three-step process.

1. Ensure that you have configured the device correctly, created and assigned a policy to the device, and established a connection between the device and the management server.
2. From the Device Manager launchpad, select **Update Device**. The launchpad displays the Update Device(s) dialog box.

All connected and managed devices appear in the device list. Modeled devices and devices awaiting import for the first time do not appear.

3. Select the devices or device groups you want to update and click **Apply Changes**. NSM updates the selected devices or device groups with the modeled configuration.

NSM uses centralized control and tracking to indicate when you need to update a device, and to follow the progress of the device configuration you are updating. Before updating your managed devices, you can use other NSM modules and tools to identify devices that need to be updated, validate their modeled configurations, and preview how those devices accept the new configuration. After updating, you can use the same tools to verify a successful update. These tools include:

- **Audit Log Viewer**—This NSM module records changes made to a device configuration. The audit log entry also identifies the administrator who performed the change, shows when the change was updated on the device, and provides a history of change details.
- **Configuration Summaries**—These tools provide a preview of the modeled configuration, enabling you to compare it with the configuration that is running on the device. Use configuration summaries to ensure the modeled configuration is consistent with what you want to update on the device.
- **Job Manager**—This NSM module tracks the status of running and completed update processes. The Job Manager displays details of the update process in a dedicated information window and includes the update's success or failure and errors involved in a failed update.

For more information about updating devices, including knowing when to update, using preview tools, performing updates, tracking updates and rebooting devices, see “Updating Devices” in the *Network and Security Manager Administration Guide*.

**Related
Documentation**

- [How the Update Process Works on page 32](#)
- [Job Manager on page 33](#)
- [Tracking Updated Devices Using Job Manager on page 34](#)
- [Reviewing Job Information Displayed in Job Manager on page 35](#)
- [Device States Displayed in Job Manager During Update on page 36](#)
- [Understanding Updating Errors Displayed in the Job Manager on page 37](#)

How the Update Process Works

After you have successfully added the device to NSM, reviewed the device configuration, updated the device, and have the managed device functioning normally, an event might occur on the managed device that requires a change to the device configuration. For example, malicious traffic might have entered your network, requiring you to update the device to detect and prevent that attack.

1. Using the NSM monitoring tools, you learn of the attack and locate the cause of the event. Using NSM modules such as the Realtime Monitor and Log Viewer, you determine the exact attack that penetrated the device. From the Report Manager, you also determine what rule in the security policy was ineffective in blocking the attack.
2. You update the modeled device configuration, editing the configuration to detect and prevent the attack from entering your network again.

3. Before updating the running configuration, you review the modeled device configuration. Using a delta configuration summary, compare the modeled configuration with the running configuration on the device to confirm the differences. Fine-tune the modeled configuration, if needed.
4. When you are confident that the modeled configuration is valid, update the device. NSM updates the running configuration with only the new changes (delta). During the update, you track the update progress using Job Manager in real time and observe the transfer of the configuration from NSM to the device.

If the update is unsuccessful, use the information in the Job information dialog box to correct the problems in the modeled configuration.

5. After updating, run a second delta configuration summary to identify any remaining differences between the modeled configuration and the running configuration on the device. When the delta configuration summary reveals no differences between the new configuration and the old configuration on the device, you have successfully updated the running configuration.

**Related
Documentation**

- [About Updating M Series and MX Series Devices on page 31](#)
- [Job Manager on page 33](#)
- [Tracking Updated Devices Using Job Manager on page 34](#)
- [Reviewing Job Information Displayed in Job Manager on page 35](#)
- [Device States Displayed in Job Manager During Update on page 36](#)
- [Understanding Updating Errors Displayed in the Job Manager on page 37](#)

Job Manager

You can view the progress of communication to and from your devices in the Job Manager, that is located in the Administer panel. NSM sends commands to managed devices at your request, typically to import, update or reboot devices, and view configuration and delta configuration summaries. When you send a command to a device or group of devices, NSM creates a job for that command and displays information about that job in the Job Manager module.

Job Manager tracks the progress of the command as it travels to the device and back to the management system. Each job contains:

- Name of the command
- Date and time the command was sent
- Completion status for each device that received the command
- Detailed description of command progress
- Command output, such as a configuration list or command-line interface (CLI) changes on the device



NOTE: Job Manager configuration summaries and job information details do not display passwords in the list of CLI commands for administrators that do not have the assigned activity “View Device Passwords.” By default, only the super administrator has this assigned activity.

Related Documentation

- [About Updating M Series and MX Series Devices on page 31](#)
- [How the Update Process Works on page 32](#)
- [Tracking Updated Devices Using Job Manager on page 34](#)
- [Reviewing Job Information Displayed in Job Manager on page 35](#)
- [Device States Displayed in Job Manager During Update on page 36](#)
- [Understanding Updating Errors Displayed in the Job Manager on page 37](#)

Tracking Updated Devices Using Job Manager

Use Job Manager to track device updates in real time. You can view the status of a running update and the status of completed updates in the Job Manager module.

When you send a command to a device or group of devices using NSM, the management system creates a *job* for that command and displays information about that job in the Job Information dialog box. The command you send is called a *directive*.

Job Manager includes the following utilities and information:

- View Controls—Use View controls to set the information level you want displayed in Job Manager:
 - *Expand All* displays all devices associated with a directive type.
 - *Collapse All* displays the directive type.
- Job Type (Directive) List—Displays the job type (directives) and associated timestamp completion status information. All current and completed jobs appear, including device updates. However, if you have not yet performed an update using NSM, the Job List does not display an Update Configuration directive.
- Notification Controls—Enables you to manually view job completion status.
- Job Information—Enables you to view job information, including errors, job completion status, job state, automatic job completion notification setting, and start time of job.

Related Documentation

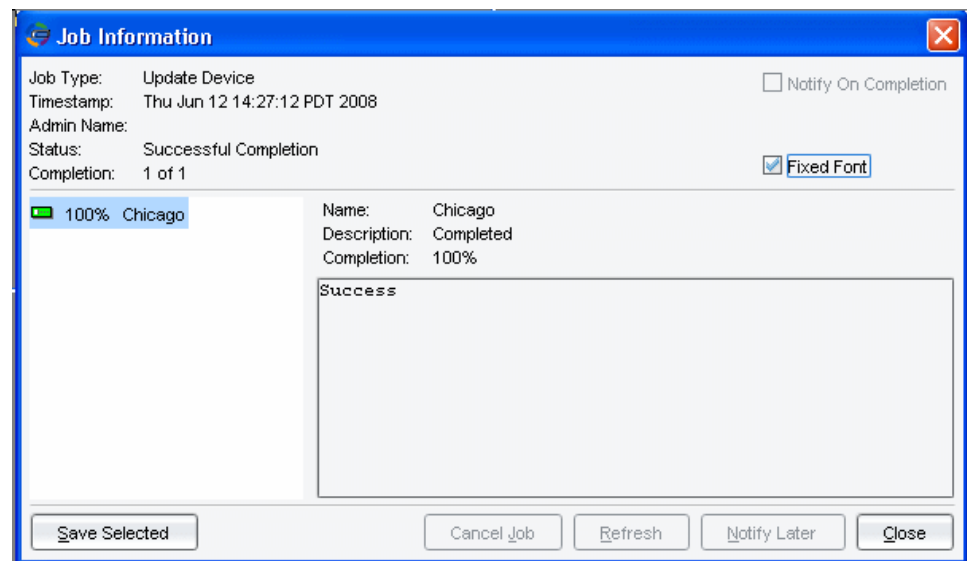
- [About Updating M Series and MX Series Devices on page 31](#)
- [How the Update Process Works on page 32](#)
- [Job Manager on page 33](#)
- [Reviewing Job Information Displayed in Job Manager on page 35](#)

- [Device States Displayed in Job Manager During Update on page 36](#)
- [Understanding Updating Errors Displayed in the Job Manager on page 37](#)

Reviewing Job Information Displayed in Job Manager

The Job Information dialog box displays the changing device states as the directive is executed. Device state changes, error messages, and warning messages are displayed in real time. A sample Job Information dialog box is shown in [Figure 3 on page 35](#).

Figure 3: Job Information Dialog Box



Job Manager tracks the overall progress of one or more jobs executed on a single device. For multiple device updates, Job Manager tracks the progress of each job on each device in addition to the overall progress for all devices. To view the job status for an individual device (including error messages and percent complete), select the device in the Percent Complete pane; the status appears in the Output pane.

The job information includes:

- **Job Type**—The type of task being tracked. Job types include Update Device, Reboot Device, and Config Summary. Job type is also known as a directive.
- **Timestamp**—The time at which NSM began executing the directive.
- **Admin Name**—The name of the administrator logged into NSM.
- **Status**—The current state of the job.
- **Completion**—The number of jobs completed out of the total number of jobs.
- **Percent**—The percentage of total jobs successfully executed. When performing multiple jobs on multiple devices, this field displays the percentage complete for each device. When the job has completed, successfully or unsuccessfully, this field displays 100%.

- Name—The name of the device on which the job is executed.
- Description—The current state of the job.
- Completion—The percentage of a job that has executed successfully.
- Output—Displays the content of the update, including commands that have been interpreted from the NSM data model into device-specific commands, error messages, and existing commands deleted from the device. The Output Display Region displays all errors, warnings, device verification output, and device state information associated with the job.



NOTE: If the Job Information dialog box might contain Chinese, Japanese, or Korean characters, you must clear the Fixed Font box to display them.



NOTE: Job Manager configuration summaries and job information details do not display passwords in the list of CLI commands for administrators that do not have the assigned activity “View Device Passwords.” By default, only the super administrator has this assigned activity.

Related Documentation

- [About Updating M Series and MX Series Devices on page 31](#)
- [How the Update Process Works on page 32](#)
- [Job Manager on page 33](#)
- [Tracking Updated Devices Using Job Manager on page 34](#)
- [Device States Displayed in Job Manager During Update on page 36](#)
- [Understanding Updating Errors Displayed in the Job Manager on page 37](#)

Device States Displayed in Job Manager During Update

During an update, the managed device changes device state. You can view the current device state in real time in the State Description field of the Job Information dialog box. [Table 4 on page 36](#) lists the states that a device can have.

Table 4: Device States During Update

Device State	Description
None	No update activity has occurred on the device.
Loading in Progress	NSM is sending the update image to the flash memory of the device.
Pending	Device is accepting the parameters from the update configuration that has been sent to the device flash memory.

Table 4: Device States During Update (*continued*)

Device State	Description
Converting Data Model to Device Data Model	The parameters that have been set in the NSM configuration are being changed to corresponding device-specific CLI commands that execute on the device.
Successful Completion	Device has successfully been updated with the modeled configuration.
Failed	Device has not been successfully updated with the modeled configuration. The Job Information dialog box displays error messages and error codes.

Related Documentation

- [About Updating M Series and MX Series Devices on page 31](#)
- [How the Update Process Works on page 32](#)
- [Job Manager on page 33](#)
- [Tracking Updated Devices Using Job Manager on page 34](#)
- [Reviewing Job Information Displayed in Job Manager on page 35](#)
- [Understanding Updating Errors Displayed in the Job Manager on page 37](#)

Understanding Updating Errors Displayed in the Job Manager

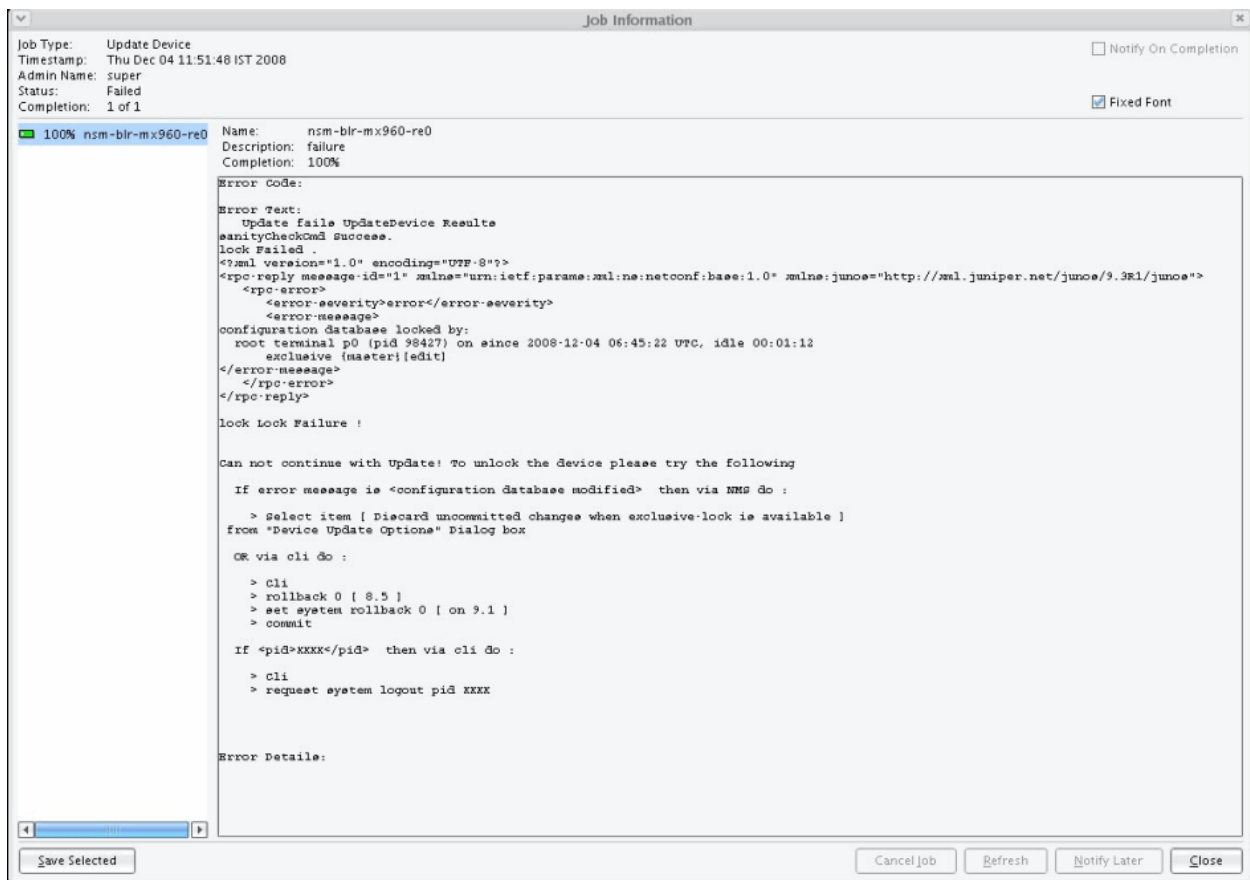
When an update fails for any reason, Job Manager displays error codes and error messages that can help you identify and locate the problem. Typical errors include:

- The modeled configuration contained invalid values that the device could not process.
- During the update process, the connection between the managed device and the Device Server was lost.
- The modeled configuration caused the managed device to lose its connection to NSM.
- An exclusive lock on the configuration prevented NSM from completing an update. This error is specific to devices running the Device Management Interface (DMI), such as the M Series and MX Series devices.

For these update errors, the Job Information dialog box displays the job status as “Failed.”

[Figure 4 on page 38](#) shows that on December 4 a configuration update to an MX960 failed. The super user was locked out by the root user as indicated in the text of the error that shows **lock Failed** and **configuration database locked by: root**. For an M Series or MX Series device, NSM attempts to acquire an exclusive lock on the candidate configuration so that the update can proceed. In this instance, the root user was updating the configuration, probably from the CLI, preventing NSM from locking and successfully updating the configuration.

Figure 4: Failed Update Job Information Dialog Box



In the Job Information dialog box, the update:

- Successfully checked sanity
- Unsuccessfully attempted to lock the configuration that was already locked by the root user

At the end of the error message, there are some suggestions as to how to proceed. In this particular case, the second solution, **> request system logout pid xxxx**, is the appropriate action. From the CLI, the **request system logout pid *pid*** command can be used to forcibly log out the root user. The root user is represented by **pid *pid***, which indicates the user session using the specified management process identifier (PID). After the root user is locked out, you can try to update the configuration again. NSM should lock the configuration and continue successfully.

After a device is updated, you can run a delta configuration summary to determine any remaining differences between the modeled configuration and the running configuration; the output of this summary appears in the Job Information dialog box. For successful updates, no discrepancies are found or displayed. For failed updates, the Job Information dialog box lists the remaining discrepancies.

You can also check the Connection Status and Configuration Status columns for the device in the Realtime Monitor to determine whether the device is running. For more information, see “About the Realtime Monitor.”

**Related
Documentation**

- [About Updating M Series and MX Series Devices on page 31](#)
- [How the Update Process Works on page 32](#)
- [Job Manager on page 33](#)
- [Tracking Updated Devices Using Job Manager on page 34](#)
- [Reviewing Job Information Displayed in Job Manager on page 35](#)
- [Device States Displayed in Job Manager During Update on page 36](#)

PART 3

Configuration

- [Configuration of M Series and MX Series Devices on page 43](#)
- [Configuration of Access on page 49](#)
- [Configuration of Accounting Options on page 75](#)
- [Configuration of Application on page 83](#)
- [Configuration of Bridge Domains on page 85](#)
- [Configuration of Chassis on page 91](#)
- [Configuration of User Authentication on page 107](#)
- [Configuration of Class of Service Features on page 117](#)
- [Configuration of Event Options on page 149](#)
- [Configuration of Firewall on page 157](#)
- [Configuration of Forwarding Options on page 181](#)
- [Configuration of Interfaces on page 207](#)
- [Configuration of Multicast Snooping Options on page 239](#)
- [Configuration of Policy Options on page 243](#)
- [Configuration of Protocols on page 253](#)
- [Configuration of Routing Options on page 365](#)
- [Configuration of Security on page 393](#)
- [Configuration of Services on page 427](#)
- [Configuration of SNMP for Network Management on page 523](#)
- [Configuration of System on page 531](#)

CHAPTER 6

Configuration of M Series and MX Series Devices

- [About Device Configuration on page 43](#)
- [M Series and MX Series Device Configuration Settings Supported in NSM on page 44](#)
- [Configuring Device Features on page 46](#)
- [Example: Configuration of Interfaces for MPLS in the CLI and NSM on page 47](#)

About Device Configuration

This topic does not provide extensive details for configuring features on M Series and MX Series devices in Network and Security Manager (NSM). For detailed information about configuring specific features for M Series and MX Series devices, see the following Junos OS configuration guide:

- *Junos OS System Basics Configuration Guide* for system, chassis, security, and access parameters.
- *Junos OS Network Interfaces Configuration Guide* for interface parameters.
- *Junos OS Framework Configuration Guide* for forwarding options and firewall parameters.
- *Junos OS Configuration and Diagnostic Automation Guide* for event options parameters.
- *Junos OS Network Management Configuration Guide* for SNMP and accounting options parameters.
- *Junos OS Routing Protocols Configuration Guide* for routing options and protocols parameters.
- *Junos OS VPNs Configuration Guide* for policy options parameters.
- *Junos OS Class of Service Configuration Guide* for class of service parameters.
- *Junos OS with Enhanced Services Security Configuration Guide* for security parameters.
- *Junos OS Services Interface Configuration Guide* for service parameters.

For more information about editing device configurations in NSM, including using device templates, using configuration groups, and using configuration groups with templates, see “Configuring Devices” in the *Network and Security Manager Administration Guide*.

Related Documentation

- [M Series and MX Series Device Configuration Settings Supported in NSM on page 44](#)
- [Configuring Device Features on page 46](#)
- [Example: Configuration of Interfaces for MPLS in the CLI and NSM on page 47](#)

M Series and MX Series Device Configuration Settings Supported in NSM

You can configure Junos OS features in NSM. Although the configuration screens rendered in NSM look different than the Junos OS command-line interface (CLI), the top-level configuration elements mostly correspond to commands in the CLI.



NOTE: For detailed information about configuring specific features for M Series and MX Series devices, see the appropriate Junos OS configuration guide.



NOTE: Because the NSM device-side configuration guides are not updated on the same release schedule as the Junos OS releases, consult the Junos OS Documentation for information about configuration settings that might occur in NSM and not in the device-side configuration guides or vice versa.

[Table 5 on page 44](#) provides a general guideline of the CLI hierarchy levels that are supported in the NSM configuration tree. For the exact parameters available, double-click the device in the Device Manager and select the **Configuration** tab. The configuration tree appears in the main display area with all parameters viewable or configurable from NSM.

Table 5: The Junos OS Configuration Hierarchy and the NSM Configuration Tree

Hierarchy Level	Available in the NSM Configuration Tree
edit access	Yes
edit accounting-options	Yes
edit applications	Yes
edit bridge domains	Yes
edit chassis	Yes
edit class-of-service	Yes
edit dynamic profiles	Yes

Table 5: The Junos OS Configuration Hierarchy and the NSM Configuration Tree (continued)

Hierarchy Level	Available in the NSM Configuration Tree
edit ethernet-switching-options	No
edit event-options	Yes
edit firewall	Yes
edit forwarding-options	Yes
edit groups	Yes
edit interfaces	Yes
edit logical-systems	Yes
edit multicast-monitoring-options	Yes
edit poe	No
edit policy-options	Yes
edit protocols	Yes.
edit routing-instances]	Yes
edit routing-options	Yes
edit schedulers	No
edit security	Yes
edit services	Yes
edit snmp	Yes
edit switch-options	Yes
edit system	Yes
edit virtual-chassis	No
edit vlans	No

When you use NSM to edit the software configuration on the device, you initially make the changes to a device object that models the device in NSM. When you are satisfied with your configuration changes, you use the Update Device directive to push the

configuration from the device object in NSM to the device itself. At that point, the edited configuration becomes active.



NOTE: If you import an existing device configuration, NSM automatically imports all objects defined in that configuration.

For more information about editing device configurations, using device templates, using configuration groups, and using configuration groups with templates, see “Configuring Devices” in the *Network and Security Manager Administration Guide*.

**Related
Documentation**

- [About Device Configuration on page 43](#)
- [Configuring Device Features on page 46](#)
- [Example: Configuration of Interfaces for MPLS in the CLI and NSM on page 47](#)

Configuring Device Features

You can configure Junos OS features in NSM. Although the configuration screens rendered in NSM look different than the Junos OS command-line interface (CLI), the top-level configuration elements mostly correspond to commands in the CLI.



NOTE: For detailed information about configuring specific features for M Series and MX Series devices, see the appropriate Junos OS configuration guide.

To configure a device that has been added, imported, or modeled in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. Open the device configuration using one of the following methods:
 - Double-click the device object in the security device tree or the device list.
 - Select the device object and then click the Edit icon.
 - Right-click the device object and select **Edit**.
3. Select the **Configuration** tab.

The device configuration tree appears in the left pane.
4. In the device navigation tree, select a function heading to see device parameters, and then select the configuration parameter you want to configure.
5. Make your changes to the device configuration, then choose one of the following:
 - Click **OK** to save your changes and close the device configuration.
 - Click **Apply** to save your changes and continue making changes.
 - Click **Cancel** to discard all changes and close the device configuration.

To reset a device feature to its default value, right-click on the feature name in the device editor and select **Revert to template/default value**.

Related Documentation

- [About Device Configuration on page 43](#)
- [M Series and MX Series Device Configuration Settings Supported in NSM on page 44](#)
- [Example: Configuration of Interfaces for MPLS in the CLI and NSM on page 47](#)

Example: Configuration of Interfaces for MPLS in the CLI and NSM

With NSM you can manage most of the parameters that you can configure through the CLI. Although the configuration screens rendered in NSM look different, the top-level configuration elements essentially correspond to commands in the CLI. You can configure an M Series or MX Series device using the CLI, then import the configuration into NSM to create a template and apply it to multiple devices.

The following figures show the same configuration displayed in the CLI and the NSM UI. [Figure 5 on page 47](#) shows the CLI configuration of MPLS at the **[edit protocols mpls]** hierarchy level, and [Figure 6 on page 48](#) shows the same configuration in the NSM UI.

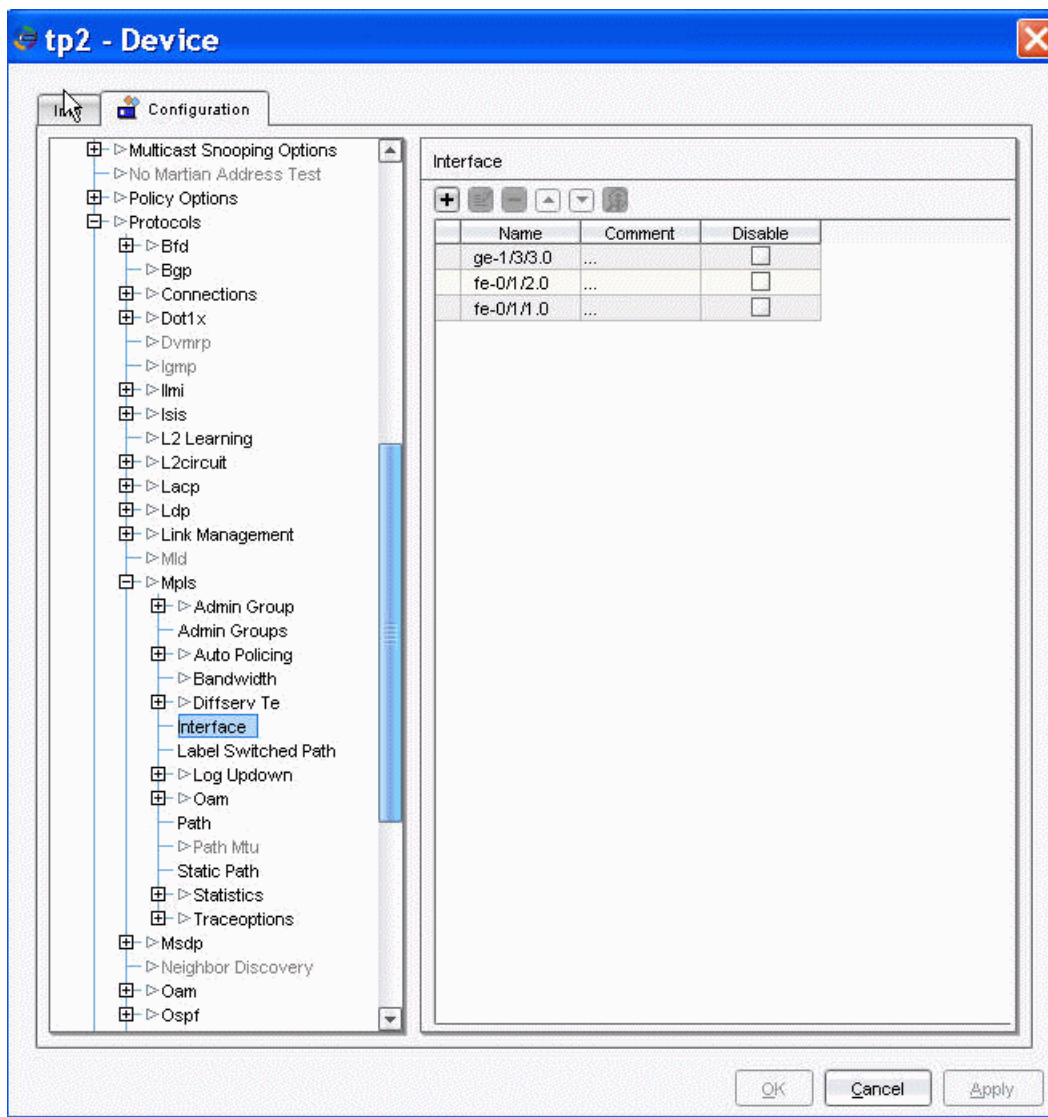
[Figure 5 on page 47](#) shows output for the **show** command in configuration mode. At this level, the **show** command typically displays the entire configuration for the device. For the purpose of this illustration, all parts of the configuration not relevant to our example were removed [...Output Truncated...]. The remaining output shows the protocols and MPLS hierarchy levels. Included at the hierarchy level are three interfaces, two Fast Ethernet interfaces (**fe**) and one Gigabit Ethernet interface (**ge**).

Figure 5: MPLS Configuration in the CLI

```
[edit]
user@host# show
[...Output Truncated...]
protocols {
  mpls {
    interface ge-1/3/3.0;
    interface fe-0/1/2.0;
    interface fe-0/1/1.0;
  }
}
```

[Figure 6 on page 48](#) shows the NSM UI with the same information as in the CLI example. On the left, the Navigation tree is expanded at Protocols, and then further expanded at MPLS, similar to the CLI hierarchy levels. Within MPLS, Interface is highlighted, indicating that the information about the right relates to interfaces within MPLS. The information in the NSM UI example is similar to the information in the CLI example though the presentation is somewhat different.

Figure 6: MPLS Configuration in NSM



In addition, [Figure 6 on page 48](#) shows parts of the configuration tree that appear dim, indicating that those particular parameters are not supported for the M Series and MX Series devices.

Related Documentation

- [About Device Configuration on page 43](#)
- [M Series and MX Series Device Configuration Settings Supported in NSM on page 44](#)
- [Configuring Device Features on page 46](#)

CHAPTER 7

Configuration of Access

- [Configuring Address-Assignment Pools \(NSM Procedure\) on page 49](#)
- [Configuring Access Address Pools \(NSM Procedure\) on page 52](#)
- [Configuring Access Group Profile \(NSM Procedure\) on page 53](#)
- [Configuring the LDAP Options \(NSM Procedure\) on page 54](#)
- [Configuring the LDAP Server \(NSM Procedure\) on page 55](#)
- [Configuring Access Profiles for L2TP or PPP Parameters \(NSM Procedure\) on page 56](#)
- [Configuring the RADIUS Parameters \(NSM Procedure\) on page 70](#)
- [Configuring the RADIUS for Subscriber Access Management, L2TP, or PPP \(NSM Procedure\) on page 71](#)
- [Configuring the SecurID Server \(NSM Procedure\) on page 72](#)
- [Configuring the Access Profile \(NSM Procedure\) on page 73](#)

Configuring Address-Assignment Pools (NSM Procedure)

The address-assignment pool feature supports subscriber management functionality by enabling you to create address pools that can be shared by different client applications. An address-assignment pool can support either IPv4 address or IPv6 addresses. You cannot use the same pool for both types of address.

To configure address assignment pools in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Address Assignment**.
5. Add or modify settings as specified in [Table 6 on page 50](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 6: Address Assignment Configuration Details

Task	Your Action
Configure the name of an address-assignment pool.	<ol style="list-style-type: none"> 1. Click Pool next to Address Assignment. 2. Click Add new entry next to Pool. 3. In the Name box, enter the name to be assigned to the address-assignment pool. 4. In the Comment box, enter the comment.
Configure subnet information for an IPv4 address-assignment pool.	<ol style="list-style-type: none"> 1. Click Family next to Pool. 2. Click Enable Feature check box to enable the option. 3. Click Inet next to Family. 4. In the Comment box, enter the comment. 5. In the Network box, enter the subnet information for an IPv4 address-assignment pool.
Configure address pools that can be used by different client applications.	<ol style="list-style-type: none"> 1. Click Dhcp Attributes next to Inet. 2. In the Comment box, enter the comment. 3. From the Maximum Lease Time list, select the maximum length of time, in seconds, that the lease is held for a client if the client does not renew the lease. This is equivalent to DHCP option 51. 4. From the Grace Period list, select the amount of time that the client retains the address lease after the lease expires. Range: 0 through 4,294,967,295 seconds Default: 0 (no grace period) 5. In the Domain Name box, enter the name of the domain in which clients search for a DHCP server host. 6. In the Boot File box, enter the location of the boot file on the boot server. The filename can include a pathname. 7. In the Boot Server box, enter the name of the boot server advertised to DHCP clients. 8. In the Tftp Server box, enter the IP address of the TFTP server. 9. From the Netbios Node Type list, select one of the following node types. b-node—Broadcast node h-node—Hybrid node m-node—Mixed node p-node—Peer-to-peer node 10. In the Sip Server Domain Name box, enter the domain name of the SIP outbound proxy server.
Configure one or more Domain Name System (DNS) name servers available to the client to resolve hostname-to-client mappings.	<ol style="list-style-type: none"> 1. Click Name Sever next to Dhcp Attributes. 2. Click Add new entry next to Name Server. 3. In the Name box, enter the IP addresses of the domain name servers, listed in order of preference. 4. In the Comment box, enter the comment.

Table 6: Address Assignment Configuration Details (*continued*)

Task	Your Action
Specify user-defined options that are added to client packets.	<ol style="list-style-type: none"> 1. Click Option next to Dhcp Attributes. 2. Click Add new entry next to Option. 3. From the Name list, select the ID number to be used to index the option. 4. In the Comment box, enter the comment. 5. Click Flag next to option. 6. From the Flag list, select the flag type.
Specify a list of match criteria used to determine which named address range in the address-assignment pool to use.	<ol style="list-style-type: none"> 1. Click Option Match next to Dhcp Attributes. 2. In the Comment box, enter the comment. 3. Click Option 82 next to Option Match. 4. In the Comment box, enter the comment. 5. Click Circuit Id next to Option 82. 6. Click Add new entry next to Circuit Id. 7. In the Name box, enter the name of the address-assignment pool range to be used. 8. In the Comment box, enter the comment. 9. In the Range box, enter the range. 10. Click Remote Id next to Option 82. 11. Click Add new entry next to Remote Id. 12. In the Name box, enter the name of the address-assignment pool range to be used. 13. In the Comment box, enter the comment. 14. In the Range box, enter the range.
Specify one or more routers located on the client's subnet.	<ol style="list-style-type: none"> 1. Click Router next to Dhcp Attributes. 2. Click Add new entry next to Router. 3. In the Name box, enter the name of the router. 4. In the Comment box, enter the comment.
Specify SIP Servers list of IPv6 addresses available to the client.	<ol style="list-style-type: none"> 1. Click Sip Server Address next to Dhcp Attributes. 2. Click Add new entry next to Sip Server Address. 3. In the Name box, enter the SIP Servers list of IPv6 addresses available to the client. 4. In the Comment box, enter the comment.
Specify one or more NetBIOS name servers (NBNS) that the client uses to resolve NetBIOS names.	<ol style="list-style-type: none"> 1. Click Wins Server next to Dhcp Attributes. 2. Click Add new entry next to Wins Server. 3. In the Name box, enter the IP address of each NetBIOS name server. 4. In the Comment box, enter the comment.

Table 6: Address Assignment Configuration Details (*continued*)

Task	Your Action
Configure a static binding for the specified client.	<ol style="list-style-type: none"> 1. Click Host next to Inet. 2. Click Add new entry next to Host. 3. In the Name box, enter the name of the client. 4. In the Comment box, enter the comment. 5. In the Hardware Address box, enter the MAC address of the client. 6. In the IP Address box, enter the IP version 4 (IPv4) address.
Configure a named range of IPv4 addresses or IPv6 prefixes, used within an address-assignment pool.	<ol style="list-style-type: none"> 1. Click Range next to Inet. 2. Click Add new entry next to Range. 3. In the Name box, enter the name assigned to the range of IPv4 addresses or IPv6 prefixes. 4. In the Comment box, enter the comment. 5. In the Low box, enter the lower limit of an address range or IPv6 prefix range. 6. In the High box, enter the upper limit of an address range or IPv6 prefix range.

Related Documentation

- [Configuring Access Address Pools \(NSM Procedure\) on page 52](#)
- [Configuring Access Group Profile \(NSM Procedure\) on page 53](#)

Configuring Access Address Pools (NSM Procedure)

With an address pool, you configure an address or address range. When you define an address pool for a client, the layer2 tunneling protocol network server (LNS) allocates IP addresses for clients from an address pool.

To configure access address pools in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Address Pool**.
5. Add or modify settings as specified in [Table 7 on page 53](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 7: Access Address Pool Configuration Details

Task	Your Action
Allocate IP addresses for clients.	<ol style="list-style-type: none"> 1. Click Address Pool next to Access. 2. Click Add new entry next to Address Pool. 3. In the Name box, enter the name to be assigned to an address pool. 4. In the Comment box, enter the comment. 5. Click Address next to address-pool. Select one of the following: <ul style="list-style-type: none"> • Select address to enter the address. Enter the address. • Select address-range to configure the address range. <ol style="list-style-type: none"> a. In the Low box, enter the lower limit of an address range. b. In the High box, enter the upper limit of an address range.

**Related
Documentation**

- [Configuring Address-Assignment Pools \(NSM Procedure\) on page 49](#)
- [Configuring Access Group Profile \(NSM Procedure\) on page 53](#)

Configuring Access Group Profile (NSM Procedure)

You can configure the group profile to define the Point-to-Point Protocol (PPP) using the Group Profile option.

To configure access group profile in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Group Profile**.
5. Add or modify settings as specified in [Table 8 on page 53](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 8: Access Group Profile Configuration Details

Task	Your Action
Configure the group profile.	<ol style="list-style-type: none"> 1. Click Add new entry next to Group Profile. 2. In the Name box, enter the name to be assigned to the group profile. 3. In the Comment box, enter the comment.

Table 8: Access Group Profile Configuration Details (*continued*)

Task	Your Action
Configure the PPP attributes for a group profile.	<ol style="list-style-type: none"> 1. Click Ppp next to group-profile. 2. Select the Enable Feature check box to enable the option. 3. In the Comment box, enter the comment. 4. From the Framed Pool list, select the configured address pool. 5. From the Idle Timeout list, select the number of seconds a user can remain idle before the session is terminated. Range: 0 through 4,294,967,295 seconds Default: 0 6. From the Keep Alive list, select the time period that must elapse before the Junos OS checks the status of the Point-to-Point Protocol (PPP) session by sending an echo request to the peer. Range: 0 through 32,767 seconds Default: 10 7. In the Primary Dns box, enter the primary Domain Name System (DNS) server. 8. In the Secondary Dns box, enter the secondary Domain Name System (DNS) server. 9. In the Primary Wins box, enter the primary Windows Internet name server. 10. In the Secondary Wins box, enter the secondary Windows Internet name server. 11. From the Encapsulation Overhead list, select the number of bytes used as encapsulation overhead for the session. 12. Select the Cell Overhead check box to configure the session to use Asynchronous Transfer Mode (ATM)-aware egress shaping on the IQ2 PIC. 13. In the Interface Id box, enter the interface identifier.

Related Documentation

- [Configuring Access Profiles for L2TP or PPP Parameters \(NSM Procedure\) on page 56](#)

Configuring the LDAP Options (NSM Procedure)

You can configure Lightweight Directory Access Protocols (LDAP) options using the LDAP Options option.

To configure LDAP options in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Ldap Options**.
5. Add or modify settings as specified in [Table 9 on page 55](#).
6. Click one:
 - **OK**—Saves the changes.

- **Cancel**—Cancels the modifications.

Table 9: LDAP Options Configuration Details

Task	Your Action
Configure lightweight directory access protocol options.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment. 2. From the Revert Interval list, select the amount of time the router waits after a server has become unreachable. Range: 60 through 4,294,967,295 Default: 600 3. In the Base Distinguished Name box, enter the suffix when assembling user distinguished name (DN) or base DN under which to search for user DN.
Derive user distinguished name from common-name and base-distinguished-name.	<ol style="list-style-type: none"> 1. Click Assemble next to Ldap Options. 2. Select one of the following: <ul style="list-style-type: none"> • assemble—To derive user distinguished name from common-name and base-distinguished-name. <ol style="list-style-type: none"> a. In the Comment box, enter the comment. b. In the Common Name box, enter the common name. • search—To search for user's distinguished name. <ol style="list-style-type: none"> a. In the Comment box, enter the comment. b. In the Search Filter box, enter the filter to use in search. c. Click Admin Search next to Search. d. In the Comment box, enter the comment. e. In the Distinguished Name box, enter the user distinguished name. f. In the Password box, enter the password.

Related Documentation

- [Configuring the LDAP Server \(NSM Procedure\) on page 55](#)

Configuring the LDAP Server (NSM Procedure)

You can configure the Lightweight Directory Access Protocol (LDAP) server, using the LDAP Server option.

To configure LDAP server:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Ldap Server**.
5. Add or modify settings as specified in [Table 10 on page 56](#).
6. Click one:
 - **OK**—Saves the changes.

- **Cancel**—Cancels the modifications.

Table 10: LDAP Server Configuration Details

Task	Your Action
Configure the LDAP server.	<ol style="list-style-type: none"> 1. Click Add new entry next to Ldap Server. 2. In the Name box, enter the name of the server. 3. In the Comment box, enter the comment. 4. From the Port list, select the port number on which to contact the RADIUS server (LDAP server) 5. In the Source Address box, enter a valid IPv4 address configured on one of the router interfaces. On M Series routers only, the source address can be an IPv6 address and the UDP source port is 514. 6. From the Routing Instances list, select the routing instance name. 7. From the Retry list, select the number of times that the router is allowed to attempt to contact a RADIUS server. Range: 1 through 10 Default: 3 8. From the Timeout list, select the amount of time that the local router waits to receive a response from a RADIUS server. Range: 3 through 90 Default: 5

**Related
Documentation**

- [Configuring LDAP Options \(NSM Procedure\)](#)

Configuring Access Profiles for L2TP or PPP Parameters (NSM Procedure)

You can set up access profiles to validate Layer 2 Tunneling Protocol (L2TP) connections and session requests. You can configure multiple profiles. You can also configure multiple clients for each profile. See the following topics:

1. [Configuring Access Profile \(NSM Procedure\) on page 57](#)
2. [Configuring Accounting Parameters for Access Profiles \(NSM Procedure\) on page 57](#)
3. [Configuring the Accounting Order \(NSM Procedure\) on page 58](#)
4. [Configuring the Authentication Order \(NSM Procedure\) on page 59](#)
5. [Configuring the Authorization Order \(NSM Procedure\) on page 59](#)
6. [Configuring the L2TP Client \(NSM Procedure\) on page 60](#)
7. [Configuring the Client Filter Name \(NSM Procedure\) on page 61](#)
8. [Configuring the LDAP Options \(NSM Procedure\) on page 62](#)
9. [Configuring the LDAP Server \(NSM Procedure\) on page 63](#)
10. [Configuring the Provisioning Order \(NSM Procedure\) on page 64](#)
11. [Configuring RADIUS Parameters for AAA Subscriber Management \(NSM Procedure\) on page 65](#)

12. [Configuring the RADIUS Parameters \(NSM Procedure\) on page 68](#)
13. [Configuring the RADIUS for Subscriber Access Management, L2TP, or PPP \(NSM Procedure\) on page 69](#)
14. [Configuring Session Limit \(NSM Procedure\) on page 69](#)

Configuring Access Profile (NSM Procedure)

To configure an access profile in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in [Table 11 on page 57](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 11: Access Profile Properties Configuration Details

Task	Your Action
Configure access profile properties.	<ol style="list-style-type: none"> 1. Click Add new entry next to Profile. 2. In the Name box, enter the name of the profile. 3. In the Comment box, enter the comment.

Configuring Accounting Parameters for Access Profiles (NSM Procedure)

To configure RADIUS accounting parameters for an access profile in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in [Table 12 on page 58](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 12: Accounting Parameter Configuration Details

Task	Your Action
Configure RADIUS accounting parameters and enable RADIUS accounting for an access profile.	<ol style="list-style-type: none"> 1. Click Add new entry next to Profile. 2. Click Accounting next to profile. 3. In the Comment box, enter the comment. 4. Select the Accounting Stop On Failure check box to configure RADIUS accounting to send an Acct-Stop message when client access fails AAA but the AAA server grants access. 5. Select the Accounting Stop On Access Deny check box to configure RADIUS accounting to send an Acct-Stop message when the AAA server denies a client access. 6. Select the Immediate Update check box to configure the router to send an Acct-Update message to the RADIUS accounting server on receipt of a response (for example, an ACK or timeout) to the Acct-Start message. 7. From the Update Interval list, select the amount of time between updates, in minutes. Range: 10 through 1440 minutes Default: no updates 8. From the Statistics list, select the time statistics for the sessions being managed by AAA.

Configuring the Accounting Order (NSM Procedure)

Beginning with Junos OS Release 8.0, you can configure RADIUS accounting for an Layer 2 Tunneling Protocol (L2TP) profile. With RADIUS accounting enabled, Juniper Networks routers, acting as RADIUS clients, can notify the RADIUS server about user activities such as software logins, configuration changes, and interactive commands. When you enable RADIUS accounting for an L2TP profile, it applies to all the clients within that profile. You must enable RADIUS accounting on at least one L2TP profile for the RADIUS authentication server to send accounting stop and start messages.

To configure accounting order in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in [Table 13 on page 59](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 13: Accounting Order Configuration Details

Task	Your Action
Configure the accounting order.	<ol style="list-style-type: none"> 1. Click Add new entry next to Profile. 2. Click Accounting Order next to Profile. 3. Click Add new entry next to Accounting Order. 4. In the New accounting-order window, select radius to use RADIUS accounting method.

Configuring the Authentication Order (NSM Procedure)

You can configure the order in which the Junos OS tries different authentication methods when authenticating peers. For each access attempt, the software tries the authentication methods in order, from first to last.

To configure authentication order in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in [Table 14 on page 59](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 14: Authentication Order Configuration Details

Task	Your Action
Configure the authentication order.	<ol style="list-style-type: none"> 1. Click Add new entry next to Profile. 2. Click Authentication Order next to Profile. 3. Click Add new entry next to Accounting Order. 4. In the New authentication-order window, select the order in which the Junos OS tries different authentication methods when verifying that a client can access the router.

Configuring the Authorization Order (NSM Procedure)

To configure authorization order in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.

5. Add or modify settings as specified in [Table 15 on page 60](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 15: Authorization Order Configuration Details

Task	Your Action
Configure the authorization order.	<ol style="list-style-type: none"> 1. Click Add new entry next to Profile. 2. Click Authorization Order next to Profile. 3. Click Add new entry next to Authorization Order. 4. In the New authorization-order window, select the authorization order.

Configuring the L2TP Client (NSM Procedure)

To configure the Layer 2 Tunneling Protocol (L2TP) Client in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in [Table 16 on page 60](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 16: Client Configuration Details

Task	Your Action
Configure the client.	<ol style="list-style-type: none"> 1. Click Add new entry next to Profile. 2. Click Client next to Profile. 3. Click Add new entry next to Client. 4. In the Name box, enter the client name. 5. In the Comment box, enter the comment. 6. In the Chap Secret box, enter the secret key associated with a peer. 7. In the pap password box, enter the Password Authentication Protocol (PAP) password.
Configure a client group.	<ol style="list-style-type: none"> 1. Click Client Group next to client. 2. Click Add new entry next to Client Group. 3. In the New client-group window, enter the client group.

Table 16: Client Configuration Details (*continued*)

Task	Your Action
Configure a firewall user.	<ol style="list-style-type: none"> 1. Click Firewall User next to client. 2. In the Comment box, enter the comment. 3. In the Password box, enter the password.
Configure PPP properties for a client profile.	<ol style="list-style-type: none"> 1. Click Ppp next to client. 2. Select ike to configure an IKE access profile. <ol style="list-style-type: none"> a. In the Comment box, enter the comment. b. Select Initiate Dead Peer Detection to detect inactive peers on dynamic IPSec tunnels. c. In the Interface Id box, enter the interface identifier. d. Click Allowed Proxy Pair next to Ike. e. Click Add new entry next to Allowed Proxy Pair. f. In the Local box, enter the network address of the local peer. g. In the Remote box, enter the network address of the remote peer. h. In the Comment box, enter the comment. i. Click Pre Shared Key next to Ike. <ol style="list-style-type: none"> a. Select pre-shared-key to configure the key used to authenticate a dynamic peer during IKE phase 1 negotiation and select the key. b. In the Comment box, enter the comment. c. Click Ascii Text next to Pre Shared key. d. In the ascii-text box, enter the string. e. Select Ike-policy to authenticate dynamic peers during IKE negotiation and select the policy name.

Configuring the Client Filter Name (NSM Procedure)

To configure restrictions on client names in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in [Table 20 on page 64](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 17: Client Filter Name Configuration Details

Task	Your Action
Configure the restrictions on client names.	<ol style="list-style-type: none"> 1. Click Add new entry next to Profile. 2. Click Client Name Filter next to profile. 3. In the Comment box, enter the comment. 4. In the Domain Name box, enter the domain name. 5. In the Separator box, enter the separator character in domain name. 6. From the Count list, select the number of separator instances. Range: 0 through 255

Configuring the LDAP Options (NSM Procedure)

To configure Lightweight Directory Access Protocol (LDAP) options in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in [Table 18 on page 62](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 18: LDAP Options Configuration Details

Task	Your Action
Configure lightweight directory access protocol options.	<ol style="list-style-type: none"> 1. Click Add new entry next to Profile. 2. Click Ldap Options next to profile. 3. In the Comment box, enter the comment. 4. From the Revert Interval list, select the amount of time the router waits after a server has become unreachable. Range: 60 through 4294967295 Default: 600 5. In the Base Distinguished Name box, enter the suffix when assembling user distinguished name (DN) or base DN under which to search for user DN.

Table 18: LDAP Options Configuration Details (*continued*)

Task	Your Action
Derive user distinguished name from common-name and base-distinguished-name.	<ol style="list-style-type: none"> Click Assemble next to Ldap Options. Select one of the following: <ul style="list-style-type: none"> assemble—To derive user distinguished name from common-name and base-distinguished-name. <ol style="list-style-type: none"> In the Comment box, enter the comment. In the Common Name box, enter the common name. search—To search for user's distinguished name. <ol style="list-style-type: none"> In the Comment box, enter the comment. In the Search Filter box, enter the filter to use in search. Click Admin Search next to Search. In the Comment box, enter the comment. In the Distinguished Name box, enter the user distinguished name. In the Password box, enter the password.

Configuring the LDAP Server (NSM Procedure)

To configure Lightweight Directory Access Protocol (LDAP) server in NSM:

- In the NSM navigation tree, select **Device Manager > Devices**.
- Click the **Device Tree** tab, and then double-click the device to select it.
- Click the **Configuration** tab. In the configuration tree, expand **Access**.
- Select **Profile**.
- Add or modify settings as specified in [Table 19 on page 64](#).
- Click one:
 - OK**—Saves the changes.
 - Cancel**—Cancels the modifications.

Table 19: LDAP Server Configuration Details

Task	Your Action
Configure LDAP server.	<ol style="list-style-type: none"> 1. Click Add new entry next to Profile. 2. Click Ldap Server next to profile. 3. Click Add new entry next to Ldap Server. 4. In the Name box, enter the name of the server. 5. In the Comment box, enter the comment. 6. From the Port list, select the port number on which to contact the RADIUS server (LDAP server) 7. In the Source Address box, enter a valid IPv4 address configured on one of the router interfaces. On M Series routers only, the source address can be an IPv6 address and the UDP source port is 514. 8. From the Routing Instances list, select the routing instance name. 9. From the Retry list, select the number of times that the router is allowed to attempt to contact a RADIUS server. Range: 1 through 10 Default: 3 10. From the Timeout list, select the amount of time that the local router waits to receive a response from a RADIUS server. Range: 3 through 90 Default: 5

Configuring the Provisioning Order (NSM Procedure)

To configure the provisioning order in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in [Table 20 on page 64](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 20: Provisioning Order Configuration Details

Task	Your Action
Configure the provisioning order.	<ol style="list-style-type: none"> 1. Click Add new entry next to Profile. 2. Click Provisioning Order next to profile. 3. Click Add new entry next to Provisioning Order. 4. In the New provisioning-order window, select the order in which provisioning mechanisms are used.

Configuring RADIUS Parameters for AAA Subscriber Management (NSM Procedure)

You can specify the RADIUS parameters for the subscriber access manager feature. You can specify the IP addresses of the RADIUS servers used for authentication and accounting, options that provide configuration information for the RADIUS servers, and how RADIUS attributes are used.

To configure RADIUS parameters for AAA subscriber management in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in [Table 21 on page 65](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 21: RADIUS Parameter Configuration Details

Task	Your Action
Configure the RADIUS parameters.	<ol style="list-style-type: none"> 1. Click Add new entry next to Profile. 2. Click Radius next to Profile. 3. In the Comment box, enter the comment.
Specify a list of the RADIUS accounting servers used for accounting for Dynamic Host Configuration Protocol (DHCP), Layer 2 Tunneling Protocol (L2TP), and Point-to-Point Protocol (PPP) clients.	<ol style="list-style-type: none"> 1. Click Attributes next to Radius. 2. In the Comment box, enter the comment.

Table 21: RADIUS Parameter Configuration Details (*continued*)

Task	Your Action
Configure the router to exclude the specified attributes from the specified type of RADIUS message.	<ol style="list-style-type: none"> 1. Click Exclude next to Radius. 2. In the Comment box, enter the comment. 3. From the listed RADIUS attribute type, select the attributes to be excluded. RADIUS attribute types are: <ul style="list-style-type: none"> • accounting-authentic—RADIUS attribute 45, Acct-Authentic • accounting-delay-time—RADIUS attribute 41, Acct-Delay-Time • accounting-session-id—RADIUS attribute 44, Acct-Session-Id • accounting-terminate-cause—RADIUS attribute 49, Acct-Terminate-Cause • called-station-id—RADIUS attribute 30, Called-Station-Id • calling-station-id—RADIUS attribute 31, Calling-Station-Id • class—RADIUS attribute 25, Class • dhcp-gi-address—Juniper VSA 26-57, DHCP-GI-Address • dhcp-mac-address—Juniper VSA 26-56, DHCP-MAC-Address • Dhcp Options—Excludes RADIUS attribute 26-55 • event-timestamp—RADIUS attribute 55, Event-Timestamp • framed-ip-address—RADIUS attribute 8, Framed-IP-Address • framed-ip-netmask—RADIUS attribute 9, Framed-IP-Netmask • input-filter—Juniper VSA 26-10, Ingress-Policy-Name • input-gigapackets—Juniper VSA 26-42, Acct-Input-Gigapackets • input-gigawords—RADIUS attribute 52, Acct-Input-Gigawords • interface-description—Juniper VSA 26-53, Interface-Desc • nas-identifier—RADIUS attribute 32, NAS-Identifier • nas-port—RADIUS attribute 5, NAS-Port • nas-port-id—RADIUS attribute 87, NAS-Port-Id. • nas-port-type—RADIUS attribute 61, NAS-Port-Type • output-filter—Juniper VSA 26-11, Egress-Policy-Name • output-gigapackets—Juniper VSA 25-43, Acct-Output-Gigapackets • output-gigawords—RADIUS attribute 53, Acct-Output-Gigawords

Table 21: RADIUS Parameter Configuration Details (*continued*)

Task	Your Action
Configure the router to ignore the specified attributes in RADIUS Access-Accept messages.	<ol style="list-style-type: none"> 1. Click Ignore next to client. 2. In the Comment box, enter the comment. 3. Select the following check boxes to ignore the specified attributes: <ul style="list-style-type: none"> • output-filter—Egress-Policy-Name (VSA 26-11) • input-filter—Ingress-Policy-Name (VSA 26-10) • framed-ip-netmask—Framed-IP-Netmask (RADIUS attribute 9) • logical-system-routing-instance—Virtual-Router (VSA 26-1)
Specify a list of the RADIUS authentication servers used to authenticate DHCP, L2TP, and PPP clients.	<ol style="list-style-type: none"> 1. Click Authentication Server next to Radius. 2. Click Add new entry next to Authentication Server. 3. In the New authentication-server window, enter the IPv4 address.
Configure the options used by RADIUS authentication and accounting servers.	<ol style="list-style-type: none"> 1. Click Options next to Radius. 2. In the Comment box, enter the comment. 3. Select the Ethernet Port Type Virtual check box to specify a port type of virtual. 4. From the Interface Description Format list, select the information that is included in or omitted from the interface description that the router passes to RADIUS for inclusion in the RADIUS attribute 87 (NAS-Port-Id). Select one of the following: <ul style="list-style-type: none"> • sub-interface—To specify the logical interface. • adapter—To specify the adapter. 5. In the Nas Identifier box, enter a string in the range from 1 to 64 characters. 6. From the Accounting Session Id Format list, select the format the router uses to identify the accounting session. Select one of the following: <ul style="list-style-type: none"> • decimal—To use the decimal format. • description—To use the generic format, in the form <code>jnpr interface-specifier:subscriber-session-id</code>. Default: decimal 7. From the Revert Interval list, select the amount of time the router waits after a server has become unreachable. Range: 60 through 4294967295 seconds Default: 600 seconds 8. Select the vlan-nas-port-stacked-format check box to configure RADIUS attribute 5 (NAS-Port) to include the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces.

Table 21: RADIUS Parameter Configuration Details (*continued*)

Task	Your Action
Configure the RADIUS client to use the extended format for RADIUS attribute 5 (NAS-Port) and specify the width of the fields in the NAS-Port attribute.	<ol style="list-style-type: none"> 1. Click Nas Port Extended Format next to Options. 2. In the Comment box, enter the comment. 3. From the Slot Width list, select the number of bits in the slot field. 4. From the Adapter Width list, select the number of bits in the adapter field. 5. From the Port Width list, select the number of bits in the port field. 6. From the Stacked Vlan Width list, select the number of bits in the SVLAN ID field. 7. From the Vlan Width list, select the number of bits in the VLAN ID field.

Configuring the RADIUS Parameters (NSM Procedure)

You can specify the options used by the RADIUS authentication and accounting servers.

To configure the RADIUS parameters in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in [Table 22 on page 68](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.



NOTE: To create a profile, the device should be in the in-device policy mode.

Table 22: RADIUS Parameters Configuration Details

Task	Your Action
Configure the RADIUS parameters.	<ol style="list-style-type: none"> 1. Click Add new entry next to Profile. 2. Click Radius Options next to Profile. 3. In the Comment box, enter the comment. 4. From the Revert Interval list, select the amount of time the router waits after a server has become unreachable. Default: 600 seconds

Configuring the RADIUS for Subscriber Access Management, L2TP, or PPP (NSM Procedure)

You can configure RADIUS for subscriber access management, L2TP, or PPP. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.

To configure the RADIUS server in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in [Table 23 on page 69](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 23: RADIUS Server Configuration Details

Task	Your Action
Configure the RADIUS servers.	<ol style="list-style-type: none"> 1. Click Add new entry next to Profile 2. Click Radius Server next to Profile. 3. In the Name box, enter the profile name. 4. In the Comment box, enter the comment. 5. From the Port list, select the port number on which to contact the RADIUS server. Default: 1812 (as specified in RFC 2865) 6. In the Secret box, enter the password to use with the RADIUS server. The secret password used by the local router must match that used by the server. 7. From the Timeout list, select the amount of time that the local router waits to receive a response from a RADIUS server. Range: 3 through 90 seconds Default: 3 seconds 8. From the Retry list, select the number of times that the router is allowed to attempt to contact a RADIUS server. Range: 1 through 10 Default: 3 9. In the Source Address box, enter a valid IPv4 address configured on one of the router interfaces. 10. From the Routing Instance list, select the routing instance name.

Configuring Session Limit (NSM Procedure)

To configure the timeout limit in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in [Table 24 on page 70](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 24: Session Limit Configuration Details

Task	Your Action
Configure the timeout interval.	<ol style="list-style-type: none"> 1. Click Add new entry next to Profile. 2. Click Session Options next to Profile. 3. In the Comment box, enter the comment. 4. From the Client Idle Timeout list, select the time in minutes of idleness after which access is denied. Range: 1 through 255 minutes 5. From the Client Session Timeout list, select the time in minutes since initial access after which access is denied.
Configure a client group.	<ol style="list-style-type: none"> 1. Click Client Group next to Session Option. 2. Click Add new entry next to Client Group. 3. In the New client-group window, enter the client group.

Configuring the RADIUS Parameters (NSM Procedure)

You can specify the options used by the RADIUS authentication and accounting servers.

To configure the RADIUS parameters in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in [Table 22 on page 68](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.



NOTE: To create a profile, the device should be in the in-device policy mode.

Table 25: RADIUS Parameters Configuration Details

Task	Your Action
Configure the RADIUS parameters.	<ol style="list-style-type: none"> 1. Click Add new entry next to Profile. 2. Click Radius Options next to Profile. 3. In the Comment box, enter the comment. 4. From the Revert Interval list, select the amount of time the router waits after a server has become unreachable. Default: 600 seconds

Configuring the RADIUS for Subscriber Access Management, L2TP, or PPP (NSM Procedure)

You can configure RADIUS for subscriber access management, layer 2 tunneling protocol (L2TP), or point-to-point protocol (PPP). The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.

To configure the RADIUS server in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Radius Server**.
5. Add or modify settings as specified in [Table 26 on page 72](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 26: RADIUS Server Configuration Details

Task	Your Action
Configure the RADIUS servers.	<ol style="list-style-type: none"> 1. Click Add new entry next to Radius Server 2. In the Name box, enter the profile name. 3. In the Comment box, enter the comment. 4. From the Accounting Port list, select the port number on which to contact the accounting server. Default: 1813 (as specified in RFC 2865) 5. From the Port list, select the port number on which to contact the RADIUS server. Default: 1812 (as specified in RFC 2865) 6. In the Secret box, enter the password to use with the RADIUS server. The secret password used by the local router must match that used by the server. 7. From the Timeout list, select the amount of time that the local router waits to receive a response from a RADIUS server. Range: 1 through 90 seconds Default: 3 seconds 8. From the Retry list, select the number of times that the router is allowed to attempt to contact a RADIUS server. Range: 1 through 10 Default: 3 9. In the Source Address box, enter a valid IPv4 address configured on one of the router interfaces. 10. From the Routing Instance list, select the routing instance name.

Related Documentation

- [Configuring the RADIUS Parameters \(NSM Procedure\) on page 68](#)

Configuring the SecurID Server (NSM Procedure)

You can configure the SecurID server using the Securid Server option.

To configure the SecurID server in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Securid Server**.
5. Add or modify settings as specified in [Table 27 on page 73](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 27: SecurID Server Configuration Details

Task	Your Action
Configure the SecurID server.	<ol style="list-style-type: none"> 1. Click Add new entry next to Securid Server 2. In the Name box, enter the name of the SecurID server. 3. In the Comment box, enter the comment. 4. In the Configuration File box, enter the path to the SecurID server configuration (sdconf.rec) file.

Related Documentation • [Configuring the RADIUS for Subscriber Access Management, L2TP, or PPP \(NSM Procedure\) on page 71](#)

Configuring the Access Profile (NSM Procedure)

To configure the access profile in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, select **Access Profile**.
4. Add or modify settings as specified in [Table 28 on page 73](#).
5. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 28: Access Profile Configuration Details

Task	Your Action
Configuring the access profile.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment. 2. In the Name box, enter the name of the access profile.

Related Documentation • [Configuring Access Profiles for L2TP or PPP Parameters \(NSM Procedure\) on page 56](#)
 • [Configuring the RADIUS Parameters \(NSM Procedure\) on page 68](#)

CHAPTER 8

Configuration of Accounting Options

- [Configuring Accounting Options \(NSM Procedure\) on page 75](#)

Configuring Accounting Options (NSM Procedure)

An accounting profile represents common characteristics of collected accounting data. You can configure multiple accounting profiles using this option. See the following topics:

- [Configuring Class Usage Profiles \(NSM Procedure\) on page 75](#)
- [Configuring a Log File \(NSM Procedure\) on page 76](#)
- [Configuring the Filter Profile \(NSM Procedure\) on page 77](#)
- [Configuring the Interface Profile \(NSM Procedure\) on page 78](#)
- [Configuring the Policy Decision Statistics Profile \(NSM Procedure\) on page 79](#)
- [Configuring the MIB Profile \(NSM Procedure\) on page 80](#)
- [Configuring the Routing Engine Profile \(NSM Procedure\) on page 81](#)

Configuring Class Usage Profiles (NSM Procedure)

You can configure the class usage profile to collect statistics for particular source and destination classes.

To configure class usage profiles in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Accounting Options**.
4. Select **Class Usage Profile**.
5. Add or modify the settings as specified in [Table 29 on page 76](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 29: Class Usage Profile Configuration Details

Task	Your Action
Configure the class usage profile.	<ol style="list-style-type: none"> 1. Click Add new entry next to Class Usage Profile. 2. Expand class-usage-profile. 3. In the Name box, enter the name of the destination class profile. 4. In the Comment box, enter the comment for the class usage profile. 5. In the File box, enter the name of the log file. 6. From the Interval list, select the amount of time between each collection of statistics. Range: 1 through 1048576 minutes Default: 30 minutes 7. Click Destination Classes next to class-usage-profile and select one of the following: <ul style="list-style-type: none"> • destination-classes—To configure the class usage profile to filter by source classes. • source-classes—To configure the class usage profile to filter by destination classes. 8. In the Name box, enter the name of the source classes or the destination classes. 9. In the Comment box, enter the comment.

Configuring a Log File (NSM Procedure)

An accounting profile specifies what statistics should be collected and written to a log file. You can configure an accounting-data log file using this option.

To configure a log file in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Accounting Options**.
4. Select **File**.
5. Add or modify the settings as specified in [Table 30 on page 77](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 30: Log File Configuration Details

Task	Your Action
Configure an accounting-data log file.	<ol style="list-style-type: none"> 1. Click Add new entry next to File. 2. In the Name box, enter the filename. 3. In the Comment box, enter the comment for the file. 4. In the Size box, enter the maximum size of each log file in the range from 262144 through 1073741824 bytes. 5. From the Files list, select the maximum number of files. Range: 1 through 1000 Default : 10 6. From the Transfer Interval list, select the time the file remains open and receives new statistics before it is closed and transferred to an archive site. Range: 5 through 2880 minutes Default: 30 minutes 7. In the Start Time box, enter the start time for transfer of an accounting-data log file in the format <i>yyyy-mm-dd.hh:mm</i>
Configure archive sites.	<ol style="list-style-type: none"> 1. Click Add new entry next to Archive Sites. 2. In the Name box, enter the site name. 3. In the Comment box, enter the comment. 4. In the Password box, enter the password.

Configuring the Filter Profile (NSM Procedure)

A filter profile specifies error and statistics information collected and written to a file. A filter profile must specify counter names for which statistics are collected.

To configure the filter profile in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Accounting Options**.
4. Select **Filter Profile**.
5. Add or modify the settings as specified in [Table 31 on page 78](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 31: Filter Profile Configuration Details

Task	Your Action
Configure a filter profile.	<ol style="list-style-type: none"> 1. Click Add new entry next to Filter Profile. 2. Expand filter-profile. 3. In the Name box, enter the filename. 4. In the Comment box, enter the comment for the file. 5. In the File box, enter the name of the file. 6. From the Interval list, select the amount of time between each collection of statistics. Range: 1 through 1048576 minutes Default: 30 minutes
Configure the counters.	<ol style="list-style-type: none"> 1. Click Counters next to filter-profile. 2. Click Add new entry next to Counters. 3. In the Name box, enter the site name. 4. In the Comment box, enter the comment.

Configuring the Interface Profile (NSM Procedure)

An interface profile specifies the information collected and written to a log file. You can configure a profile to collect error and statistic information for input and output packets on a particular physical or logical interface.

To configure the interface profile in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Accounting Options**.
4. Select **Interface Profile**.
5. Add or modify the settings as specified in [Table 32 on page 79](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 32: Interface Profile Configuration Details

Task	Your Action
Configure an interface profile.	<ol style="list-style-type: none"> 1. Click Add new entry next to Interface Profile. 2. Expand interface-profile. 3. In the Name box, enter the name of the log file. 4. In the Comment box, enter the comment for the interface profile. 5. In the File box, enter the name of the log file. 6. From the Interval list, select the amount of time between each collection of statistics. Range: 1 through 2880 minutes Default: 30 minutes
Configure the statistics to be collected in an accounting-data log file for an interface.	<ol style="list-style-type: none"> 1. Click Fields next to interface-profile. 2. In the Comment box, enter the comment. 3. Select the corresponding field name: <ul style="list-style-type: none"> • Input Bytes—Input bytes • Output Bytes—Output bytes • Input Packets—Input packets • Output Packets—Output packets • Input Errors—Generic input error packets • Output Errors—Generic output error packets • Input Multicast—Input packets arriving by multicast • Output Multicast—Output packets sent by multicast • Input Unicast—Input unicast packets • Output Unicast—Output unicast packets • Unsupported Protocol—Log Packets of unsupported protocols • Rpf Check Bytes—Number of bytes that have failed the RPF check • Rpf Check Packets—Number of packets that have failed the RPF check • Rpf Check6 Bytes—Log number of bytes that have failed the IPv6 reverse-path-forwarding check • Rpf Check6 Packets—Log number of packets that have failed the IPv6 reverse-path-forwarding check

Configuring the Policy Decision Statistics Profile (NSM Procedure)

The policy decision statistics profile collects the statistical records and formats for the local policy decision function (L-PDF) and logs them to specified file. The `aacl-fields` under the policy decision statistics profile specifies the files according to which the statistics will be collected.

To configure the policy decision statistics profile in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.

3. Click the **Configuration** tab. In the configuration tree, expand **Accounting Options**.
4. Select **Policy Decision Statistics Profile**.
5. Add or modify the settings as specified in [Table 33 on page 80](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 33: Policy Decision Statistics Profile Configuration Details

Task	Your Action
Configure policy decision statistics profile.	<ol style="list-style-type: none"> 1. Click Add new entry next to Policy Decision Statistics Profile. 2. Expand policy-decision-statistics-profile. 3. In the Name box, enter the name of the policy decision statistics profile. 4. In the Comment box, enter the comment for the policy decision statistics profile. 5. In the File box, enter the name of the log file.
Configure application awareness access list.	<ol style="list-style-type: none"> 1. Click Application Awareness Access List next to policy-decision-statistics-profile. 2. Select the name of the field: <ul style="list-style-type: none"> • address—Address of subscriber • application—Application • application-group—Application group • input-bytes—Input bytes • input-interface—Interface of subscriber • input-packets—Input packets • mask—Mask of subscriber • output-bytes—Output bytes • output-packets—Output packets • subscriber-name—Name of subscriber • timestamp—Timestamp of statistics record • vrf-name—VRF where subscriber resides

Configuring the MIB Profile (NSM Procedure)

The MIB profile collects MIB statistics and logs them to a file. The MIB profile specifies the SNMP operation and MIB object names for which statistics are collected.

To configure the MIB profile in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Accounting Options**.
4. Select **MIB Profile**.

5. Add or modify the settings as specified in [Table 34 on page 81](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 34: MIB Profile Configuration Details

Task	Your Action
Configure mib profile.	<ol style="list-style-type: none"> 1. Click Add new entry next to Mib Profile. 2. Expand mib-profile. 3. In the Name box, enter the name of the MIB statistics profile. 4. In the Comment box, enter the comment for the MIB profile. 5. In the File box, enter the name of the log file. 6. From the Interval list, select the amount of time between each collection of statistics. Range: 1 through 2880 minutes Default: 30 minutes 7. From the Operation list, select the name of the operation to use. You can select a get, get-next, or walk operation. Default: walk
Configure the name of the MIB objects for which MIB statistics are collected for an accounting-data log file.	<ol style="list-style-type: none"> 1. Click Object Names next to mib-profile. 2. In the Name box, enter the name of a MIB object. You can specify more than one MIB object name. 3. In the Comment box, enter the comment.

Configuring the Routing Engine Profile (NSM Procedure)

The Routing Engine profile collects Routing Engine statistics and logs them to a file. The Routing Engine profile specifies the fields for which statistics are collected

To configure the Routing Engine profile in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Accounting Options**.
4. Select **Routing Engine Profile**.
5. Add or modify the settings as specified in [Table 35 on page 82](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 35: Routing Engine Profile Configuration Details

Task	Your Action
Configure Routing Engine profile.	<ol style="list-style-type: none"> 1. Click Add new entry next to Routing Engine Profile. 2. Expand routing-engine-profile. 3. In the Name box, enter the name of the Routing Engine statistics profile. 4. In the Comment box, enter the comment for the routing engine profile. 5. In the File box, enter the name of the log file. 6. From the Interval list, select the amount of time between each collection of statistics. Range: 1 through 2880 minutes Default: 30 minutes
Configure the statistics to collect in an accounting-data log file for a Routing Engine.	<ol style="list-style-type: none"> 1. Click Fields next to routing-engine-profile. 2. In the Comment box, enter the comment. 3. Select the name of the field: <ul style="list-style-type: none"> • host-name—Hostname for the router. • date—Date, in <i>yyyymmdd</i> format. • time-of-day—Time of day, in <i>hhmmss</i> format. • uptime—Time since last reboot, in seconds. • cpu-load-1—Average system load over the last 1 minute. • cpu-load-5—Average system load over the last 5 minutes. • cpu-load-15—Average system load over the last 15 minutes. • Memory Usage—Memory usage in bytes. • Total Cpu Usage—Amount of CPU time used.

Configuration of Application

- [Configuring the Application and Application Set \(NSM Procedure\)](#) on page 83

Configuring the Application and Application Set (NSM Procedure)

You can define application protocols for the stateful firewall and Network Address Translation (NAT) services to use in match condition rules. An application protocol, or application layer gateway (ALG), defines application parameters using information from network Layer 3 and above. You can configure properties of an application and whether to include it in an application set using the application option. You can configure one or more applications to include in an application set using the application set option.

To configure an application set in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Applications**.
4. Add or modify settings as specified in [Table 36 on page 84](#).
5. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.



NOTE: Application and application set are configurable, only if the device is in the in-device policy mode.

Table 36: Applications Configuration Details

Task	Your Action
Configure properties of an application and whether to include it in an application set.	<ol style="list-style-type: none"> 1. Click Application next to Applications. 2. Click Add new entry next to Application. 3. In the Name box, enter the identifier of the application. 4. In the Comment box, enter the comment. 5. From the Application Protocol list, select the name of the protocol. 6. From the Protocol list, select the networking protocol type. 7. From the Source Port list, select the identifier for the port. 8. From the Destination Port list, select the Identifier for the port. 9. From the Snmp Command list, select the SNMP command format. 10. From the Icmp Type list, select the ICMP packet type value. 11. From the Icmp Code list, select the Internet Control Message Protocol (ICMP) code value. 12. From the Ttl Threshold list, select the TTL threshold value. 13. In the Rpc Program number box, enter the Remote procedure call (RPC) or Distributed Computing Environment (DCE) value. Range: 100,000 through 400,000 14. In the Uuid box, enter the Universal Unique Identifier (UUID) for DCE RPC objects. 15. From the Inactivity Timeout list, select the length of time the application is inactive before it times out. 16. Select the Learn Sip Register check box to activate SIP register to accept potential incoming SIP calls. 17. From the Sip Call Hold Timeout list select the length of time the application holds a SIP call open before it times out. Default: 7200 seconds Range: 0 through 36,000 seconds (10 hours) 18. Select one of the following: <ul style="list-style-type: none"> • do-not-translate-AAAA-query-to-A-query—To control the translation of AAAA query to A query. • do-not-translate-A-query-to-AAAA—To control the translation of A query to AAAA query.
Configuring application sets.	<ol style="list-style-type: none"> 1. Click Application Set next to Applications. 2. Click Add new entry next to Application Set. 3. Expand application-set. 4. In the Name box, enter the identifier of an application set. 5. In the Comment box, enter the comment. 6. Click Application next to application-set. 7. Click Add new entry next to Application. 8. From the Name list, select the identifier of the application. 9. In the Comment box, enter the comment.

CHAPTER 10

Configuration of Bridge Domains

- [Configuring Bridge Domains Properties \(NSM Procedure\) on page 85](#)

Configuring Bridge Domains Properties (NSM Procedure)

You can configure the bridge domain properties using the following options. See the following topics:

- [Configuring Logical Interfaces \(NSM Procedure\) on page 85](#)
- [Configuring Multicast Monitoring Options \(NSM Procedure\) on page 86](#)
- [Configuring VLAN ID \(NSM Procedure\) on page 89](#)

Configuring Logical Interfaces (NSM Procedure)

You can specify the logical interfaces to include in the bridge domain, VPLS instance, or virtual switch.

To configure logical interfaces in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Bridge Domains**.
4. Select **Domain**.
5. Add or modify settings as specified in [Table 37 on page 86](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 37: Logical Interface Configuration Details

Task	Your Action
Configure logical interface to include in the bridge domain, VPLS instance, or virtual switch.	<ol style="list-style-type: none">1. Click Add new entry next to Domain.2. Click Interface.3. Click Add new entry next to Interface.4. From the Name list, select the name of a logical interface.5. In the Comment box, enter the comment.

Configuring Multicast Monitoring Options (NSM Procedure)

Multicast monitoring is a way for a Layer 2 device to monitor at the Layer 3 packet content to determine which actions are to be taken to process or forward a frame. There are specific forms of monitoring, such as IGMP monitoring or PIM monitoring. In all cases, monitoring involves a device configured to function at Layer 2 having access to Layer 3 (packet) information. monitoring makes multicasting more efficient in these devices.

To configure Multicast Monitoring:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Bridge Domains**.
4. Select **Domain**.
5. Add or modify the settings as specified in [Table 38 on page 87](#).
6. Click one:
 - OK—saves the changes
 - Cancel—cancels the modifications

Table 38: Multicast Monitoring Options Configuration Details

Task	Your Action
Establish multicast monitoring option values.	<ol style="list-style-type: none"> 1. Click Add new entry next to Domain. 2. Click Multicastmonitoring Options next to domain.
Establish a list of flood group addresses for multicast monitoring.	<ol style="list-style-type: none"> 1. Click Flood Groups next to Multicast Monitoring Options. 2. Click Add new entry next to Flood Groups. 3. In the dialog box, enter the IP addresses.
Configure multicast forwarding cache properties.	<ol style="list-style-type: none"> 1. Click Forwarding Cache next to Multicast Monitoring Options. 2. In the Comment box, enter the comments. 3. Expand Forwarding Cache. 4. Click Threshold next to Forwarding Cache. 5. In the Comment box, enter the comments. 6. From the Suppress list, select the threshold value for a forwarding cache. Range: 1 through 200,000 7. From the Reuse list, select the reuse value for the threshold. The reuse value must be less than the suppression threshold value. Range: 1 through 200,000
Establish the graceful restart duration for multicast monitoring.	<ol style="list-style-type: none"> 1. Click Graceful Restart next to Multicast Monitoring Options. 2. In the Comment box, enter the comments. 3. From the Restart Duration list, select the duration for graceful restart. Range: 0 to 300 seconds Default : 180 seconds

Table 38: Multicast Monitoring Options Configuration Details (*continued*)

Task	Your Action
Establish multicast monitoring option values.	<ol style="list-style-type: none"> 1. Click Option next to Multicast Monitoring Options. 2. In the Comment box, enter the comments. 3. Expand Options. 4. Click Syslog next to Options. 5. In the Comment box, enter the comments. 6. From the Upto list, select the level up to which severity the messages are to be system logged. 7. From the Mark list, select the time interval in seconds to mark the trace file. Range : -2147483647 seconds to 2147483647 Seconds Default : 0 8. Expand Syslog. 9. Click Level next to Syslog. 10. Select the Level of severity to be logged.
Configure tracing options.	<ol style="list-style-type: none"> 1. Click Traceoptions next to Multicast Monitoring Options. 2. In the Comment box, enter the comments. 3. Expand Traceoptions. 4. Click File next to Trace Options. 5. In the Comment box, enter the comments. 6. In the Filename box, enter the name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. 7. In the Size box, enter the maximum size of each trace file in bytes. Range : 10240 to 4,294,967,295 bytes 8. From the Files list, select the maximum number of files. 9. Select one of the following: <ul style="list-style-type: none"> • world-readable—To enable log file access to all users. • no-world-readable—To prevent all users from reading the log file. 10. Click Flag next to Trace Options. 11. Click Add new entry next to flag. 12. From the Name list, select a tracing operation to perform. 13. In the Comment box, enter the comments.

Configuring VLAN ID (NSM Procedure)

You can configure VLAN IDs using the Vlan Id option.

To configure VLAN ID in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Bridge Domains**.
4. Select **Domain**.
5. Add or modify settings as specified in [Table 39 on page 89](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 39: VLAN ID Configuration Details

Task	Your Action
Configure a VLAN ID	<ol style="list-style-type: none">1. Click Add new entry next to Domain.2. Click Vlan Id.3. Select vlan-id and enter the VLAN ID.4. Select vlan tag to tag the VLAN interface so that it can be compared with the normalizing VLAN identifier.5. In the Comment box, enter the comment.6. In the Inner box, enter the VLAN identifier.7. In the Outer box, enter the VLAN identifier.

Configuration of Chassis

- [Configuring Aggregated Devices \(NSM Procedure\) on page 91](#)
- [Configuring Chassis Alarms \(NSM Procedure\) on page 92](#)
- [Configuring Container Interfaces \(NSM Procedure\) on page 93](#)
- [Configuring Chassis FPC \(NSM Procedure\) on page 94](#)
- [Configuring a T640 Router on a Routing Matrix \(NSM Procedure\) on page 99](#)
- [Configuring Routing Engine Redundancy \(NSM Procedure\) on page 104](#)
- [Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors \(NSM Procedure\) on page 105](#)

Configuring Aggregated Devices (NSM Procedure)

The Junos OS supports the aggregation of physical devices into the defined virtual links, such as the link aggregation of Ethernet interfaces defined by the IEEE 802.3ad standard. You can configure the properties for Ethernet and sonet aggregated devices on the router.

To configure the aggregated devices on the router:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Chassis > Aggregated Devices**.
4. Add or modify the settings as specified in [Table 40 on page 92](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 40: Aggregated Devices Configuration Details

Task	Your Action
Configure properties for Ethernet aggregated devices.	<ol style="list-style-type: none"> 1. Click Ethernet next to Aggregated Devices. 2. Enter the number of aggregated logical devices available to the router. Range: 1 through 256 devices 3. Click Lacp next to Ethernet. 4. In the System Priority box, enter the priority for the aggregated Ethernet system. 5. Click Link Protection next to Lacp. 6. Select the Non Revertive check box if you want to disable the ability to switch to a better priority link (if one is available) once a link is established as active and a collection or distribution is enabled.
Configure properties for sonet aggregated devices.	<ol style="list-style-type: none"> 1. Click Sonet next to Aggregated Devices. 2. From the Device Count list, select the number of aggregated logical devices available to the router. Range: 1 through 16 Devices

Related Documentation

- [Configuring Chassis Alarms \(NSM Procedure\) on page 92](#)
- [Configuring a T640 Router on a Routing Matrix \(NSM Procedure\) on page 99](#)
- [Configuring Routing Engine Redundancy \(NSM Procedure\) on page 104](#)
- [Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors \(NSM Procedure\) on page 105](#)

Configuring Chassis Alarms (NSM Procedure)

You can configure the chassis alarms for an interface type to trigger a red or yellow alarm or to ignore an alarm. Various conditions related to the chassis components trigger yellow and red alarms.

To configure chassis alarm on the router:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Chassis > Alarm**.
4. Add or modify the alarm settings as specified in [Table 41 on page 93](#).
5. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 41: Chassis Alarms Configuration Details

Task	Your Action
Configuring the alarm type.	<ol style="list-style-type: none"> 1. Select the interface type listed next to Alarm. 2. Select the alarm type for the chassis condition for each interface type.

Related Documentation

- [Configuring Aggregated Devices \(NSM Procedure\) on page 91](#)
- [Configuring Chassis FPC \(NSM Procedure\) on page 94](#)
- [Configuring Routing Engine Redundancy \(NSM Procedure\) on page 104](#)

Configuring Container Interfaces (NSM Procedure)

To configure a container interface, you must first create the number of container devices that you require. You can create up to a maximum of 128 container interfaces per router using the Container Interfaces option.

To configure container interfaces in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Chassis**.
4. Select **Container Devices**.
5. Add or modify settings as specified in [Table 42 on page 93](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 42: Container Interfaces Configuration Details

Task	Your Action
Specify the container devices configuration.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment. 2. From the Device list, select the number of container devices. Range: 1 through 128

Related Documentation

- [Configuring Aggregated Devices \(NSM Procedure\) on page 91](#)
- [Configuring Chassis FPC \(NSM Procedure\) on page 94](#)

Configuring Chassis FPC (NSM Procedure)

For MX Series routers, there is a one-to-one mapping of the Packet Forwarding Engines and the PICs. Therefore, you can override the port-mirroring instance properties configured at the DPC level and configure a PIC-level port-mirroring instance. To bind a port-mirroring instance to a specific Packet Forwarding Engine and its associated ports, you can use this option.

You can also configure aggregate ports, maximum queue per interface, and tunneling services for PICs.

To configure chassis FPC in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Chassis > Fpc**.
4. Add or modify settings as specified in [Table 43 on page 94](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 43: FPC Configuration Details

Task	Your Action
Configure a port-mirroring instance for the DPC and its corresponding Packet Forwarding Engines.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. From the Name list, select the slot number of the DPC. 3. From the Power list, configure the Flexible PIC Concentrator (FPC) to stay offline or to come online automatically.

Table 43: FPC Configuration Details (*continued*)

Task	Your Action
Configure aggregate port, maximum queues per interface and port mirroring instances for the PICs.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Pic next to fpc. 3. Click Add new entry next to Pic. 4. From the Name list, select the slot number of the DPC. 5. In the Comment box, enter the comment. 6. From the Framing list, select the framing type. 7. From the Vtmapping list, select one of the virtual tributary mapping. <ul style="list-style-type: none"> • klm—KLM standard. • itu-t—International Telephony Union standard. 8. Select the No Concatenate check box to not concatenate (multiplex) the output of a SONET/SDH PIC (an interface with a name so-fpc/pic/port). 9. Select the Aggregate Ports check box if you want to aggregate multiple ports on a PIC as a single port. 10. Select the Sparse Dlcis check box to support a full data-link connection identifier (DLCI) range (1 through 1022). 11. From the Mlfr Uni Nni Bundles list, select the number of multilink frame relay user-to-network interface network-to-network interface (UNI-NNI) (FRF.16) bundles to allocate on a link services PIC. Range: 1 through 255 12. From the Max Queues Per Interface list, select the required egress queues on IQ interfaces.
Enable a service package on adaptive services interfaces.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Pic next to fpc. 3. Click Add new entry next to Pic. 4. Click Adaptive Services next to pic. 5. Select Adaptive Services to enable a service package on adaptive services interfaces.
Configure channelized E1 port and channel specifications.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Pic next to fpc. 3. Click Add new entry next to pic. 4. Click Ce1 next to pic. 5. In the Comment box, enter the comment. 6. Click E1 next to Ce1. 7. Click Add new entry next to E1. 8. From the Name list, select the port number. 9. In the Comment box, enter the comment. 10. Click Channel Group next to e1. 11. Click Add new entry next to Channel Group. 12. From the Name list, select the channel number. 13. In the Comment box, enter the comment. 14. In the Timeslots box, enter the actual time slot number.

Table 43: FPC Configuration Details (*continued*)

Task	Your Action
Configure channelized T3 port and channel specifications.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Pic next to fpc. 3. Click Add new entry next to Pic. 4. Click Ct3 next to pic. 5. In the Comment box, enter the comment. 6. Click Port next to Ct3. 7. Click Add new entry next to Port. 8. From the Name list, select the port number. 9. In the Comment box, enter the comment. 10. Click T1 next to Port. 11. Click Add new entry next to T1. 12. From the Name list, select the link number. 13. In the Comment box, enter the comment. 14. Click Channel Group next to t1. 15. Click Add new entry next to Channel Group. 16. From the Name list, select the channel number. 17. In the Comment box, enter the comment. 18. In the Timeslots box, enter the actual time slot number.
Configure data used in a hash key for a protocol family.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Pic next to fpc. 3. Click Add new entry next to Pic. 4. Click Hash Key next to pic. 5. In the Comment box, enter the comment. 6. Click Family next to Hash Key. 7. In the Comment box, enter the comment.
Configure data used in a hash key for the Inet protocol family when configuring PIC-level symmetrical load balancing on an 802.3ad link aggregation group.	<ol style="list-style-type: none"> 1. Click Inet next to Family. 2. In the Comment box, enter the comment. 3. Click Layer 3 next to Inet. 4. In the Comment box, enter the comment. 5. Select the Destination Address check box to compute symmetrical hashing based on the destination address. 6. Click Layer 4 next to Inet. 7. In the Comment box, enter the comment. 8. Click Symmetric Hash next to Inet. 9. In the Comment box, enter the comment. 10. Select the Complement check box to include the complement of the symmetric hash in the hash key.

Table 43: FPC Configuration Details (*continued*)

Task	Your Action
Configure data used in a hash key for the multiservice protocol family when configuring PIC-level symmetrical hashing for load balancing on an 802.3ad link aggregation group.	<ol style="list-style-type: none"> 1. Click Multiservice next to Family. 2. In the Comment box, enter the comment. 3. Select the Source Mac check box to include source MAC address in the hash key. 4. Select the Destination Mac check box to include destination MAC address in the hash key. 5. Click Payload next to Multiservice. 6. Click IP next to Payload. 7. In the Comment box, enter the comment. 8. Select the Layer 4 check box to include Layer 4 IP information in the hash key. 9. Click Layer 3 next to IP. 10. Select one of the following: <ul style="list-style-type: none"> • source-ip-only—To include source IP only in hash-key. • destination-ip-only—To include destination IP only in hash-key. 11. Click Symmetric Hash next to Multiservice. 12. In the Comment box, enter the comment. 13. Select the Complement check box to include the complement of the symmetric hash in the hash key.
Configure the channelized T3 port number on the PIC.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Pic next to fpc. 3. Click Add new entry next to Pic. 4. Click Port next to pic. 5. From the Name list, select the port number. 6. In the Comment box, enter the comment. 7. From the Framing list, select the framing type.
Configure delay buffers.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Pic next to fpc. 3. Click Add new entry next to Pic. 4. Click Q Pic Large Buffer next to pic. 5. In the Comment box, enter the comment.
Configure port-mirroring instances.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Pic next to fpc. 3. Click Add new entry next to Pic. 4. Click Port Mirror Instance next to pic and perform the following: <ul style="list-style-type: none"> • Add—Adds the selected port-mirroring instances from the Non member list to the Members list. • Remove—Removes the selected port-mirroring instances from the Members list. • Add All—Adds all the port-mirroring instances from the Non-members list to the Members list. • Remove All—Removes all the port-mirroring instances from the Members list.

Table 43: FPC Configuration Details (*continued*)

Task	Your Action
Enable shaping on an L2TP session.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Pic next to fpc. 3. Click Add new entry next to Pic. 4. Click Traffic Manager next to pic. 5. From the Ingress Shaping Overhead list, select the number of CoS shaping overhead bytes to add to the packets on the ingress side of the L2TP tunnel to determine the shaped session packet length. Range: 0 through 255 6. From the Egress Shaping Overhead list, select the number of CoS shaping overhead bytes to add to the packets on the egress interface. Range: 0 through 255 7. From the Mode list, select the mode of shaping.
Configure the amount of bandwidth for tunnel services.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Pic next to fpc. 3. Click Add new entry next to Pic. 4. Click Tunnel Service next to pic. 5. From the Bandwidth list, select the bandwidth of 1 Gbps or 10 Gbps on the Packet Forwarding Engine connected to a Gigabit Ethernet 40-port DPC.
Configure Port-Mirroring Instances.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Port Mirror Instance next to fpc and perform the following: <ul style="list-style-type: none"> • Add—Adds the selected port-mirroring instances from the Non member list to the Members list. • Remove—Removes the selected port-mirroring instances from the Members list. • Add All—Adds all the port-mirroring instances from the Non-members list to the Members list. • Remove All—Removes all the port-mirroring instances from the Members list.
Associate a sampling instance.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Sampling Instances next to fpc. 3. Click Add new entry next to Sampling Instances. 4. From the Name list, select the sampling instance name. 5. In the Comment box, enter the comment.

Related Documentation

- [Configuring Aggregated Devices \(NSM Procedure\) on page 91](#)
- [Configuring Chassis Alarms \(NSM Procedure\) on page 92](#)
- [Configuring a T640 Router on a Routing Matrix \(NSM Procedure\) on page 99](#)

Configuring a T640 Router on a Routing Matrix (NSM Procedure)

To configure a T640 router on a routing matrix in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Chassis > Lcc**.
4. Add or modify settings as specified in [Table 44 on page 99](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 44: Lcc Configuration Details

Task	Your Action
Configure the T640 routing node.	<ol style="list-style-type: none"> 1. Click Add new entry next to Lcc. 2. From the Name list, select the number that specifies a T640 router on a routing matrix. Range: 0 through 3 3. In the Comment box, enter the comment. 4. Select one of the following: <ul style="list-style-type: none"> • online-expected—On a TX Matrix router, configures a T640 router so that if it does not come online, an alarm is sent to the TX Matrix router. On a TX Matrix Plus router, configure a T1600 router so that if it does not come online, an alarm is sent to the TX Matrix Plus router. • offline—On a TX Matrix router, configures a T640 router so that it is not part of the routing matrix. On a TX Matrix Plus router, configure a T1600 router so that it is not part of the routing matrix.
Configure a port-mirroring instance for the DPC and its corresponding Packet Forwarding Engines.	<ol style="list-style-type: none"> 1. Click Fpc next to Lcc. 2. Click Add new entry next to Fpc. 3. From the Name list, select the slot number of the DPC. 4. From the Power list, configure the Flexible PIC Concentrator (FPC) to stay offline or to come online automatically.

Table 44: Lcc Configuration Details (*continued*)

Task	Your Action
Configures aggregate port, maximum queues per interface and port-mirroring instances for the PICs.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Pic next to fpc. 3. Click Add new entry next to PIC. 4. From the Name list, select the slot number of the DPC. 5. In the Comment box, enter the comment. 6. From the Framing list, select the framing type. 7. From the Vtmapping list, select one of the virtual tributary mapping. <ul style="list-style-type: none"> • klm—KLM standard. • itu-t—International Telephony Union standard. 8. Select the No Concatenate check box to not concatenate (multiplex) the output of a SONET/SDH PIC (an interface with a name so-fpc/pic/port). 9. Select the Aggregate Ports check box if you want to aggregate multiple ports on a PIC as a single port. 10. Select the Sparse Dlcis check box to support a full data-link connection identifier (DLCI) range (1 through 1022). 11. From the Mlfr Uni Nni Bundles list, select the number of multilink frame relay user-to-network interface network-to-network interface (UNI-NNI) (FRF.16) bundles to allocate on a Link Services PIC. Range: 1 through 255 12. From the Max Queues Per Interface list, select the required egress queues on IQ interfaces.
Enable a service package on adaptive services interfaces.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Pic next to fpc. 3. Click Add new entry next to Pic. 4. Click Adaptive Services next to pic. 5. Choose Adaptive Services to enable a service package on adaptive services interfaces.
Configure channelized E1 port and channel specifications.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Pic next to fpc. 3. Click Add new entry next to pic. 4. Click Ce1 next to pic. 5. In the Comment box, enter the comment. 6. Click E1 next to Ce1. 7. Click Add new entry next to E1. 8. From the Name list, select the port number. 9. In the Comment box, enter the comment. 10. Click Channel Group next to e1. 11. Click Add new entry next to Channel Group. 12. From the Name list, select the channel number. 13. In the Comment box, enter the comment. 14. In the Timeslots box, enter the actual time slot number.

Table 44: Lcc Configuration Details (*continued*)

Task	Your Action
Configure channelized T3 port and channel specifications.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Pic next to fpc. 3. Click Add new entry next to Pic. 4. Click Ct3 next to pic. 5. In the Comment box, enter the comment. 6. Click Port next to Ct3. 7. Click Add new entry next to Port. 8. From the Name list, select the port number. 9. In the Comment box, enter the comment. 10. Click T1 next to Port. 11. Click Add new entry next to T1. 12. From the Name list, select the link number. 13. In the Comment box, enter the comment. 14. Click Channel Group next to t1. 15. Click Add new entry next to Channel Group. 16. From the Name list, select the channel number. 17. In the Comment box, enter the comment. 18. In the Timeslots box, enter the actual time slot number.
Configure data used in a hash key for a protocol family.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Pic next to fpc. 3. Click Add new entry next to Pic. 4. Click Hash Key next to pic. 5. In the Comment box, enter the comment. 6. Click Family next to Hash Key. 7. In the Comment box, enter the comment.
Configure data used in a hash key for the Inet protocol family when configuring PIC-level symmetrical load balancing on an 802.3ad link aggregation group.	<ol style="list-style-type: none"> 1. Click Inet next to Family. 2. In the Comment box, enter the comment. 3. Click Layer 3 next to Inet. 4. In the Comment box, enter the comment. 5. Select the Destination Address check box to compute symmetrical hashing based on the destination address. 6. Click Layer 4 next to Inet. 7. In the Comment box, enter the comment. 8. Click Symmetric Hash next to Inet. 9. In the Comment box, enter the comment. 10. Select the Complement check box to include the complement of the symmetric hash in the hash key.

Table 44: Lcc Configuration Details (*continued*)

Task	Your Action
Configure data used in a hash key for the multiservice protocol family when configuring PIC-level symmetrical hashing for load balancing on an 802.3ad link aggregation group.	<ol style="list-style-type: none"> 1. Click Multiservice next to Family. 2. In the Comment box, enter the comment. 3. Select the Source Mac check box to include source MAC address in the hash key. 4. Select the Destination Mac check box to include destination MAC address in the hash key. 5. Click Payload next to Multiservice. 6. Click IP next to Payload. 7. In the Comment box, enter the comment. 8. Select the Layer 4 check box to include Layer 4 IP information in the hash key. 9. Click Layer 3 next to IP. 10. Select one of the following: <ul style="list-style-type: none"> • source-ip-only—To include source IP only in hash-key. • destination-ip-only—To include destination IP only in hash-key. 11. Click Symmetric Hash next to Multiservice. 12. In the Comment box, enter the comment. 13. Select the Complement check box to include the complement of the symmetric hash in the hash key.
Configure the channelized T3 port number on the PIC.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Pic next to fpc. 3. Click Add new entry next to Pic. 4. Click Port next to pic. 5. From the Name list, select the port number. 6. In the Comment box, enter the comment. 7. From the Framing list, select the framing type.
Configure delay buffers.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Pic next to fpc. 3. Click Add new entry next to Pic. 4. Click Q Pic Large Buffer next to pic. 5. In the Comment box, enter the comment.
Configure port-mirroring instances for PIC.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Pic next to fpc. 3. Click Add new entry next to Pic. 4. Click Port Mirror Instance next to pic and perform the following: <ul style="list-style-type: none"> • Add—Adds the selected port-mirroring instances from the Non member list to the Members list. • Remove—Removes the selected port-mirroring instances from the Members list. • Add All—Adds all the port-mirroring instances from the Non-members list to the Members list. • Remove All—Removes all the port-mirroring instances from the Members list.

Table 44: Lcc Configuration Details (*continued*)

Task	Your Action
Enable shaping on an L2TP session.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Pic next to fpc. 3. Click Add new entry next to Pic. 4. Click Traffic Manager next to pic. 5. From the Ingress Shaping Overhead list, select the number of CoS shaping overhead bytes to add to the packets on the ingress side of the L2TP tunnel to determine the shaped session packet length. Range: 0 through 255 6. From the Egress Shaping Overhead list, select the number of CoS shaping overhead bytes to add to the packets on the egress interface. Range: 0 through 255 7. From the Mode list, select the mode of shaping.
Configure the amount of bandwidth for tunnel services.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Pic next to fpc. 3. Click Add new entry next to Pic. 4. Click Tunnel Service next to pic. 5. From the Bandwidth list, select the bandwidth of 1 Gbps or 10 Gbps on the Packet Forwarding Engine connected to a Gigabit Ethernet 40-port DPC.
Configure port-mirroring instances for FPC.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Port Mirror Instance next to fpc and perform the following: <ul style="list-style-type: none"> • Add—Adds the selected port-mirroring instances from the Non member list to the Members list. • Remove—Removes the selected port-mirroring instances from the Members list. • Add All—Adds all the port-mirroring instances from the Non-members list to the Members list. • Remove All—Removes all the port-mirroring instances from the Members list.
Associate a sampling instance.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fpc. 2. Click Sampling Instances next to fpc. 3. Click Add new entry next to Sampling Instances. 4. From the Name list, select the sampling instance name. 5. In the Comment box, enter the comment.

Related Documentation

- [Configuring Aggregated Devices \(NSM Procedure\) on page 91](#)
- [Configuring Routing Engine Redundancy \(NSM Procedure\) on page 104](#)
- [Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors \(NSM Procedure\) on page 105](#)

Configuring Routing Engine Redundancy (NSM Procedure)

You can configure redundancy properties for routers that have multiple Routing Engines or these multiple switching control boards: Switching and Forwarding Modules (SFMs), System and Switch Boards (SSBs), Forwarding Engine Boards (FEBs), or Compact Forwarding Engine Boards (CFEBs).

To configure routing engine redundancy in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, select **Chassis > Redundancy**.
4. Add or modify settings as specified in [Table 45 on page 104](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 45: Chassis Redundancy Configuration Details

Task	Your Action
Configure redundancy options.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment. 2. From the keepalive list, select the time before the backup router takes mastership when it detects loss of the keepalive signal. Range: 2 through 10,000
Instruct the backup router to take mastership if it detects hard disk errors or a loss of a keepalive signal from the master Routing Engine.	<ol style="list-style-type: none"> 1. Click Failover next to Redundancy. 2. In the Comment box, enter the comment. 3. Select the type of failover.
For routing platforms with two Routing Engines, configure a master Routing Engine to switch over gracefully to a backup Routing Engine without interruption to packet forwarding.	<ol style="list-style-type: none"> 1. Click Graceful Switchover next to Redundancy. 2. In the Comment box, enter the comment.

Table 45: Chassis Redundancy Configuration Details (*continued*)

Task	Your Action
Sets the function of the Routing Engine for the specified slot. By default, the Routing Engine in slot 0 is the master Routing Engine and the Routing Engine in slot 1 is the backup Routing Engine.	<ol style="list-style-type: none"> 1. Click Routing Engine next to Redundancy. 2. From the Name list, select the slot number. 3. In the Comment box, enter the comment. 4. Select the function of the Routing Engine for the specified slot. 5. Select one of the following: <ul style="list-style-type: none"> • master—To configure the routing engine to be the master. • backup—To configure the routing engine to be the backup. • disabled—To disable the routing engine.

- Related Documentation**
- [Configuring Aggregated Devices \(NSM Procedure\) on page 91](#)
 - [Configuring a T640 Router on a Routing Matrix \(NSM Procedure\) on page 99](#)
 - [Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors \(NSM Procedure\) on page 105](#)

Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors (NSM Procedure)

You can configure a Routing Engine to halt or reboot automatically when a hard disk error occurs. A hard disk error may cause a Routing Engine to enter a state in which it responds to local pings and interfaces remain up, but no other processes are responding.

To Configure Routing Engine to reboot or halt:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, select **Chassis > Routing Engine**.
4. Add or modify Routing Engine settings as specified in [Table 46 on page 105](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 46: Chassis Routing Engine Configuration Details

Option	Your Action
On disk failure.	From the Disk Failure Action list, select the action to instruct the router on detecting the hard disk errors on the Routing Engine.

- Related Documentation**
- [Configuring Aggregated Devices \(NSM Procedure\) on page 91](#)
 - [Configuring a T640 Router on a Routing Matrix \(NSM Procedure\) on page 99](#)
 - [Configuring Routing Engine Redundancy \(NSM Procedure\) on page 104](#)

Configuration of User Authentication

- [Configuring RADIUS Authentication \(NSM Procedure\) on page 107](#)
- [Configuring TACACS+ Authentication \(NSM Procedure\) on page 108](#)
- [Configuring Authentication Order \(NSM Procedure\) on page 109](#)
- [Configuring User Access \(NSM Procedure\) on page 110](#)
- [Configuring Template Accounts \(NSM Procedure\) on page 113](#)

Configuring RADIUS Authentication (NSM Procedure)

To use RADIUS authentication, you must configure at least one RADIUS server. Configuring RADIUS authentication involves identifying the RADIUS server, specifying the secret (password) of the RADIUS server, and setting the source address of the device's RADIUS requests to the loopback address of the device.

To configure RADIUS authentication:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure RADIUS authentication.
3. Click the **Configuration** tab. In the configuration tree, select **System > Radius Server**.
4. Add or modify Radius settings as specified in [Table 47 on page 107](#).
5. Click one:
 - **New**—Adds a new RADIUS server.
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 47: RADIUS Authentication Configuration Details

Option	Function	Your Action
Name	Specifies the IP address of the RADIUS server.	Enter the IP address of the RADIUS server.

Table 47: RADIUS Authentication Configuration Details (*continued*)

Option	Function	Your Action
Secret	Specifies the shared secret (password) of the RADIUS server. The secret is stored as an encrypted value in the configuration database.	Enter the shared secret of the RADIUS server.
Source Address	Specifies the source address to be included in the RADIUS server requests by the device. In most cases, you can use the loopback address of the device.	Enter the loopback address of the device.

Related Documentation

- [Configuring TACACS+ Authentication \(NSM Procedure\) on page 108](#)
- [Configuring Authentication Order \(NSM Procedure\) on page 109](#)
- [Configuring User Access \(NSM Procedure\) on page 110](#)

Configuring TACACS+ Authentication (NSM Procedure)

To use TACACS+ authentication, you must configure at least one TACACS+ server. Configuring TACACS+ authentication involves identifying the TACACS+ server, specifying the secret (password) of the TACACS+ server, and setting the source address of the device's TACACS+ requests to the loopback address of the device.

To configure TACACS+ authentication:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab and then double-click the device for which you want to configure TACACS+ authentication.
3. Click the **Configuration** tab. In the configuration tree, select **System > TACACS+ Server**.
4. Add or modify TACACS+ settings as specified in [Table 48 on page 108](#).
5. Click one:
 - **New**—Adds a new TACACS+ server.
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 48: TACACS+ Authentication Configuration Details

Option	Function	Your Action
Name	Specifies the IP address of the TACACS+ server.	Enter the IP address of the TACACS+ server.
Secret	Specifies the shared secret (password) of the TACACS+ server. The secret is stored as an encrypted value in the configuration database.	Enter the shared secret of the TACACS+ server.

Table 48: TACACS+ Authentication Configuration Details (*continued*)

Option	Function	Your Action
Source Address	Specifies the source address to be included in the TACACS+ server requests by the device. In most cases, you can use the loopback address of the device.	Enter the loopback address of the device.

Related Documentation

- [Configuring RADIUS Authentication \(NSM Procedure\) on page 107](#)
- [Configuring Authentication Order \(NSM Procedure\) on page 109](#)
- [Configuring User Access \(NSM Procedure\) on page 110](#)

Configuring Authentication Order (NSM Procedure)

You can configure the device so that user authentication occurs with the local password first, then with the RADIUS server, and finally with the TACACS+ server.

To configure authentication order:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab and then double-click the device for which you want to configure authentication order.
3. Click the **Configuration** tab. In the configuration tree, select **System > Authentication Order**.
4. In the Authentication Order workspace, click the **New** button. The New authentication-order list appears.
5. To add RADIUS authentication to the authentication order, select **radius** from the New authentication-order list.
6. To add TACACS+ authentication to the authentication order, select **tacplus** from the New authentication-order list.
7. To add Password authentication to the authentication order, select **password** from the New authentication-order list.
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Related Documentation

- [Configuring RADIUS Authentication \(NSM Procedure\) on page 107](#)
- [Configuring TACACS+ Authentication \(NSM Procedure\) on page 108](#)
- [Configuring User Access \(NSM Procedure\) on page 110](#)

Configuring User Access (NSM Procedure)

This section includes the following topics:

- [Configuring Login Classes on page 110](#)
- [Configuring User Accounts on page 112](#)

Configuring Login Classes

You can define any number of login classes and then apply one login class to an individual user account. All users who can log in to the router must be in a login class. With login classes, you define the following:

- Access privileges users have when they are logged in to the router
- Commands and statements that users can and cannot specify
- How long a login session can be idle before it times out and the user is logged out

To configure login classes:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab and then double-click the device for which you want to configure a login class.
3. Click the **Configuration** tab. In the configuration tree, select **System>Login>Class**.
4. Add or modify login class settings as specified in [Table 49 on page 110](#).
5. Click one:
 - **New**—Adds a new login class.
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Search**—Search a login class.

Table 49: Login Class Authentication Configuration Details

Option	Function	Your Action
Class		
Name	Specifies a name for the login class.	Enter a name for the login class.
Comment	Specifies the comment added to the class.	Enter a comment.
Access Start	Specifies the start time for remote access.	Enter the start time for remote access in hh:mm format.
Access End	Specifies the end time for remote access.	Enter the end time for remote access in hh:mm format.

Table 49: Login Class Authentication Configuration Details (*continued*)

Option	Function	Your Action
Idle Timeout	Specifies the maximum idle time before logout.	Enter the maximum idle time before logout in minutes.
Login Alarms	Displays the system alarms when logging in.	–
Login Script	Executes the login-script when logging in.	–
Login Tip	Displays tips when logging in.	–
Allow Commands	Specifies the operational mode commands that members of a login class can use.	Enter the command name enclosed in quotation marks. For example, " request system reboot ".
Deny Commands	Specifies the regular expression for commands to deny explicitly.	Enter the command name enclosed in quotation marks. For example, " (show system statistics) (show bgp summary) ".
Allow Configuration	Specifies the regular expression for configure to be allowed explicitly.	Enter the configuration in quotation marks. For example, " regular expression 1 ".
Deny Configuration	Specifies the regular expression for configure to be denied explicitly.	Enter the configuration in quotation marks. For example, " system services ".
Security Roles	Specifies the common criteria for security role.	<p>The options available are:</p> <ul style="list-style-type: none"> • none • audit-administrator • crypto-administrator • ids-administrator • security-administrator
Login > Class > Allow Configuration Regexp		
Allow Configuration Regexp	Specifies the object path regular expressions to be allowed.	Enter a regular expression string. For example, " interfaces.* description.* "interfaces.* unit.* description.* "interfaces.* unit.* family inet address.* "interfaces.* disable" ".
Login > Class > Allowed Days		
Allowed Days	Specifies the day(s) of week when access is allowed.	Select the day(s) from the drop down box. For example, Monday .
Login > Class > Deny Configuration Regexp		

Table 49: Login Class Authentication Configuration Details (*continued*)

Option	Function	Your Action
Deny Configuration Regular Expressions	Specifies the object path regular expressions to be denied.	Enter the regular expression string. For example, " system " " protocols ".
Login > Class > Permissions		
Permissions	Configures the login access privileges to be provided on the device.	Enter a new permission.

Configuring User Accounts

User accounts provide one way for users to access the device. (Users can access the router without accounts if you configured RADIUS or TACACS+ servers.) For each account, define the login name for the user and, optionally, information that identifies the user. After you have created an account, a home directory is created for the user.

To configure user accounts:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab and then double-click the device for which you want to configure login class.
3. Click the **Configuration** tab. In the configuration tree, select **System > Login > User**.
4. Add or modify login class settings as specified in [Table 50 on page 112](#).
5. Click one:
 - **New**—Adds a new user account.
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Search**—Search the available login classes.

Table 50: User Authentication Configuration Details

Option	Function	Your Action
Name	Identifies the user with a unique name.	Enter a unique name for the user.
Comment	Specifies the comment added to the login class.	Enter a comment.
Full Name	Specifies the full name of the user.	Enter the full name.
Uid	Specifies the user identifier.	Enter an user ID. For example, 100...64000 .

Table 50: User Authentication Configuration Details (*continued*)

Option	Function	Your Action
Class	Specifies the user's login class.	Select the class name.
Login > User > Authentication		
Plain Text Password Value	Specifies the user's password.	Enter the plain text password for the user.
Login > User > Authentication > Ssh DSA		
Ssh DSA	Specifies the secure shell (ssh) DSA public key string.	Enter a DSA public key string.
Name	Specifies the name of the DSA public string.	Enter an unique name for the DSA public string.
Comment	Specifies the comment added to the ssh data.	Enter a comment.
From	Specifies the pattern-list of hosts allowed.	—
Login > User > Authentication > Ssh Rsa		
Ssh RSA	Specifies the secure shell (ssh) RSA public key string.	Enter a RSA public key string.
Name	Specifies the name of the RSA public string.	Enter an unique name for the RSA public string.
Comment	Specifies the comment added to the RSA data.	Enter a comment.
From	Specifies the pattern-list of hosts allowed.	—

Related Documentation

- [Configuring RADIUS Authentication \(NSM Procedure\) on page 107](#)
- [Configuring TACACS+ Authentication \(NSM Procedure\) on page 108](#)
- [Configuring Authentication Order \(NSM Procedure\) on page 109](#)

Configuring Template Accounts (NSM Procedure)

You can create template accounts that are shared by a set of users when you are using RADIUS or TACACS+ authentication. When a user is authenticated by a template account,

the CLI username is the login name, and the privileges, file ownership, and effective user ID are inherited from the template account.

To configure template accounts, follow these procedures:

- [Creating a Remote Template Account on page 114](#)
- [Creating a Local Template Account on page 115](#)

Creating a Remote Template Account

You can create a remote template that is applied to users authenticated by RADIUS or TACACS+ that do not belong to a local template account.

By default, Junos OS with enhanced services uses the remote template account when:

- The authenticated user does not exist locally on the Services Router.
- The authenticated user's record in the RADIUS or TACACS+ server specifies local user, or the specified local user does not exist locally on the device.

The following procedure creates a sample user named remote that belongs to the operator login class.

To create a remote template account:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab and then double-click the device for which you want to create a remote template account.
3. Click the **Configuration** tab. In the configuration tree, select **System > Login > User**.
4. Add or modify login class settings as specified in [Table 51 on page 114](#).
5. Click one:
 - **New**—Creates a new remote template account.
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 51: Remote Template Account Details

Option	Function	Your Action
Name	Specifies a name for the user name.	Enter the user name. For example, type remote .
Uid	Specifies the user identifier for a login account.	Enter the number associated with the login account.
Class	Specifies the login class for the user.	Select the login class. For example, select operator .

Creating a Local Template Account

You can create a local template that is applied to users authenticated by RADIUS or TACACS+ that are assigned to the local template account. You use local template accounts when you need different types of templates. Each template can define a different set of permissions appropriate for the group of users who use that template.

The following procedure creates a sample user named admin that belongs to the superuser login class.

To create a local template account:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab and then double-click the device for which you want to create a local template account.
3. Click the **Configuration** tab. In the configuration tree, select **System > Login > User**.
4. Add or modify login class settings as specified in [Table 52 on page 115](#).
5. Click one:
 - **New**—Creates a new local template account.
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 52: Local Template Account Details

Option	Function	Your Action
Name	Specifies a name for the user name.	Enter the user name. For example, type admin .
Uid	Specifies the user identifier for a login account.	Enter the number associated with the login account.
Class	Specifies the login class for the user.	Select the login class. For example, select superuser .

Related Documentation

- [Configuring RADIUS Authentication \(NSM Procedure\) on page 107](#)
- [Configuring TACACS+ Authentication \(NSM Procedure\) on page 108](#)
- [Configuring Authentication Order \(NSM Procedure\) on page 109](#)

CHAPTER 13

Configuration of Class of Service Features

- [Configuring CoS Classifiers \(NSM Procedure\) on page 118](#)
- [Configuring CoS Code Point Aliases \(NSM Procedure\) on page 120](#)
- [Configuring CoS Drop Profile \(NSM Procedure\) on page 121](#)
- [Configuring CoS Forwarding Classes \(NSM Procedure\) on page 123](#)
- [Configuring CoS Forwarding Policy \(NSM Procedure\) on page 125](#)
- [Configuring CoS Fragmentation Maps \(NSM Procedure\) on page 126](#)
- [Configuring CoS Host Outbound Traffic \(NSM Procedure\) on page 127](#)
- [Configuring CoS Interfaces \(NSM Procedure\) on page 128](#)
- [Configuring CoS Rewrite Rules \(NSM Procedure\) on page 134](#)
- [Configuring CoS Routing Instances \(NSM Procedure\) on page 137](#)
- [Configuring CoS Schedulers \(NSM Procedure\) on page 138](#)
- [Configuring CoS and Applying Scheduler Maps \(NSM Procedure\) on page 140](#)
- [Configuring CoS Restricted Queues \(NSM Procedure\) on page 141](#)
- [Configuring Tracing Operations \(NSM Procedure\) on page 142](#)
- [Configuring CoS Traffic Control Profiles \(NSM Procedure\) on page 143](#)
- [Configuring CoS Translation Table \(NSM Procedure\) on page 144](#)

Configuring CoS Classifiers (NSM Procedure)

Packet classification associates incoming packets with a particular class-of-service (Cos) servicing level. Classifiers associate packets with a forwarding class and loss priority and, based on the associated forwarding class, assign packets to output queues. Junos OS supports two general types of classifiers:

- Behavior aggregate or CoS value traffic classifiers—Examines the CoS value in the packet header. The value in this single field determines the CoS settings applied to the packet. BA classifiers allow you to set the forwarding class and loss priority of a packet based on the Differentiated Services code point (DSCP) value, IP precedence value, and IEEE 802.1p value. The default classifier is based on the DSCP value.
- Multifield traffic classifiers—Examines multiple fields in the packet such as source and destination addresses and source and destination port numbers of the packet. With multifield classifiers, you set the forwarding class and loss priority of a packet based on firewall filter rules.

To configure and apply behavior aggregate classifiers for the switch:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure and apply behavior aggregate classifiers.
3. Click the **Configuration** tab. In the configuration tree expand **Class of Service**.
4. Select **Classifiers**.
5. Add or modify settings as specified in [Table 53 on page 118](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Network and Security Manager Administration Guide* for more information.

Table 53: Configuring and Applying Behavior Aggregate Classifiers

Task	Action
Configure behavior aggregate classifiers for DiffServ CoS.	<ol style="list-style-type: none"> 1. Click Add new entry next to Dscp. 2. In the Name box, type the name of the behavior aggregate classifier—for example, ba-classifier. 3. In the Import box, type the name of the default DSCP map.

Table 53: Configuring and Applying Behavior Aggregate Classifiers (*continued*)

Task	Action
Configure a best-effort forwarding class classifier.	<ol style="list-style-type: none"> 1. Click Add new entry next to Forwarding class. 2. In the Class name box, type the name of the previously configured best-effort forwarding class—for example, be-class. 3. Click Add new entry next to Loss priority. 4. From the Loss val list, select high. 5. Click Add new entry next to Code points. 6. In the Value box, type the value of the high-priority code point for best-effort traffic—for example, 00001. 7. Click OK three times.
Configure an expedited forwarding class classifier.	<ol style="list-style-type: none"> 1. Click Add new entry next to Forwarding class. 2. In the Class name box, type the name of the previously configured expedited forwarding—for example, class-ef-class. 3. Click Add new entry next to Loss priority. 4. From the Loss val list, select high. 5. Click Add new entry next to Code points. 6. In the Value box, type the value of the high-priority code point for expedited forwarding traffic—for example, 101111. 7. Click OK three times.
Configure an assured forwarding class classifier.	<ol style="list-style-type: none"> 1. Click Add new entry next to Forwarding class. 2. In the Class name box, type the name of the previously configured assured forwarding—for example, class-af-class. 3. Click Add new entry next to Loss priority. 4. From the Loss val list, select high. 5. Click Add new entry next to Code points. 6. In the Value box, type the value of the high-priority code point for assured forwarding traffic—for example, 001100. 7. Click OK three times.
Apply the behavior aggregate classifier to an interface.	<ol style="list-style-type: none"> 1. Click Add new entry next to Interfaces. 2. In the Interface name box, type the name of the interface—for example, ge-0/0/0. 3. Click Add new entry next to Unit. 4. In the Unit number box, type the logical interface unit number—for example, 0. 5. Click Configure next to Classifiers. 6. In the Classifiers box, under Dscp, type the name of the previously configured behavior aggregate classifier—for example, ba-classifier. 7. Click OK.

Related Documentation

- [Configuring CoS Code Point Aliases \(NSM Procedure\) on page 120](#)
- [Configuring CoS Drop Profile \(NSM Procedure\) on page 121](#)
- [Configuring CoS Forwarding Classes \(NSM Procedure\) on page 123](#)
- [Configuring CoS Interfaces \(NSM Procedure\) on page 128](#)
- [Configuring CoS Rewrite Rules \(NSM Procedure\) on page 134](#)
- [Configuring CoS Schedulers \(NSM Procedure\) on page 138](#)
- [Configuring CoS and Applying Scheduler Maps \(NSM Procedure\) on page 140](#)

Configuring CoS Code Point Aliases (NSM Procedure)

You can use code-point aliases to streamline the process of configuring CoS features on your device. A code-point alias assigns a name to a pattern of code-point bits. You can use this name instead of the bit pattern when you configure other CoS components such as classifiers, drop-profile maps, and rewrite rules.

To configure code-point aliases:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure CoS code point aliases.
3. Click the **Configuration** tab. In the configuration tree, expand **Class of Service**.
4. Select **Code Point Aliases**.
5. Add or modify the settings as specified in [Table 54 on page 121](#)
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Network and Security Manager Administration Guide* for more information.

Table 54: Configuring Code Point Aliases

Task	Action
Assign an alias to the dscp code point.	<ol style="list-style-type: none"> 1. In the Configuration tree, expand Code Point Aliases. 2. Select Dscp. 3. Click the Add New icon. 4. In the Name box, type the alias that you want to assign to the code point—for example, my1. 5. In the Bits box, type the code point—for example, 110001. 6. Click OK.

- Related Documentation**
- [Configuring CoS Classifiers \(NSM Procedure\) on page 118](#)
 - [Configuring CoS Drop Profile \(NSM Procedure\) on page 121](#)
 - [Configuring CoS Forwarding Classes \(NSM Procedure\) on page 123](#)
 - [Configuring CoS Interfaces \(NSM Procedure\) on page 128](#)
 - [Configuring CoS Rewrite Rules \(NSM Procedure\) on page 134](#)
 - [Configuring CoS Schedulers \(NSM Procedure\) on page 138](#)
 - [Configuring CoS and Applying Scheduler Maps \(NSM Procedure\) on page 140](#)

Configuring CoS Drop Profile (NSM Procedure)

Drop profiles provide a congestion management mechanism that enables a switch or routing platform to drop the arriving packets when queue buffers become full or begin to overflow. Drop profiles define the meanings of loss priorities. When you configure drop profiles you are essentially setting the value for queue fullness. The queue fullness represents the percentage of the memory used to store packets in relation to the total amount of memory that has been allocated for that specific queue. The queue fullness defines the delay-buffer bandwidth, which provides packet buffer space to absorb burst traffic up to the specified duration of delay. Once the specified delay buffer becomes full, packets with 100 percent drop probability are dropped from the tail of the buffer.

You specify drop probabilities in the drop profile section of the CoS configuration hierarchy and reference them in each scheduler configuration. By default, if you do not configure any drop profile then the drop profile that is in effect functions as the primary mechanism for managing congestion. In the default tail drop profile, when the fill level is 0 percent, the drop probability is 0 percent. When the fill level is 100 percent, the drop probability is 100 percent.

To configure drop profiles in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure drop profiles.

3. Click the **Configuration** tab. In the configuration tree expand **Class of Service**.
4. Select **Drop Profiles**.
5. Add or modify the drop profiles as specified in [Table 55 on page 122](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 55: Drop Profile Configuration Fields

Option	Function	Your Action
Drop Profile		
Name	Specifies the drop profile name.	<ol style="list-style-type: none"> 1. Click the New button or Edit button in the Drop Profile interface. 2. Enter the drop profile name in the Name box.
Comment	Specifies the comment for the drop profile.	<ol style="list-style-type: none"> 1. Click the New button or Edit button in the Drop Profile interface. 2. Enter the comment for the drop profile in the Comment box.
Fill Level		
Name	Specifies the fill level for the drop profile.	<ol style="list-style-type: none"> 1. On Drop Profile interface click the New button or select a profile and click the Edit button. 2. Expand the Drop Profile tree and select Fill Level. 3. Click the New button or select a fill level and click the Edit button. 4. Select a value from Name list.

Table 55: Drop Profile Configuration Fields (*continued*)

Option	Function	Your Action
Comment	Specifies the comment for the fill level	<ol style="list-style-type: none"> 1. On the Drop Profile interface click the New button or select a profile and click the Edit button. 2. Expand the Drop Profile tree and select Fill Level. 3. Click the New button or select a fill level and click the Edit button. 4. Enter a comment in the Comment box.

Related Documentation

- [Configuring CoS Classifiers \(NSM Procedure\) on page 118](#)
- [Configuring CoS Code Point Aliases \(NSM Procedure\) on page 120](#)
- [Configuring CoS Forwarding Classes \(NSM Procedure\) on page 123](#)
- [Configuring CoS Interfaces \(NSM Procedure\) on page 128](#)
- [Configuring CoS Rewrite Rules \(NSM Procedure\) on page 134](#)
- [Configuring CoS Schedulers \(NSM Procedure\) on page 138](#)
- [Configuring CoS and Applying Scheduler Maps \(NSM Procedure\) on page 140](#)

Configuring CoS Forwarding Classes (NSM Procedure)

Forwarding classes allow you to group packets for transmission. Based on forwarding classes, you assign packets to output queues.

By default, four categories of forwarding classes are defined: best effort, assured forwarding, expedited forwarding, and network control.



NOTE: EX Series switches support up to 16 forwarding classes.

To configure CoS forwarding classes:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure CoS forwarding classes.
3. Click the **Configuration** tab. In the configuration tree, expand **Class of Service**.
4. Select **Forwarding Classes**.
5. Add or modify settings as specified in [Table 56 on page 124](#).
6. Click one:
 - **OK**—Saves the changes.

- **Cancel**—Cancels the modifications.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Network and Security Manager Administration Guide* for more information.

Table 56: Assigning Forwarding Classes to Output Queues

Task	Action
Assign best-effort traffic to queue 0.	<ol style="list-style-type: none"> 1. Select Queue and click Add new entry. 2. In the Queue num box, type 0. 3. In the Class name box, type the previously configured name of the best-effort class—for example, be-class. 4. Click OK.
Assign expedited forwarding traffic to queue 1.	<ol style="list-style-type: none"> 1. Select Queue and click Add new entry. 2. In the Queue num box, type 1. 3. In the Class name box, type the previously configured name of the expedited forwarding class—for example, ef-class. 4. Click OK.
Configure an assured forwarding class classifier.	<ol style="list-style-type: none"> 1. Select Queue and click Add new entry. 2. In the Queue num box, type 3. 3. In the Class name box, type the previously configured name of the assured forwarding class—for example, af-class. 4. Click OK.

Related Documentation

- [Configuring CoS Classifiers \(NSM Procedure\) on page 118](#)
- [Configuring CoS Code Point Aliases \(NSM Procedure\) on page 120](#)
- [Configuring CoS Drop Profile \(NSM Procedure\) on page 121](#)
- [Configuring CoS Interfaces \(NSM Procedure\) on page 128](#)
- [Configuring CoS Rewrite Rules \(NSM Procedure\) on page 134](#)
- [Configuring CoS Schedulers \(NSM Procedure\) on page 138](#)
- [Configuring CoS and Applying Scheduler Maps \(NSM Procedure\) on page 140](#)

Configuring CoS Forwarding Policy (NSM Procedure)

Class-of-service (CoS)-based forwarding (CBF) enables you to control next-hop selection based on a packet's class of service and, in particular, the value of the IP packet's precedence bits.

You can specify a particular interface or next hop to carry high-priority traffic while all best-effort traffic takes some other path. When a routing protocol discovers equal-cost paths, it can pick a path at random or load-balance across the paths through either hash selection or round robin. CBF allows path selection based on class.

To configure CoS forwarding policy in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Class of Service**.
4. Select **Forwarding Policy**.
5. Add or modify forwarding policy settings as specified in [Table 57 on page 125](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 57: Forwarding Policy Configuration Details

Task	Your Action
Specify the name of forwarding class and override the incoming packet classification.	<ol style="list-style-type: none"> 1. Click Add new entry next to Class. 2. In the Name box, enter the name of forwarding class. 3. Click Classification Override next to Class. 4. In the Forwarding Class box, enter the name of the forwarding class.

Table 57: Forwarding Policy Configuration Details (*continued*)

Task	Your Action
Specify the map for CoS forwarding routes.	<ol style="list-style-type: none"> 1. Click Add new entry next to Next Hop Map. 2. In the Name box, enter the map that defines next-hop routes. 3. Click Forwarding Class next to next-hop-map. 4. Click Add new entry next to Forwarding Class. 5. In the Name box, enter the name of the forwarding class. 6. Select the Non LSP Next Hop check box to use a non-LSP next hop for traffic sent to the forwarding class next-hop map of the forwarding policy. 7. Select the Discard check box to discard the traffic sent to the forwarding class for the next-hop map referenced by the forwarding policy. 8. Click Lsp Next Hop next to forwarding-class. 9. Click New button next to Lsp Next Hop. 10. In the New Lsp-next-hop dialog box, enter the LSP regular expression to which to map the forwarded traffic. 11. Click Next Hop next to forwarding-class. 12. In the New next-hop dialog box, enter the next-hop name or address to which to map forwarded traffic.

- Related Documentation**
- [Configuring CoS Classifiers \(NSM Procedure\) on page 118](#)
 - [Configuring CoS Routing Instances \(NSM Procedure\) on page 137](#)
 - [Configuring Tracing Operations \(NSM Procedure\) on page 142](#)

Configuring CoS Fragmentation Maps (NSM Procedure)

For AS PIC link services IQ (lsq-) interfaces only, you can configure fragmentation properties on a particular forwarding class. You can set a per-forwarding class fragmentation threshold using fragment-threshold option. This option sets the maximum size of each multilink fragment. You can also set traffic on a particular forwarding class to be interleaved rather than fragmented. An extra fragmentation header is not prepended to the packets received on this queue and that static link load balancing is used to ensure in-order packet delivery. You can also change the resequencing interval for each fragmentation class.

To configure CoS fragmentation maps in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure CoS Fragmentation Maps.
3. Click the **Configuration** tab. In the configuration tree, expand **Class of Service**.
4. Select **Fragmentation Maps**.
5. Add or modify settings as specified in [Table 58 on page 127](#).
6. Click one:

- OK—Saves the changes.
- Cancel—Cancels the modifications.

Table 58: Fragmentation Maps Configuration Details

Task	Your Action
Defines fragmentation properties for individual forwarding classes.	<ol style="list-style-type: none"> 1. Click Add new entry next to Fragmentation Maps. 2. In the Name box, enter the name of the fragmentation map. 3. Click Forwarding Class next to fragmentation-maps. 4. Click Add new entry next to Forwarding Class. 5. In the Name box, enter the name of the forwarding class. 6. From the Multilink Class, select the multilink class to be assigned to the forwarding class. Range: 0 through 7 7. From the Drop Timeout list, select the sequencing timeout interval for each forwarding class of a multiclass MLPPP. Range: 0 through 2000
Set the fragmentation threshold for an individual forwarding class for only AS PIC link services IQ interfaces (lsq).	<ol style="list-style-type: none"> 1. Click Add new entry next to Fragmentation Maps. 2. Click Forwarding Class next to fragmentation-maps. 3. Click Add new entry next to Forwarding Class. 4. Click Fragment Threshold next to forwarding-class. 5. Set the fragmentation threshold for an individual forwarding class. Range: 64 through 9192 bytes

Related Documentation

- [Configuring CoS Forwarding Policy \(NSM Procedure\) on page 125](#)
- [Configuring CoS Schedulers \(NSM Procedure\) on page 138](#)
- [Configuring CoS Traffic Control Profiles \(NSM Procedure\) on page 143](#)

Configuring CoS Host Outbound Traffic (NSM Procedure)

You can modify the default queue assignment (forwarding class) and Differentiated Services Code Point (DSCP) bits used in the Type Of Service (ToS) field of packets generated by the Routing Engine.

To configure CoS Host Outbound Traffic in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure Class-of-Service Host Outbound Traffic.
3. Click the **Configuration** tab. In the configuration tree, expand **Class of Service**.
4. Select **Host Outbound Traffic**.
5. Add or modify settings as specified in [Table 59 on page 128](#).
6. Click one:

- OK—Saves the changes.
- Cancel—Cancels the modifications.

Table 59: Host Outbound Traffic Configuration Details

Option	Function	Your Action
Forwarding Class	Defines a forwarding class name.	In the Forwarding Class box, enter the name for the forwarding class.
Dscp Code Point	Sets the value of the DSCP code point in the ToS field of the packet generated by the Routing Engine (host).	From the Dscp Code Point list, select the DSCP code point value.

Related Documentation

- [Configuring CoS Forwarding Classes \(NSM Procedure\) on page 123](#)
- [Configuring CoS Fragmentation Maps \(NSM Procedure\) on page 126](#)
- [Configuring CoS Traffic Control Profiles \(NSM Procedure\) on page 143](#)
- [Configuring CoS Interfaces \(NSM Procedure\) on page 128](#)

Configuring CoS Interfaces (NSM Procedure)

An interface is configured for optimal performance in a high-traffic network. This feature enables you to configure interface-specific CoS properties for incoming packets.

To configure CoS interfaces in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure CoS interfaces.
3. Click the **Configuration** tab. In the configuration tree, expand **Class of Service**.
4. Select **Interfaces**.
5. Add or modify the interfaces as specified in [Table 60 on page 129](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Network and Security Manager Administration Guide* for more information.

Table 60: Interfaces Configuration Fields

Option	Function	Your Action
Interface		
Name	Specifies the interface name.	<ol style="list-style-type: none"> 1. Expand the Interfaces tree and select Interface. 2. Click the New button or select an interface and click the Edit button in Interface. 3. Enter the interface name in the Name box.
Comment	Specifies the comment for the interface.	<ol style="list-style-type: none"> 1. Expand the Interfaces tree and select Interface. 2. Click the New button or select an interface and click the Edit button in Interface. 3. Enter the comment for the interface in the Comment box.
Scheduler Map	Specifies the scheduler configuration mapped to the forwarding class.	<ol style="list-style-type: none"> 1. Expand the Interfaces tree and select Interface. 2. Click the New button or select an interface and click the Edit button in Interface. 3. Select the scheduler map from the list.
Scheduler Map Chassis	Specifies the scheduler configuration mapped to the forwarding class for the particular chassis in the chassis queue.	<ol style="list-style-type: none"> 1. Expand the Interfaces tree and select Interface. 2. Click the New button or select an interface and click the Edit button in Interface. 3. Select the scheduler map chassis from the list.

Table 60: Interfaces Configuration Fields (*continued*)

Option	Function	Your Action
Input Traffic Control Profile	Applies an input traffic scheduling and shaping profile to the logical interface.	<ol style="list-style-type: none"> 1. Click the New button or select an interface and click the Edit button in Interface. 2. Expand the Interface tree and select Input Traffic Control Profile. 3. Specify the comment and the profile name. 4. Click Ok.
Input Traffic Control Profile Remaining	Applies an input traffic scheduling and shaping profile for remaining traffic to the logical interface.	<ol style="list-style-type: none"> 1. Click the New button or select an interface and click the Edit button in Interface. 2. Expand the Interface tree and select Input Traffic Control Profile Remaining. 3. Specify a comment and a profile name. 4. Click Ok.
Output Traffic Control Profile	Applies an output traffic scheduling and shaping profile to the logical interface.	<ol style="list-style-type: none"> 1. Click the New button or select an interface and click the Edit button in Interface. 2. Expand the Interface tree and select Output Traffic Control Profile. 3. Specify a comment and a profile name. 4. Click Ok.
Output Traffic Control Profile Remaining	Applies an output traffic scheduling and shaping profile for remaining traffic to the logical interface.	<ol style="list-style-type: none"> 1. Click the New button or select an interface and click the Edit button in Interface. 2. Expand the Interface tree and select Output Traffic Control Profile Remaining. 3. Specify a comment and a profile name. 4. Click Ok.

Table 60: Interfaces Configuration Fields (*continued*)

Option	Function	Your Action
Shaping Rate	Shapes the output of the physical interface, so that the interface transmits less traffic than it is physically capable of carrying.	<ol style="list-style-type: none"> 1. Click the New button or select an interface and click the Edit button in Interface. 2. Expand Interface tree and select Shaping Rate. 3. Specify the comment and the rate 4. Click Ok.
Unit	Sets the units that need to be allocated to the specific forwarding class and scheduling map.	<ol style="list-style-type: none"> 1. Click the New button or select an interface and click the Edit button in Interface. 2. Expand Interface tree and select Unit. 3. Specify the Unit, Classifiers, Output Traffic Control Profile and Shaping Rate. 4. Click Ok.
Interface Set		
Name	Specifies the interface set name.	<ol style="list-style-type: none"> 1. Expand the Interfaces tree and select Interface Set. 2. Click the New button or select an interface set and click the Edit button. 3. Select the name from the list.
Comment	Specifies the comment for the interface.	<ol style="list-style-type: none"> 1. Expand the Interfaces tree and select Interface Set. 2. Click the New button or select an interface set and click the Edit button. 3. Enter the comment.
Internal Node	Sets the scheduler node as internal, allowing resource scheduling to be applied equally to interface sets that include child nodes and those that do not include child nodes.	<ol style="list-style-type: none"> 1. Expand the Interfaces tree and select Interface Set. 2. Click the New button or select an interface set and click the Edit button. 3. Set the internal node.

Table 60: Interfaces Configuration Fields (*continued*)

Option	Function	Your Action
Excess Bandwidth Share	Sets the excess bandwidth sharing value.	<ol style="list-style-type: none"> 1. Expand the Interfaces tree and select Interface Set. 2. Click the New button or select an interface set and click the Edit button. 3. Expand interface—set tree and select Excess Bandwidth Share. 4. Specify the comment and proportion. 5. Click Ok.
Input Excess Bandwidth Share	Sets the excess input bandwidth sharing value.	<ol style="list-style-type: none"> 1. Expand the Interfaces tree and select Interface Set. 2. Click the New button or select an interface set and click the Edit button. 3. Expand interface—set tree and select Input Excess Bandwidth Share. 4. Specify the comment and proportion. 5. Click Ok.
Input Traffic Control Profile	Applies an input traffic scheduling and shaping profile to the logical interface.	<ol style="list-style-type: none"> 1. Expand the Interfaces tree and select Interface Set. 2. Click the New button or select an interface set and click the Edit button. 3. Expand interface—set tree and select Input Traffic Control Profile. 4. Specify the comment and profile name. 5. Click Ok.

Table 60: Interfaces Configuration Fields (*continued*)

Option	Function	Your Action
Input Traffic Control Profile Remaining	Applies an input traffic scheduling and shaping profile for remaining traffic to the logical interface.	<ol style="list-style-type: none"> 1. Expand the Interfaces tree and select Interface Set. 2. Click the New button or select an interface set and click the Edit button. 3. Expand interface—set tree and select Input Traffic Control Profile Remaining. 4. Specify the comment and profile name. 5. Click Ok.
Output Traffic Control Profile	Applies an output traffic scheduling and shaping profile to the logical interface.	<ol style="list-style-type: none"> 1. Expand the Interfaces tree and select Interface Set. 2. Click the New button or select an interface set and click the Edit button. 3. Expand interface—set tree and select Output Traffic Control Profile. 4. Specify the comment and profile name. 5. Click Ok.
Output Traffic Control Profile Remaining	Applies an output traffic scheduling and shaping profile for remaining traffic to the logical interface.	<ol style="list-style-type: none"> 1. Expand the Interfaces tree and select Interface Set. 2. Click the New button or select an interface set and click the Edit button. 3. Expand interface—set tree and select Output Traffic Control Profile Remaining. 4. Specify the comment and profile name. 5. Click Ok.

Related Documentation

- [Configuring CoS Classifiers \(NSM Procedure\) on page 118](#)
- [Configuring CoS Code Point Aliases \(NSM Procedure\) on page 120](#)
- [Configuring CoS Drop Profile \(NSM Procedure\) on page 121](#)
- [Configuring CoS Forwarding Classes \(NSM Procedure\) on page 123](#)
- [Configuring CoS Rewrite Rules \(NSM Procedure\) on page 134](#)
- [Configuring CoS Schedulers \(NSM Procedure\) on page 138](#)

- [Configuring CoS and Applying Scheduler Maps \(NSM Procedure\) on page 140](#)

Configuring CoS Rewrite Rules (NSM Procedure)

You configure rewrite rules to alter CoS values in outgoing packets on the outbound interfaces of a device to match the policies of a targeted peer. Policy matching allows the downstream router in a neighboring network to classify each packet into the appropriate service group.

In addition, you often need to rewrite a given marker such as IP precedence, DSCP, or IEEE 802.1p at the switch's inbound interfaces to accommodate behavior aggregate (BA) classification by core devices.

You do not need to explicitly apply rewrite rules to interfaces. By default, rewrite rules are applied to routed packets.

To configure CoS rewrite rules:

1. In the navigation tree, select **Device Manager > Devices**
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure CoS rewrite rules.
3. Click the **Configuration** tab. In the configuration tree, expand **Class of Service**
4. Select **Rewrite Rules**.
5. Add or modify settings as specified in [Table 61 on page 134](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Network and Security Manager Administration Guide* for more information.

Table 61: Configuring and Applying Rewrite Rules

Task	Action
Configure rewrite rules for DiffServ CoS.	<ol style="list-style-type: none"> 1. Click Configure next to Rewrite Rules. 2. Click Add new entry next to Dscp. 3. In the Name box, type the name of the rewrite rules—for example, rewrite-dscps.

Table 61: Configuring and Applying Rewrite Rules (*continued*)

Task	Action
Configure best-effort forwarding class rewrite rules.	<ol style="list-style-type: none"> 1. Click Add new entry next to Forwarding class. 2. In the Queue num box, type 1. 3. In the Class name box, type the name of the previously configured best-effort forwarding class—for example, be-class. 4. Click Add new entry next to Loss priority. 5. From the Loss val list, select low. 6. In the Code point box, type the value of the low-priority code point for best-effort traffic—for example, 000000. 7. Click OK. 8. Click Add new entry next to Loss priority. 9. From the Loss val list, select high. 10. In the Code point box, type the value of the high-priority code point for best-effort traffic—for example, 000001. 11. Click OK twice.
Configure expedited forwarding class rewrite rules.	<ol style="list-style-type: none"> 1. Click Add new entry next to Forwarding class. 2. In the Class name box, type the name of the previously configured expedited forwarding class—for example, ef-class. 3. Click Add new entry next to Loss priority. 4. From the Loss val list, select low. 5. In the Code point box, type the value of the low-priority code point for expedited forwarding traffic—for example, 101110. 6. Click OK. 7. Click Add new entry next to Loss priority. 8. From the Loss val list, select high. 9. In the Code point box, type the value of the high-priority code point for expedited forwarding traffic—for example, 101111. 10. Click OK twice.

Table 61: Configuring and Applying Rewrite Rules (*continued*)

Configure assured forwarding class rewrite rules.	<ol style="list-style-type: none"> 1. Click Add new entry next to Forwarding class. 2. In the Class name box, type the name of the previously configured expedited forwarding class—for example, af-class. 3. Click Add new entry next to Loss priority. 4. From the Loss val list, select low. 5. In the Code point box, type the value of the low-priority code point for assured forwarding traffic—for example, 001010. 6. Click OK. 7. Click Add new entry next to Loss priority. 8. From the Loss val list, select high. 9. In the Code point box, type the value of the high-priority code point for assured forwarding traffic—for example, 001100. 10. Click OK twice.
Apply rewrite rules to an interface.	<ol style="list-style-type: none"> 1. Click Add new entry next to Interfaces. 2. In the Interface name box, type the name of the interface—for example, ge-0/0/0. 3. Click Add new entry next to Unit. 4. In the Unit number box, type the logical interface unit number—for example, 0. 5. Click Configure next to Rewrite rules. 6. In the Rewrite rules name box, under Dscp, type the name of the previously configured rewrite rules—for example, rewrite-dscps. 7. Click OK.

**Related
Documentation**

- [Configuring CoS Classifiers \(NSM Procedure\) on page 118](#)
- [Configuring CoS Code Point Aliases \(NSM Procedure\) on page 120](#)
- [Configuring CoS Drop Profile \(NSM Procedure\) on page 121](#)
- [Configuring CoS Forwarding Classes \(NSM Procedure\) on page 123](#)
- [Configuring CoS Interfaces \(NSM Procedure\) on page 128](#)
- [Configuring CoS Schedulers \(NSM Procedure\) on page 138](#)
- [Configuring CoS and Applying Scheduler Maps \(NSM Procedure\) on page 140](#)

Configuring CoS Routing Instances (NSM Procedure)

You can apply a custom MPLS EXP classifier to the routing instance with VPN routing and forwarding (VRF) table labels enabled using this option. The default MPLS EXP classifier or one that is previously defined can be applied for routing instance.

To configure Class-of-Service routing instances in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Class of Service**.
4. Select **Routing Instances**.
5. Add or modify settings as specified in [Table 62 on page 137](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 62: Routing Instances Configuration Details

Task	Your Action
Apply a custom MPLS EXP classifier to the routing instance for routing instances with VRF table labels enabled.	<ol style="list-style-type: none"> 1. Click Add new entry next to Routing Instances. 2. In the Name box, enter the name of the routing instance.
Specify the classifier name.	<ol style="list-style-type: none"> 1. Click Classifiers next to routing-instances. 2. Click Dscp next to Classifiers. 3. In the Comment box, enter the comment. 4. From the Classifier name list, select the classifier name. 5. Click Dscp IPv6 next to Classifiers. 6. In the Comment box, enter the comment. 7. From the Classifier name list, select the classifier name. 8. Click Exp next to Classifiers. 9. From the Classifier Name list, select the classifier name. 10. Click Ieee 802.1 next to Classifiers. 11. In the Comment box, enter the comment. 12. From the Classifier name list, select the classifier name. 13. From the Vlan tag list, select the VLAN tag.

Table 62: Routing Instances Configuration Details (*continued*)

Task	Your Action
Specify a rewrite-rules mapping for the traffic that passes through all queues on the interface.	<ol style="list-style-type: none"> 1. Click Rewrite Rules next to routing-instances. 2. In the Comment box, enter the comment. 4. Click ieee 802.1 next to Rewrite Rules. 5. Select one of the following: <ul style="list-style-type: none"> • ieee-802.1d—To apply an IEEE-802.1 rewrite rule • ieee-802.1ad—To apply an IEEE-802.1ad rewrite rule 6. In the Comment box, enter the comment. 7. From the Rewrite Rule Name list, select the name of a rewrite-rules mapping. 8. From the Vlan tag list, select the VLAN tag.

Related Documentation

- [Configuring CoS Classifiers \(NSM Procedure\) on page 118](#)
- [Configuring CoS Forwarding Policy \(NSM Procedure\) on page 125](#)
- [Configuring CoS Restricted Queues \(NSM Procedure\) on page 141](#)
- [Configuring Tracing Operations \(NSM Procedure\) on page 142](#)

Configuring CoS Schedulers (NSM Procedure)

Using schedulers, you can assign attributes to queues and thereby provide congestion control for a particular class of traffic. These attributes include the amount of interface bandwidth, memory buffer size, transmit rate, and schedule priority.

To configure CoS schedulers:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure CoS schedulers.
3. Click the **Configuration** tab. In the configuration tree expand **Class of Service**.
4. Select **Schedulers**.
5. Add or modify the settings as specified in [Table 63 on page 139](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Network and Security Manager Administration Guide* for more information.

Table 63: Configuring Schedulers

Task	Action
Specify the buffer size.	<ol style="list-style-type: none"> 1. Click the Add New icon. 2. Expand Buffer Size. 3. Select Percent. 4. Under Percent, select the appropriate option: <ul style="list-style-type: none"> • To specify no buffer size, select None. • To specify buffer size as a percentage of the total buffer, select percent and type an integer from 1 through 100. • To specify buffer size as the remaining available buffer, select remainder. 5. Click OK.
Configure drop profile map.	<ol style="list-style-type: none"> 1. Click the Add New icon. 2. Select drop-profile-map. 3. In the Loss Priority box, select the required loss priority—for example, high. 4. In the Protocol box, select the type of protocol—for example, any. 5. In the Drop Profile box, select the previously configured drop profile. 6. Click OK.
Specify the transmit rate.	<ol style="list-style-type: none"> 1. Click the Add New icon. 2. Expand Transmit Rate. 3. Select Rate. 4. Under Rate, select the appropriate option: <ul style="list-style-type: none"> • To not specify transmit rate, select None. • To enforce a specific transmission rate, select rate and type the transmission rate that you want to enforce. • To specify a percentage of transmission capacity, select percent and type an integer from 1 through 100. • To specify the remaining transmission capacity, select remainder. 5. Click OK.

Related Documentation

- [Configuring CoS Classifiers \(NSM Procedure\) on page 118](#)
- [Configuring CoS Code Point Aliases \(NSM Procedure\) on page 120](#)
- [Configuring CoS Drop Profile \(NSM Procedure\) on page 121](#)
- [Configuring CoS Forwarding Classes \(NSM Procedure\) on page 123](#)
- [Configuring CoS Interfaces \(NSM Procedure\) on page 128](#)
- [Configuring CoS Rewrite Rules \(NSM Procedure\) on page 134](#)
- [Configuring CoS and Applying Scheduler Maps \(NSM Procedure\) on page 140](#)

Configuring CoS and Applying Scheduler Maps (NSM Procedure)

You associate the schedulers with forwarding classes by means of scheduler maps. You can then associate each scheduler map with an interface, thereby configuring the queues and packet schedulers that operate according to this mapping.

To configure CoS and apply scheduler maps:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure CoS and apply scheduler maps.
3. Click the **Configuration** tab. In the configuration tree expand **Class of Service**.
4. Select **Scheduler Maps**.
5. Add or modify settings as specified in [Table 64 on page 140](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Network and Security Manager Administration Guide* for more information.

Table 64: Assigning Forwarding Classes to Output Queues

Task	Action
Configure a scheduler map for DiffServ CoS.	<ol style="list-style-type: none"> 1. Click Add new entry. 2. In the Name box, type the name of the scheduler map—for example, diffserv-cos-map.
Configure a best-effort forwarding class and scheduler.	<ol style="list-style-type: none"> 1. Select Forwarding Class and click Add new entry. 2. In the Name box, type the name of the previously configured best-effort forwarding class—for example, be-class. 3. Select the previously configured best-effort scheduler—for example, be-scheduler. 4. Click OK.
Configure an expedited forwarding class and scheduler.	<ol style="list-style-type: none"> 1. Select Forwarding Class and click Add new entry. 2. In the Name box, type the name of the previously configured expedited forwarding class—for example, ef-class. 3. Select the previously configured expedited forwarding scheduler—for example, ef-scheduler. 4. Click OK.

Table 64: Assigning Forwarding Classes to Output Queues (*continued*)

Task	Action
Configure an assured forwarding class and scheduler.	<ol style="list-style-type: none"> 1. Select Forwarding Class and click Add new entry. 2. In the Name box, type the name of the previously configured assured forwarding class—for example, af-class. 3. Select the previously configured assured forwarding scheduler—for example, af-scheduler. 4. Click OK.
Apply the scheduler map to an interface.	<ol style="list-style-type: none"> 1. Select Interfaces > Interface and click Add new entry. 2. In the Interface name box, type the name of the interface—for example, ge-0/0/0. 3. Select Unit and click Add new entry. 4. In the Unit name box, select the logical interface unit number—for example, 0. 5. In the Scheduler map box, type the name of the previously configured scheduler map—for example, diffserv-cos-map. 6. Click OK.

Related Documentation

- [Configuring CoS Classifiers \(NSM Procedure\) on page 118](#)
- [Configuring CoS Code Point Aliases \(NSM Procedure\) on page 120](#)
- [Configuring CoS Drop Profile \(NSM Procedure\) on page 121](#)
- [Configuring CoS Forwarding Classes \(NSM Procedure\) on page 123](#)
- [Configuring CoS Interfaces \(NSM Procedure\) on page 128](#)
- [Configuring CoS Rewrite Rules \(NSM Procedure\) on page 134](#)
- [Configuring CoS Schedulers \(NSM Procedure\) on page 138](#)

Configuring CoS Restricted Queues (NSM Procedure)

You can map the forwarding classes to the restricted queues for M320 and T Series routers. You can map up to eight forwarding classes to restricted queues.

To configure Class of Service restricted queues in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Class of Service**.
4. Select **Restricted Queue**.
5. Add or modify settings as specified in [Table 65 on page 142](#).
6. Click one:
 - **OK**—Saves the changes.

- **Cancel**—Cancels the modifications.

Table 65: Restricted Queue Configuration Details

Task	Your Action
Map forwarding classes to restricted queues.	In the Comment box, enter the comment.
Specify the name of the forwarding class and queue number.	<ol style="list-style-type: none"> 1. In the Name box, enter the name of the forwarding class. 2. In the Comment box, enter the comment for the forwarding class. 3. From the Rqueue Num list, select the output queue number. Range: 0 through 3

Related Documentation

- [Configuring CoS Classifiers \(NSM Procedure\) on page 118](#)
- [Configuring CoS Forwarding Policy \(NSM Procedure\) on page 125](#)
- [Configuring CoS Translation Table \(NSM Procedure\) on page 144](#)
- [Configuring Tracing Operations \(NSM Procedure\) on page 142](#)

Configuring Tracing Operations (NSM Procedure)

You can configure tracing operations using this option.

To configure tracing operations in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Class Of Service**.
4. Select **Traceoptions**.
5. Add or modify settings as specified in [Table 66 on page 142](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 66: Traceoptions Configuration Details

Task	Your Action
Configure tracing operations.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment for the traceoptions. 2. Select the No Remote Trace check box to disable remote tracing globally or for a specific tracing operation.

Table 66: Traceoptions Configuration Details (*continued*)

Task	Your Action
Specifies the name of the file to receive the output of the tracing operation and specifies the maximum number of trace files.	<ol style="list-style-type: none"> 1. Click File next to Traceoptions. 2. In the Comment box, enter the comment for the file. 3. In the Filename box, enter the name of the file to receive the output of the tracing operation. 4. In the Size box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). 5. From the Files list, select the maximum number of trace files. Range: 2 through 1000. 6. Select world-readable to enable unrestricted file access. 7. Select no-world-readable to restrict file access to owner. This is the default setting. 8. In the Match box, enter the regular expression.
Specifies the tracing operation to perform. To specify more than one tracing operation, include multiple flag statements.	<ol style="list-style-type: none"> 1. Click Flag next to Traceoptions. 2. Click Add new entry next to Flag. 3. From the Name list, select the flag. 4. In the Comment box, enter the comment for the flag.

Related Documentation

- [Configuring CoS Rewrite Rules \(NSM Procedure\) on page 134](#)
- [Configuring CoS Routing Instances \(NSM Procedure\) on page 137](#)
- [Configuring CoS Restricted Queues \(NSM Procedure\) on page 141](#)
- [Configuring CoS Traffic Control Profiles \(NSM Procedure\) on page 143](#)

Configuring CoS Traffic Control Profiles (NSM Procedure)

You can configure traffic shaping and scheduling profiles for Gigabit Ethernet IQ, Channelized IQ PICs, and AS PIC FRF.16 LSQ interfaces.

To configure CoS Traffic Control Profiles in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure CoS Restricted Queues.
3. Click the **Configuration** tab. In the configuration tree, expand **Class of Service**.
4. Select **Traffic Control Profiles**.
5. Add or modify settings as specified in [Table 67 on page 144](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 67: Traffic Control profile Configuration Details

Task	Your Action
Configure traffic shaping and scheduling profiles for Gigabit Ethernet IQ, Channelized IQ PICs, and AS PIC FRF.16 LSQ interfaces.	<ol style="list-style-type: none"> 1. In the Name box, enter the name of the traffic-control profile. 2. Select the scheduler map. 3. Expand traffic-control-profiles. 4. Select the following: <ul style="list-style-type: none"> • Select Delay Buffer Rate as default value and set the delay buffer rate. • Select Guaranteed Rate if you do not configure delay buffer rate. The delay buffer rate calculation is based on the guaranteed rate. <p>NOTE: On LSQ interfaces, you can configure the guaranteed rate as a percentage from 1 through 100.</p> <p>On IQ and IQ2 interfaces, you can configure the guaranteed rate as an absolute rate from 1000 through 160,000,000,000 bits per second.</p> <ul style="list-style-type: none"> • Select Shaping Rate if you do not configure delay buffer rate or guaranteed rate. The delay buffer rate calculation is based on the shaping rate.

Related Documentation

- [Configuring CoS Drop Profile \(NSM Procedure\) on page 121](#)
- [Configuring CoS Host Outbound Traffic \(NSM Procedure\) on page 127](#)
- [Configuring CoS Routing Instances \(NSM Procedure\) on page 137](#)
- [Configuring CoS Translation Table \(NSM Procedure\) on page 144](#)

Configuring CoS Translation Table (NSM Procedure)

On some PICs, the behavior aggregate (BA) translation tables are included for every logical interface (unit) protocol family configured on the logical interface. The proper default translation table is active even if you do not include any explicit translation tables. On M40e, M120, M320, and T Series routers with Enhanced IQ (IQE) PICs, or on any system with IQ2 or Enhanced IQ2 (IQ2E) PICs, you can replace the type-of-service (ToS) bit value on the incoming packet header on a logical interface with a user-defined value. The new ToS value is used for all class-of-service (CoS) processing and is applied before any other CoS or firewall treatment of the packet. The PIC uses the translation-table statement to determine the new ToS bit values. You can configure a physical interface (port) or logical interface (unit) with up to three translation tables. The number of frame relay data-link connection identifiers (DLCIs) (units) that you can configure on each PIC varies based on the number and type of BA classification tables configured on the interfaces.

To configure CoS Translation Table in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Class of Service**.
4. Select **Translation Table**.
5. Add or modify settings as specified in [Table 68 on page 145](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 68: Translation Table Configuration Details

Task	Your Action
Translate incoming IPv4 DSCP values to new values.	<ol style="list-style-type: none"> 1. Click To Dscp From Dscp next to Translation Table. 2. Click Add new entry next to To Dscp From Dscp. 3. In the Name box, enter the IPv4 DSCP values. 4. In the Comment box, enter the comment. 5. Click To Code Point next to to-dscp-from-dscp. 6. Click Add new entry next to to-dscp-from-dscp. 7. From the Name list, select the DSCP. 8. In the Comment box, enter the comment. 9. Click From Code Points next to to-code-point and perform the following: <ul style="list-style-type: none"> • Add—Adds the selected code points from the Non member list to the Members list. • Remove—Removes the selected code points from the Members list. • Add All—Adds all the code points from the Non-members list to the Members list. • Remove All—Removes all the code points from the Members list.

Table 68: Translation Table Configuration Details (*continued*)

Task	Your Action
Translate incoming IPv6 DSCP values to new values.	<ol style="list-style-type: none"> 1. Click To Dscp IPv6 From Dscp IPv6 next to Translation Table. 2. Click Add new entry next to To Dscp IPv6 From Dscp IPv6. 3. In the Name box, enter the IPv6 DSCP values 4. In the Comment box, enter the comment. 5. Click To Code Point next to to-dscp-ipv6-from-dscp-ipv6. 6. Click Add new entry next to to-dscp-ipv6-from-dscp-ipv6 7. From the Name list, select the DSCP. 8. In the Comment box, enter the comment. 9. Click From Code Points next to to-code-point and perform the following: <ul style="list-style-type: none"> • Add—Adds the selected code points from the Non member list to the Members list. • Remove—Removes the selected code points from the Members list. • Add All—Adds all the code points from the Non-members list to the Members list. • Remove All—Removes all the code points from the Members list.
Translate incoming MPLS EXP values to new values.	<ol style="list-style-type: none"> 1. Click To Exp From Exp next to Translation Table. 2. Click Add new entry next to To Exp From Exp. 3. In the Name box, enter the MPLS EXP values. 4. In the Comment box, enter the comment. 5. Click To Code Point next to to-exp-from-exp. 6. Click Add new entry next to to-exp-from-exp. 7. From the Name list, select the EXP code point. 8. In the Comment box, enter the comment. 9. Click From Code Points next to to-code-point and perform the following: <ul style="list-style-type: none"> • Add—Adds the selected code points from the Non member list to the Members list. • Remove—Removes the selected code points from the Members list. • Add All—Adds all the code points from the Non-members list to the Members list. • Remove All—Removes all the code points from the Members list.

Table 68: Translation Table Configuration Details (*continued*)

Task	Your Action
Translate incoming Inet precedence values to new values.	<ol style="list-style-type: none"> 1. Click To Inet Precedence From Inet Precedence next to Translation Table. 2. Click Add new entry next to To Inet Precedence From Inet Precedence. 3. In the Name box, enter the Inet precedence values. 4. In the Comment box, enter the comment. 5. Click To Code Point next to to-inet-precedence-from-inet-precedence. 6. Click Add new entry next to to-inet-precedence-from-inet-precedence. 7. From the Name list, select the INET precedence code point. 8. In the Comment box, enter the comment. 9. Click From Code Points next to to-code-point and perform the following: <ul style="list-style-type: none"> • Add—Adds the selected code points from the Non member list to the Members list. • Remove—Removes the selected code points from the Members list. • Add All—Adds all the code points from the Non-members list to the Members list. • Remove All—Removes all the code points from the Members list.

Related Documentation

- [Configuring CoS Rewrite Rules \(NSM Procedure\) on page 134](#)
- [Configuring CoS Routing Instances \(NSM Procedure\) on page 137](#)
- [Configuring Tracing Operations \(NSM Procedure\) on page 142](#)
- [Configuring CoS Traffic Control Profiles \(NSM Procedure\) on page 143](#)

Configuration of Event Options

- [Configuring Destinations for File Archiving \(NSM Procedure\) on page 149](#)
- [Configuring Event Script \(NSM Procedure\) on page 150](#)
- [Generating Internal Events \(NSM Procedure\) on page 152](#)
- [Configuring Event Policy \(NSM Procedure\) on page 152](#)
- [Configuring Event Policy Tracing Operations \(NSM Procedure\) on page 155](#)

Configuring Destinations for File Archiving (NSM Procedure)

You can define a destination with a unique name and other attributes. You can use the destination as a storage location for command output and for various files, such as system log files and core files.

To configure destinations for file archiving in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Event Options**.
4. Select **Destination**.
5. Add or modify settings as specified in [Table 69 on page 149](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 69: Destination Configuration Details

Option	Function	Your Action
Name	Specifies the name of the destination.	Enter the name for the destination.
Comment	Specifies the comment for the destination.	Enter the comment for the destination.

Table 69: Destination Configuration Details (*continued*)

Option	Function	Your Action
Transfer Delay	Specifies the number of seconds the event process (eventd) waits before beginning to upload a file or multiple files.	Select the duration of the delay.
Destination > Archive Sites		
Name	Specifies an archive site to which files are transferred. If you specify more than one archive site, the router attempts to transfer to the first archive site in the list, moving to the next site only if the transfer fails.	Enter the archive destination.
Comment	Specifies the comment for the archive sites.	Enter the comment for the archive site.
Password	Defines a plain-text password for login into the archive site.	Enter the password.

Related Documentation

- [Configuring Event Script \(NSM Procedure\) on page 150](#)
- [Generating Internal Events \(NSM Procedure\) on page 152](#)
- [Configuring Event Policy \(NSM Procedure\) on page 152](#)
- [Configuring Event Policy Tracing Operations \(NSM Procedure\) on page 155](#)

Configuring Event Script (NSM Procedure)

Event scripts allow you to automate network troubleshooting and network management.

To configure event scripting in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Event Options > Event Script**.
4. Select **Event Script**.
5. Add or modify settings as specified in [Table 70 on page 151](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 70: Event Script Configuration Details

Task	Your Action
Specify the name of an Extensible Stylesheet Language Transformations (XSLT) or Stylesheet Language Alternative Syntax (SLAX) file containing an event script.	<ol style="list-style-type: none"> 1. Click File next to Event Script. 2. Click Add new entry next to File. 3. In the Name box, enter the filename. 4. In the Comment box, enter the comment.
Calculate the checksum.	<ol style="list-style-type: none"> 1. Click Checksum next to file. 2. In the Comment box, enter the comment. 3. In the Md5 box, enter the MD5 checksum. 4. In the Sha1 box, enter the SHA-1 checksum. 5. In the Sha 256 box, enter the SHA-256 checksum.
Configure the username and passphrase for a remote machine.	<ol style="list-style-type: none"> 1. Click Remote Execution next to file. 2. Click Add new entry next to Remote Execution. 3. In the Name box, enter the filename. 4. In the Comment box, enter the comment. 5. In the Username box, enter the username for the remote machine. 6. In the Passphrase box, enter the passphrase for the remote machine.
Define tracing operations for event scripts.	<ol style="list-style-type: none"> 1. Click Traceoptions next to Event Script. 2. In the Comment box, enter the comment. 3. Expand traceoptions. 4. Click File next to Traceoptions. 5. In the Comment box, enter the comment. 6. In the Filename box, enter the name of the file to receive the output of the tracing operation. 7. In the Size box, enter the maximum trace file size. 8. From the Files list, select the maximum number of trace files. 9. Select one of the following: <ul style="list-style-type: none"> • no-world-readable—To restrict the file access to owner. • world-readable—To enable unrestricted access. 10. Click Flag next to traceoptions. 11. Click Add new entry next to Flag. 12. From the Name list, select the flag to perform the trace operation. 13. In the Comment box, enter the comment for the flag.

- Related Documentation**
- [Configuring Destinations for File Archiving \(NSM Procedure\) on page 149](#)
 - [Generating Internal Events \(NSM Procedure\) on page 152](#)
 - [Configuring Event Policy \(NSM Procedure\) on page 152](#)
 - [Configuring Event Policy Tracing Operations \(NSM Procedure\) on page 155](#)

Generating Internal Events (NSM Procedure)

To generate an internal event, based on a time interval or the time of day, you can use the generate event option.

To generate internal events in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Event Options**.
4. Select **Generate Event**.
5. Add or modify settings as specified in [Table 71 on page 152](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 71: Generate Event Details

Task	Your Action
Generate an internal event, based on a time interval or the time of day.	<ol style="list-style-type: none"> 1. In the Name box, enter the name of an internally generated event 2. In the Comment box, enter the comment for the generate event. 3. Click Time of Day next to generate-event and select one of the following: <ul style="list-style-type: none"> • time-of-day—To configure a time of day at which to generate a particular event. • time-interval—To configure a frequency at which to generate a particular event.

Related Documentation

- [Configuring Destinations for File Archiving \(NSM Procedure\) on page 149](#)
- [Configuring Event Script \(NSM Procedure\) on page 150](#)
- [Configuring Event Policy \(NSM Procedure\) on page 152](#)
- [Configuring Event Policy Tracing Operations \(NSM Procedure\) on page 155](#)

Configuring Event Policy (NSM Procedure)

Event policies can listen for specific events, create log files, invoke Junos OS commands, and invoke event scripts.

To configure an event policy in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.

3. Click the **Configuration** tab. In the configuration tree, expand **Event Options**.
4. Select **Policy**.
5. Add or modify settings as specified in [Table 72 on page 153](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 72: Configure Event Policy Details

Task	Your Action
Define an event policy to be processed by the event process (eventd) process.	<ol style="list-style-type: none"> 1. Click Add new entry next to Policy. 2. In the Name box, enter the policy name. 3. In the Comment box, enter the comment for the policy.
Execute the policy only if the attributes of two events are correlated or if the attribute of one event matches a regular expression.	<ol style="list-style-type: none"> 1. Click Add new entry next to Attributes Match. 2. In the From Event Attribute box, enter the first attribute to compare. 3. From the Condition list, select the match condition for the attributes. 4. In the To Event Attribute Value box, enter another attribute. 5. In the Comment box, enter the comment for the attributes-match.
Create a list of events that trigger this policy. If one or more of the listed events occurs, the policy is executed.	<ol style="list-style-type: none"> 1. Click Add new entry next to Events. 2. In the New events dialog box, enter the name of the event.
Define actions to take if an event occurs. For each policy, you can configure multiple actions.	<ol style="list-style-type: none"> 1. Click Then next to policy. 2. In the comment box, enter the comment. 3. Select the Ignore check box to define a policy that ignores particular events. 4. Select the Raise Trap check box to define a policy that raises a Simple Network Management Protocol (SNMP) trap in response to an event.
Specify operational mode commands to be issued, the format of the command output, and a name and destination for the output file.	<ol style="list-style-type: none"> 1. Expand Then and select Event Script. 2. Click Add new entry next to Event Script. 3. In the Name box, enter the filename. 4. In the comment box, enter the comment for the event script. 5. From the Username list, select the user associated with an action in an event policy. 6. In the Output Filename box, enter the filename to which to write command or script output for the specified commands or script. 7. From the Output Format list, select the format for the output of the specified commands.

Table 72: Configure Event Policy Details (*continued*)

Task	Your Action
Include command-line arguments to the script for Junos OS op scripts and assign a location to which to upload command or script output for the specified policy.	<ol style="list-style-type: none"> 1. Expand event-script. 2. Click Arguments next to event-script. 3. Click Add new entry next to Arguments. 4. In the Name box, enter the arguments to the script as name. 5. In the comment box, enter the comment. 6. In the Value box, enter the variables in the argument values to allow data from the triggering event to be automatically included in the argument. 7. Click Destination next to event-script. 8. From the Name list, select the location to which to upload command or script output for the specified policy. 9. In the Comment box, enter the comment. 10. From the Transfer Delay list, select the delay in seconds before transferring files. 11. Expand Destinations and select Retry Count next to it. 12. In the Comment box, enter the comment for the retry count. 13. From the Retry list, select the number of retries. 14. From the Retry Interval list, select the length of time to wait between retries.
Specify operational mode commands to be issued, the format of the command output, and a name and destination for the output file on receipt of an event.	<ol style="list-style-type: none"> 1. Expand Execute Commands. 2. Click Commands. 3. In the Name box, enter the command. 4. Click Destination next to Execute Commands. 5. See "Configuring Destinations for File Archiving (NSM Procedure)" on page 149
Specify a file to be uploaded to a destination on receipt of an event.	<ol style="list-style-type: none"> 1. Click Upload next to Event Script. 2. In the Filename box, enter the name of the file to be uploaded. 3. From the Destination list, select the name of a destination. 4. From the User Name list, select the username. 5. From the transfer relay list, select the delay before transferring files.

Table 72: Configure Event Policy Details (*continued*)

Task	Your Action
Create a list of events that must (or must not) occur within a specified time interval for the policy to be triggered.	<ol style="list-style-type: none"> 1. Click Add new entry next to Within. 2. Expand Within. 3. From the Name list, select the interval between events. 4. Click Events next to within. 5. Click Add new entry next to Events. 6. In the New events dialog box, enter the events that trigger this policy. 7. Expand Not. 8. Click Events next to Not. 9. In the New events dialog box, enter the events that trigger this policy. 10. Click Trigger next to Not. 11. In the Comment box, enter the comment. 12. Select one of the following: <ol style="list-style-type: none"> a. until—if the policy is to be executed each time a matching event is received and stops being executed when the number of matching events received equals number. b. on—if the policy is executed when the number of matching events received equals number. c. after—if the policy is executed when the number of matching events received equals number + 1. 13. From the Count list, select the number of times an event or set of events should occur within a specified time period.

Related Documentation

- [Configuring Destinations for File Archiving \(NSM Procedure\) on page 149](#)
- [Configuring Event Script \(NSM Procedure\) on page 150](#)
- [Generating Internal Events \(NSM Procedure\) on page 152](#)
- [Configuring Event Policy Tracing Operations \(NSM Procedure\) on page 155](#)

Configuring Event Policy Tracing Operations (NSM Procedure)

Event policy tracing operations track all event policy operations and record them in a log file. The logged error descriptions provide detailed information to help you solve problems faster.

To configure event policy tracing operations in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Event Options**.
4. Select **Traceoptions**.

5. Add or modify settings as specified in [Table 73 on page 156](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 73: Event Options Traceoptions Configuration Details

Task	Your Action
Define tracing operations for event policy.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment for the traceoptions. 2. Select the No Remote Trace check box to disable remote tracing globally or for a specific tracing operation.
Specify the name of the file to receive the output of the tracing operation and the maximum number of trace files.	<ol style="list-style-type: none"> 1. Click File next to Traceoptions. 2. In the Comment box, enter the comment for the file. 3. In the Filename box, enter the name of the file to receive the output of the tracing operation. 4. In the Size box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). 5. From the Files list, select the maximum number of trace files. Range: 2 through 1000. 6. Select one of the following: <ul style="list-style-type: none"> • world-readable—To enable unrestricted file access. • no-world-readable—To restrict file access to owner. This is the default setting. 7. In the Match box, enter the regular expression.
Specify the tracing operation to perform.	<ol style="list-style-type: none"> 1. Click Flag next to Traceoptions. 2. Click Add new entry next to Flag. 3. From the Name list, select the flag. 4. In the Comment box, enter the comment for the flag.

Related Documentation

- [Configuring Destinations for File Archiving \(NSM Procedure\) on page 149](#)
- [Configuring Event Script \(NSM Procedure\) on page 150](#)
- [Generating Internal Events \(NSM Procedure\) on page 152](#)
- [Configuring Event Policy \(NSM Procedure\) on page 152](#)

Configuration of Firewall

- [Configuring the Firewall Filter for Any Family Type \(NSM Procedure\) on page 157](#)
- [Configuring the Firewall Filter for Bridge Family Type \(NSM Procedure\) on page 159](#)
- [Configuring the Firewall Filter for Ccc Family Type \(NSM Procedure\) on page 161](#)
- [Configuring Filters for inet Family Type \(NSM Procedure\) on page 163](#)
- [Configuring Filters for inet6 Family Type \(NSM Procedure\) on page 168](#)
- [Configuring the Firewall Filter for MPLS Family Type \(NSM Procedure\) on page 172](#)
- [Configuring the Firewall Filter for VPLS Family Type \(NSM Procedure\) on page 175](#)
- [Configuring a Policer for a Firewall Filter on page 178](#)

Configuring the Firewall Filter for Any Family Type (NSM Procedure)

You can specify any to filter packets based upon protocol-independent fields.

To configure firewall filter in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Firewall > Family > Any**.
4. Add or modify settings as specified in [Table 74 on page 158](#).
5. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 74: Firewall Filter Configuration Details

Task	Your Action
Configure firewall filters for protocol-independent match conditions.	<ol style="list-style-type: none"> 1. Expand Any. 2. In the Comment box, enter the comment for Any. 3. Click Filter next to Any. 4. Click Add new entry next to Filter. 5. In the name box, enter the name that identifies the filter. 6. In the Comment box, enter the comment for the filter. 7. Expand Filter. 8. Click Term next to Filter. 9. Click Add new entry next to Term. 10. Expand Term. 11. In the Name box, enter the name that identifies the term. 12. In the Comment box, enter the comment for the term. 13. Expand From. 14. From the listed protocol-independent match conditions, select the filters defined for the any family type. The protocol-independent match conditions are Forwarding Class, Interface, Interface Set, Loss Priority, and Packet Length. 15. Expand Then. 16. In the Comment box, enter the comment for then. 17. In the Count box, enter the number of packets. 18. From the Loss Priority list, set the packet loss priority (PLP) to low, medium-low, medium-high, or high. 19. In the Forwarding Class box, enter the packet forwarding class name. 20. Click Accept next to Then. 21. Select one of the following: <ul style="list-style-type: none"> • Accept—To accept a packet. • Discard—To discard a packet silently, without sending an ICMP message. • Next—To evaluate the next term in the firewall filter. 22. Click Policer next to Then. 23. Select one of the following: <ul style="list-style-type: none"> • policer—To configure a new policer for each filter and select the policer name. • three-color-policer—To configure a tricolor marking policer. <ol style="list-style-type: none"> a. Expand Three Color Policer. b. Click Single Rate next to Three Color Policer. c. Select one of the following: <ul style="list-style-type: none"> • single-rate—if the named tricolor policer is a single-rate policer. • two-rate—if the named tricolor policer is a two-rate policer.

Related Documentation

- [Configuring the Firewall Filter for Bridge Family Type \(NSM Procedure\) on page 159](#)

- [Configuring the Firewall Filter for Ccc Family Type \(NSM Procedure\) on page 161](#)
- [Configuring Filters for inet Family Type \(NSM Procedure\) on page 163](#)

Configuring the Firewall Filter for Bridge Family Type (NSM Procedure)

On the MX Series router, you can filter Layer 2 packets in a bridging environment using this option.

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Firewall > Family > Bridge**.
4. Add or modify settings as specified in [Table 75 on page 159](#).
5. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 75: Bridge Filter Configuration Details

Task	Your Action
Configure firewall filters for Layer 2 packets that are part of bridging domain for MX series routers.	<ol style="list-style-type: none"> 1. Click Filter next to Bridge. 2. Click Add new entry next to Filter. 3. Expand Filter. 4. In the name box, enter the name that identifies the filter. 5. In the Comment box, enter the comment. 6. Select Interface Specific to configure interface-specific names for firewall counters.
Configure accounting for firewall filter.	<ol style="list-style-type: none"> 1. Click Accounting Profile next to filter. 2. In the New accounting-profile window, enter the name to be assigned to the accounting profile.

Table 75: Bridge Filter Configuration Details (*continued*)

Task	Your Action
Define a firewall filter term.	<ol style="list-style-type: none"> 1. Click Add new entry next to Term. 2. Expand Term. 3. In the Name box, enter the name that identifies the term. 4. In the Comment box, enter the comment for the term. 5. From the Filter list, select the name that identifies the filter. 6. Expand From. 7. In the Comment box, enter the comment. 8. In the Tcp Flags box, enter the Tcp flags. 9. From the listed protocol-independent match conditions, select the filters defined for the Bridge family type. <p>The protocol-independent match conditions are Destination Mac Address, Destination port, DSCP, Ether Type, Forwarding Class, ICMP Code, ICMP Type, Interface Group, IP Address, IP Destination Address, IP Precedence, IP Protocol, IP Source Address, Learn Vlan Ip Priority, Learn Vlan Id, Loss priority, Port, Source Mac Address, Source Port, Traffic Type, User Vlan Ip Priority, User Vlan Id, and Vlan Ether Type.</p> 10. Expand Then. 11. In the Comment box, enter the comment for then. 12. In the Count box, enter the number of packets. 13. From the Loss Priority list, set the packet loss priority (PLP) to low, medium-low, medium-high, or high. 14. In the Forwarding Class box, enter the packet forwarding class name. 15. Select Port Mirror check box to port mirror the packets. 16. Click Accept next to Then. <ul style="list-style-type: none"> • Select Accept to accept a packet. • Select Discard to discard a packet silently, without sending an ICMP message. • Select Next to evaluate the next term in the firewall filter. 17. Click Policer next to Then. 18. Select one of the following: <ul style="list-style-type: none"> • Policer—To configure a new policer for each filter and select the policer name. • three-color-policer—To configure a tricolor marking policer, <ol style="list-style-type: none"> a. Expand Three Color Policer. b. Click Single Rate next to Three Color Policer. c. Select one of the following: <ul style="list-style-type: none"> • single-rate—if the named tricolor policer is a single-rate policer. • two-rate—if the named tricolor policer is a two-rate policer.

Related Documentation

- [Configuring the Firewall Filter for Any Family Type \(NSM Procedure\) on page 157](#)
- [Configuring the Firewall Filter for Ccc Family Type \(NSM Procedure\) on page 161](#)

- [Configuring Filters for inet Family Type \(NSM Procedure\) on page 163](#)
- [Configuring Filters for inet6 Family Type \(NSM Procedure\) on page 168](#)
- [Configuring the Firewall Filter for MPLS Family Type \(NSM Procedure\) on page 172](#)

Configuring the Firewall Filter for Ccc Family Type (NSM Procedure)

On the MX Series router, you can filter Layer 2 packets in a bridging environment using this option.

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Firewall > Family > Ccc**.
4. Add or modify settings as specified in [Table 76 on page 161](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 76: Ccc Filter Configuration Details

Task	Your Action
Configure firewall filters for Layer 2 switching cross-connects.	<ol style="list-style-type: none"> 1. Click Filter next to Ccc. 2. Click Add new entry next to Filter. 3. Expand Filter. 4. In the name box, enter the name that identifies the filter. 5. In the Comment box, enter the comment. 6. Select the Interface Specific check box to configure interface-specific names for firewall counters.
Configure accounting for firewall filter.	<ol style="list-style-type: none"> 1. Click Accounting Profile next to filter. 2. Click Add new entry next to Accounting Profile. 3. In the New accounting-profile window, enter the name to be assigned to the accounting profile.

Table 76: Ccc Filter Configuration Details (*continued*)

Task	Your Action
Define a firewall filter term.	<ol style="list-style-type: none"> 1. Click Term next to Accounting Profile. 2. Click Add new entry next to Term. 3. Expand Term. 4. In the Name box, enter the name that identifies the term. 5. In the Comment box, enter the comment for the term. 6. From the Filter list, select the name that identifies the filter. 7. Expand From. 8. In the Comment box, enter the comment. 9. From the listed protocol-independent match conditions, select the filters defined for the Ccc family type. The protocol-independent match conditions are Forwarding Class, Interface Group, Vlan 1p property, Loss Priority, and User Vlan-1p Priority. 10. Expand Then. 11. In the Comment box, enter the comment for then. 12. In the Count box, enter the number of packets. 13. From the Loss Priority list, set the packet loss priority (PLP) to low, medium-low, medium-high, or high. 14. In the Forwarding Class box, enter the packet forwarding class name. 15. Click Accept next to Then. 16. Select one of the following: <ul style="list-style-type: none"> • Accept—To accept a packet. • Discard—To discard a packet silently, without sending an ICMP message. • Next—To evaluate the next term in the firewall filter. 17. Click Policer next to Then. 18. Select one of the following: <ul style="list-style-type: none"> • Policer—To configure a new policer for each filter and select the policer name. • three-color-policer—To configure a tricolor marking policer, <ol style="list-style-type: none"> a. Expand Three Color Policer. b. Click Single Rate next to Three Color Policer. c. Select one of the following: <ul style="list-style-type: none"> • single-rate—if the named tricolor policer is a single-rate policer. • two-rate—if the named tricolor policer is a two-rate policer.

Related Documentation

- [Configuring the Firewall Filter for Bridge Family Type \(NSM Procedure\) on page 159](#)
- [Configuring the Firewall Filter for MPLS Family Type \(NSM Procedure\) on page 172](#)
- [Configuring the Firewall Filter for VPLS Family Type \(NSM Procedure\) on page 175](#)

Configuring Filters for inet Family Type (NSM Procedure)

You can configure filters, prefix-actions, service filters, and simple filters for Inet using the following options. See the following topics:

- [Configuring Firewall Filter for inet Family Type \(NSM Procedure\)](#) on page 163
- [Configuring Prefix-specific Actions \(NSM Procedure\)](#) on page 165
- [Configuring Service Filters \(NSM Procedure\)](#) on page 166
- [Configuring Simple Filters \(NSM Procedure\)](#) on page 167

Configuring Firewall Filter for inet Family Type (NSM Procedure)

You can configure a firewall filter for inet family type.

To configure the firewall filter in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Firewall > Family > Inet**.
4. Select **Filter**.
5. Add or modify settings as specified in [Table 77 on page 163](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 77: Firewall Filter Configuration Details

Task	Your Action
Configure a firewall filter to filter IPv4 packets.	<ol style="list-style-type: none"> 1. Expand Inet. 2. Click Filter next to Inet. 3. Click Add new entry next to Filter. 4. Expand Filter. 5. In the name box, enter the name that identifies the filter. 6. In the Comment box, enter the comment. 7. Select the Interface Specific check box to configure interface-specific names for firewall counters.
Configure accounting for firewall filters.	<ol style="list-style-type: none"> 1. Click Accounting Profile next to filter. 2. Click Add new entry next to Accounting Profile. 3. In the New accounting-profile window, enter the name to be assigned to the accounting profile.

Table 77: Firewall Filter Configuration Details (*continued*)

Task	Your Action
Define firewall filter term.	<ol style="list-style-type: none"> 1. Click Term next to Accounting Profile. 2. Click Add new entry next to Term. 3. Expand Term. 4. In the Name box, enter the name that identifies the term. 5. In the Comment box, enter the comment for the term. 6. From the Filter list, select the name that identifies the filter. 7. Expand From. 8. In the Comment box, enter the comment. 9. Select the Is Fragment check box if the packet is a trailing fragment. 10. Select the First Fragment check box if it matches the first fragment of a fragmented packet. 11. In the Fragment Flags box, enter the IP fragmentation flags. 12. Select the Tcp Initial check box if it matches the first TCP packet of a connection. 13. Select the Tcp established check box if it matches the TCP packets other than the first packet of a connection. 14. In the Tcp Flags box, enter the TCP flags. 15. From the listed protocol-independent match conditions, select the filters defined for the Inet family type. The protocol-independent match conditions are Address, Ah Spi, Destination Address, Destination Class, Destination port, Destination prefix List, Dscp, Esp Spi, Forwarding Class, Fragment offset, Icmp Code, Icmp Type, Interface, Interface Group, Interface Set, IP Options, Loss Priority, Packet Length, Port, Precedence, prefix List, Protocol, Source Address, Source Port, Source Prefix List and Ttl. 16. Expand Then. 17. In the Comment box, enter the comment for then. 18. In the Count box, enter the number of packets. 19. Select the Log check box to store the header information of a packet on the Routing Engine. 20. Select Syslog to log an alert for the packet. 21. Select the Sample check box to sample the packet traffic. 22. Select the Port Mirror check box to port-mirror the packets. 23. From the Loss Priority list, set the packet loss priority (PLP) to low, medium-low, medium-high, or high. 24. In the Forwarding Class box, enter the packet forwarding class name. 25. From the Prefix Action list, select the prefix specific action.

Table 77: Firewall Filter Configuration Details (*continued*)

Task	Your Action
	<p>26. Click Accept next to Then.</p> <ul style="list-style-type: none"> • Select Accept to accept a packet. • Select Discard to discard a packet silently, without sending an ICMP message. • Select Next to evaluate the next term in the firewall filter. • Select Routing instance to specify a routing table to which packets are forwarded. • Select IPsec Sa to specify an IP Security (IPsec) security association (SA) for the packet. • Select Reject to discard a packet, and send an ICMP destination unreachable message. <p>27. Click Policer next to Then.</p> <p>28. Select one of the following:</p> <ul style="list-style-type: none"> • Select Policer to configure a new policer for each filter and select the policer name. • Select three-color-policer to configure a tricolor marking policer, <ul style="list-style-type: none"> a. Expand Three Color Policer. b. Click Single Rate next to Three Color Policer. c. Select one of the following: <ul style="list-style-type: none"> • single-rate—If the named tricolor policer is a single-rate policer. • two-rate—If the named tricolor policer is a two-rate policer.

Configuring Prefix-specific Actions (NSM Procedure)

Prefix-specific actions allow you to configure policers and counters for specific addresses or ranges of addresses. This allows you to essentially create policers and counters on a per-prefix level.

To configure the prefix-specific actions in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Firewall > Family > Inet**.
4. Click **Prefix Action**.
5. Add or modify settings as specified in [Table 78 on page 166](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 78: Prefix Actions Details

Task	Your Action
Configure prefix-specific actions.	<ol style="list-style-type: none"> 1. Click Prefix Action next to Inet. 2. In the Name box, enter the action name. 3. From the Policer list, select the actions to be taken. 4. Select the Count check box to include count as the action modifier. 5. Select the Filter Specific check box to configure a policer to act as a filter-specific policer. 6. From the Subnet Prefix Length list, select the subnet prefix length. Range: 0 to 32 7. Click Source Prefix Length next to prefix-action. 8. Select source-prefix-length to configure the source address range specified for a prefix-specific policer or counter and select the source prefix length. 9. Select destination-prefix-length to configure the destination address range specified for a prefix-specific policer or counter and select the destination prefix length.

Configuring Service Filters (NSM Procedure)

A service filter identifies packets on which one or more services are to be applied, and which PIC performs the service.

To configure the service filters for inet in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Firewall > Family > Inet**.
4. Click **Prefix Action**.
5. Add or modify settings as specified in [Table 79 on page 166](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 79: Service Filter Configuration Details

Task	Your Action
Configure service filter.	<ol style="list-style-type: none"> 1. Click Service Filter next to Inet. 2. Click Add new entry next to Service Filter. 3. Expand service-filter. 4. In the Name box, enter the name that identifies the service filter.

Table 79: Service Filter Configuration Details (*continued*)

Task	Your Action
Define firewall filter term.	<ol style="list-style-type: none"> 1. Click Term next to service-filter. 2. Click Add new entry next to Term. 3. Expand Term. 4. In the Name box, enter the name that identifies the term. 5. In the Comment box, enter the comment for the term. 6. Expand From. 7. In the Comment box, enter the comment. 8. Check the Is Fragment check box if the packet is a trailing fragment. 9. Check the First Fragment check box if it matches the first fragment of a fragmented packet. 10. In the Fragment Flags box, enter the IP fragmentation flags. 11. From the listed protocol-independent match conditions, select the filters defined for the Inet family type. The protocol-independent match conditions are Address, Ah Spi, Destination Address, Destination port, Destination prefix List, Esp Spi, Fragment offset, Interface Group, , IP Options, Loss Priority, Port, Prefix List, Protocol, Source Address, Source Port, and Source Prefix List. 12. Click Then next to From. 13. In the Comment box, enter the comment for then. 14. In the Count box, enter the number of packets. 15. Select the Log check box to store the header information of a packet on the Routing Engine. 16. Select the Sample check box to sample the packet traffic. 17. Select the Port Mirror check box to port-mirror the packets. 18. Select Service to direct packets for stateful-firewall service. 19. Select Skip to let packets bypass stateful-firewall service.

Configuring Simple Filters (NSM Procedure)

Simple filters are used to support Ethernet IQ2 PICs. A simple filter is a subset of a firewall filter with the following limitations:

- The **next-term** action is not supported.
- The **except** and **protocol-except** match conditions are not supported.
- Noncontiguous masks are not supported.
- Only one **source-address** and one **destination-address prefix** are allowed for each filter term.

To configure the simple filters for inet in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Firewall > Family > Inet**.
4. Select **Simple Filters**.
5. Add or modify settings as specified in [Table 80 on page 168](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 80: Simple Filter Details

Task	Your Action
Configure simple filter.	<ol style="list-style-type: none"> 1. Click Simple Filter next to Inet. 2. Click Add new entry next to Simple Filter. 3. In the Name box, enter the name that identifies the simple filter.
Define a term.	<ol style="list-style-type: none"> 1. Click Term next to simple-filter. 2. Click Add new entry next to Term. 3. Expand Term. 4. In the Name box, enter the name that identifies the term. 5. In the Comment box, enter the comment. 6. Expand From. 7. From the listed protocol-independent match conditions, select the filters defined for the Inet family type. The protocol-independent match conditions are Destination Address, Destination port, Forwarding Class, Protocol, Source Address, and Source Port. 8. Click Then next to From. 9. In the Comment box, enter the comment. 10. From the Loss Priority list, select the packet loss priority (PLP) level to set it as low, medium-low, medium-high, or high. 11. In the Forwarding Class box, enter the packet forwarding class name.

Configuring Filters for inet6 Family Type (NSM Procedure)

You can configure filter and service filters for inet6 using the Firewall option. See the following topics:

- [Configuring Firewall Filter for inet6 Family Type \(NSM Procedure\) on page 169](#)
- [Configuring Service Filters for inet6 \(NSM Procedure\) on page 171](#)

Configuring Firewall Filter for inet6 Family Type (NSM Procedure)

You can specify inet6 to filter IP version 6 (IPv6) packets.

To configure the firewall filter in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Firewall > Family > Inet6**.
4. Add or modify settings as specified in [Table 81 on page 169](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 81: Inet6 Firewall Filter Configuration Details

Task	Your Action
Configure firewall filter to filter IPv6 packets.	<ol style="list-style-type: none"> 1. Click Filter next to Inet6. 2. Click Add new entry next to Filter. 3. Expand Filter. 4. In the Name box, enter the name that identifies the filter. 5. In the Comment box, enter the comment. 6. Select the Interface Specific check box to configure interface-specific names for firewall counters.
Configure accounting for firewall filters.	<ol style="list-style-type: none"> 1. Click Accounting Profile next to filter. 2. Click Add new entry next to Accounting Profile. 3. In the New accounting-profile window, enter the name to be assigned to the accounting profile.

Table 81: Inet6 Firewall Filter Configuration Details (*continued*)

Task	Your Action
Define firewall filter term.	<ol style="list-style-type: none"> 1. Click Term next to Accounting Profile. 2. Click Add new entry next to Term. 3. Expand Term. 4. In the Name box, enter the name that identifies the term. 5. In the Comment box, enter the comment for the term. 6. From the Filter list, select the name that identifies the filter. 7. Expand From. 8. In the Comment box, enter the comment. 9. Select the Tcp Initial check box if it matches the first TCP packet of a connection. 10. Select the Tcp established check box if it matches the TCP packets other than the first packet of a connection. 11. In the Tcp Flags box, enter the TCP flags. 12. From the listed protocol-independent match conditions, select the filters defined for the inet family type. The protocol-independent match conditions are Address, Destination Address, Destination Class, Destination port, Destination prefix List, Dscp, Forwarding Class, Fragment offset, Icmp Code, Icmp Type, Interface, Interface Group, Interface Set, IP Options, Loss Priority, Packet Length, Port, prefix List, Protocol, Source Address, Source Port, Source Prefix List, and traffic list. 13. Expand Then. 14. In the Comment box, enter the comment for then. 15. In the Count box, enter the number of packets. 16. Select the Log check box to store the header information of a packet on the Routing Engine. 17. Select the Syslog check box to log an alert for the packet. 18. Select the Sample check box to sample the packet traffic. 19. Select the Port Mirror check box to port-mirror the packets. 20. From the Loss Priority list, set the packet loss priority (PLP) to low, medium-low, medium-high, or high. 21. In the Forwarding Class box, enter the packet forwarding class name. 22. From the Prefix Action list, select the prefix specific action.

Table 81: Inet6 Firewall Filter Configuration Details (*continued*)

Task	Your Action
	23. Click Accept next to Then.
	24. Select one of the following: <ul style="list-style-type: none"> • Accept—To accept a packet. • Discard—To discard a packet silently, without sending an ICMP message. • Next—To evaluate the next term in the firewall filter.
	25. Click Policer next to Then.
	26. Select one of the following: <ul style="list-style-type: none"> • policer—To configure a new policer for each filter and select the policer name. • three-color-policer—To configure a tricolor marking policer, <ol style="list-style-type: none"> a. Expand Three Color Policer. b. Click Single Rate next to Three Color Policer. c. Select one of the following: <ul style="list-style-type: none"> • Select single-rate if the named tricolor policer is a single-rate policer. • Select two-rate if the named tricolor policer is a two-rate policer.

Configuring Service Filters for inet6 (NSM Procedure)

To configure the service filters for inet6 in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Firewall > Family > Inet6**.
4. Add or modify settings as specified in [Table 82 on page 171](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 82: inet6 Service Filter Configuration Details

Task	Your Action
Configure service filter.	<ol style="list-style-type: none"> 1. Click Service Filter next to inet. 2. Click Add new entry next to Service Filter. 3. Expand service-filter. 4. In the Name box, enter the name that identifies the service filter.

Table 82: inet6 Service Filter Configuration Details (*continued*)

Task	Your Action
Define term.	<ol style="list-style-type: none"> 1. Click Term next to service-filter. 2. Click Add new entry next to Term. 3. Expand Term. 4. In the Name box, enter the name that identifies the term. 5. In the Comment box, enter the comment for the term. 6. Expand From. 7. In the Comment box, enter the comment. 8. From the listed protocol-independent match conditions, select the filters defined for the inet6 family type. The protocol-independent match conditions are Address, Ah Spi, Destination Address, Destination port, Destination prefix List, Interface Group, Next Header, Interface Set, IP Options, Loss Priority, Port, Prefix List, Protocol, Source Address, Source Port, Source Prefix List, and Esp spi. 9. Click Then next to From. 10. In the Comment box, enter the comment for then. 11. In the Count box, enter the number of packets. 12. Select the Log check box to store the header information of a packet on the Routing Engine. 13. Select the Sample check box to sample the packet traffic. 14. Select the Port Mirror check box to port-mirror the packets. 15. Select one of the following: <ul style="list-style-type: none"> • service—To direct packets for stateful-firewall service. • skip—To let packets bypass stateful-firewall service.

Configuring the Firewall Filter for MPLS Family Type (NSM Procedure)

You can configure firewall filters to filter MPLS packets.

To configure the MPLS firewall filter in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Firewall > Family > MPLS**.
4. Add or modify settings as specified in [Table 83 on page 173](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 83: MPLS Firewall Filter Configuration Details

Task	Your Action
Configure a firewall filter to filter MPLS packets.	<ol style="list-style-type: none">1. Click Filter next to MPLS.2. Click Add new entry next to Filter.3. Expand Filter.4. In the Name box, enter the name that identifies the filter.5. In the Comment box, enter the comment.6. Select the Interface Specific check box to configure interface-specific names for firewall counters.
Configure accounting for firewall filters.	<ol style="list-style-type: none">1. Click Accounting Profile next to filter.2. Click Add new entry next to Accounting Profile.3. In the New accounting-profile window, enter the name to be assigned to the accounting profile.

Table 83: MPLS Firewall Filter Configuration Details (*continued*)

Task	Your Action
Define a firewall filter term.	<ol style="list-style-type: none"> 1. Click Term next to Accounting Profile. 2. Click Add new entry next to Term. 3. Expand Term. 4. In the Name box, enter the name that identifies the term. 5. In the Comment box, enter the comment for the term. 6. From the Filter list, select the name that identifies the filter. 7. Expand From. 8. In the Comment box, enter the comment. 9. From the listed protocol-independent match conditions, select the filters defined for the MPLS family type. The protocol-independent match conditions are Exp, Forwarding Class, Interface, Interface Set, and Loss Priority. 10. Expand Then. 11. In the Comment box, enter the comment for then. 12. In the Count box, enter the number of packets. 13. Select the Sample check box to sample the packet traffic. 14. From the Loss Priority list, set the packet loss priority (PLP) to low, medium-low, medium-high, or high. 15. In the Forwarding Class box, enter the packet forwarding class name. 16. Click Accept next to Then. 17. Select one of the following: <ul style="list-style-type: none"> • Select Accept to accept a packet. • Select Discard to discard a packet silently, without sending an ICMP message. • Select Next to evaluate the next term in the firewall filter. 18. Click Policer next to Then. 19. Select one of the following: <ul style="list-style-type: none"> • Policer—To configure a new policer for each filter and select the policer name. • Select three-color-policer—To configure a tricolor marking policer, <ol style="list-style-type: none"> a. Expand Three Color Policer. b. Click Single Rate next to Three Color Policer. c. Select one of the following: <ul style="list-style-type: none"> • single-rate—If the named tricolor policer is a single-rate policer. • two-rate—If the named tricolor policer is a two-rate policer.

Related Documentation

- [Configuring the Firewall Filter for Any Family Type \(NSM Procedure\) on page 157](#)
- [Configuring Filters for inet Family Type \(NSM Procedure\) on page 163](#)
- [Configuring Filters for inet6 Family Type \(NSM Procedure\) on page 168](#)

Configuring the Firewall Filter for VPLS Family Type (NSM Procedure)

You can configure firewall filters to filter virtual private LAN service (VPLS) packets.

To configure the vpls firewall filter in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Firewall > Family > VPLS**.
4. Add or modify settings as specified in [Table 84 on page 176](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 84: VPLS Firewall Filter Configuration Details

Task	Your Action
Configure a firewall filter to filter VPLS packets.	<ol style="list-style-type: none">1. Click Filter next to VPLS.2. Click Add new entry next to Filter.3. Expand Filter.4. In the Name box, enter the name that identifies the filter.5. In the Comment box, enter the comment.6. Select the Interface Specific check box to configure interface-specific names for firewall counters.
Configure accounting for firewall filters.	<ol style="list-style-type: none">1. Click Accounting Profile next to filter.2. Click Add new entry next to Accounting Profile.3. In the New accounting-profile window, enter the name to be assigned to the accounting profile.

Table 84: VPLS Firewall Filter Configuration Details (*continued*)

Task	Your Action
Define a firewall filter term.	<ol style="list-style-type: none"> 1. Click Term next to Accounting Profile. 2. Click Add new entry next to Term. 3. Expand Term. 4. In the Name box, enter the name that identifies the term. 5. In the Comment box, enter the comment for the term. 6. From the Filter list, select the name that identifies the filter. 7. Expand From. 8. In the Comment box, enter the comment. 9. From the listed protocol-independent match conditions, select the filters defined for the VPLS family type. <p>The protocol-independent match conditions are Destination Mac Address, Destination Port, Dscp, Ether Type, Forwarding Class, Icmp Code, Icmp Type, Interface Group, IP Address, IP Destination Address, IP Precedence, IP Protocol, IP Source Address, Learn Vlan, Ip Priority, Learn Vlan id, Loss Priority, Port, Source Mac Address, Source Port, Traffic Type, User Vlan Ip priority, User Vlan id, Vlan Ether Type.</p> 10. Expand Then. 11. In the Comment box, enter the comment for then. 12. In the Count box, enter the number of packets. 13. Select the Sample check box to sample the packet traffic. 14. From the Loss Priority list, set the packet loss priority (PLP) to low, medium-low, medium-high, or high. 15. In the Forwarding Class box, enter the packet forwarding class name. 16. Select the Port Mirror check box to configure port mirroring for VPLS traffic. 17. Click Accept next to Then. 18. Select one of the following: <ul style="list-style-type: none"> • Accept—To accept a packet. • Discard—To discard a packet silently, without sending an ICMP message. • Next—To evaluate the next term in the firewall filter. 19. Click Policer next to Then. 20. Select one of the following: <ul style="list-style-type: none"> • Policer—To configure a new policer for each filter and select the policer name. • three-color-policer —To configure a tricolor marking policer, <ol style="list-style-type: none"> a. Expand Three Color Policer. b. Click Single Rate next to Three Color Policer. c. Select one of the following: <ul style="list-style-type: none"> • single-rate—If the named tricolor policer is a single-rate policer. • two-rate—If the named tricolor policer is a two-rate policer.

Related Documentation

- [Configuring the Firewall Filter for Any Family Type \(NSM Procedure\) on page 157](#)
- [Configuring the Firewall Filter for Ccc Family Type \(NSM Procedure\) on page 161](#)
- [Configuring the Firewall Filter for MPLS Family Type \(NSM Procedure\) on page 172](#)

Configuring a Policer for a Firewall Filter

You can configure policers to rate limit traffic on a device. After you configure a policer, you can include it in an ingress firewall filter configuration.

When you configure a firewall filter, you can specify a policer action for any term or terms within the filter. All traffic that matches a term that contains a policer action goes through the policer that the term references. Each policer that you configure includes an implicit counter. To get term-specific packet counts, you must configure a new policer for each filter term that requires policing.

The following policer limits apply on the switch:

- A maximum of 512 policers can be configured for port firewall filters.
 - A maximum of 512 policers can be configured for VLAN and Layer 3 firewall filters.
1. In the navigation tree, select **Device Manager > Devices**. In Device Manager, select the device for which you want to configure a policer.
 2. In the configuration tree, expand Firewall.
 3. Perform the configuration tasks as described in [Table 85 on page 178](#).



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See [Updating Devices](#) for more information.

Table 85: Configuring a Policer for a Firewall Filter

Task	Action
Create the policer for expedited forwarding, and give the policer a name—for example, ef-policer.	Select Policer and click Add new entry . In the Policer name box, type ef-policer .
Set the burst limit for the policer—for example, 2k.	1. Select If exceeding .
Set the bandwidth limit or percentage for the bandwidth allowed for this type of traffic—for example, use a bandwidth percent of 10.	2. In the Burst Size Limit box, type a limit for the burst size allowed—for example, 2k. 3. Select Bandwidth Limit , select bandwidth-limit . 4. In the box, type 10. 5. Click OK .

Table 85: Configuring a Policer for a Firewall Filter (*continued*)

Enter the loss priority for packets exceeding the limits established by the policer—for example, high.

1. Select **Then**.
 2. In the **Comment** field, enter **high**.
 3. Click **OK**.
-

Configuration of Forwarding Options

- [Configuring Accounting Options \(NSM Procedure\) on page 181](#)
- [Configuring the Extended DHCP Agent \(NSM Procedure\) on page 183](#)
- [Specifying Address Family for Filters \(NSM Procedure\) on page 191](#)
- [Configuring Load Balancing Using Hash Key \(NSM Procedure\) on page 192](#)
- [Configuring Helpers \(NSM Procedure\) on page 193](#)
- [Configuring Per-Flow and Per-Prefix Load Balancing \(NSM Procedure\) on page 202](#)
- [Configuring Port Mirroring \(NSM Procedure\) on page 203](#)

Configuring Accounting Options (NSM Procedure)

You can configure accounting for traffic passing through the router, containing a Monitoring Services PIC or an Adaptive Services PIC. Configuring an accounting option includes configuring the output flow aggregation and configuring the interface that sends out monitored information.

To configure an accounting group in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Forwarding Options**.
4. Select **Accounting**.
5. Add or modify the settings as specified in [Table 86 on page 181](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 86: Accounting Options Configuration Details

Task	Your Action
Configure an accounting group.	<ol style="list-style-type: none"> 1. Click Add new entry next to Accounting. 2. In the Name box, type the name of the accounting group.

Table 86: Accounting Options Configuration Details (*continued*)

Task	Your Action
Configure flow output.	<ol style="list-style-type: none"> 1. Expand Output. 2. In the Comment box, enter the comment for the output. 3. From the Aggregate export Interval list, select the time. 4. From the Flow Inactive Timeout list, select the interval before a flow is considered inactive. 5. From the Flow Active Timeout list, select the interval before exporting an active flow.
Configure flow aggregation.	<ol style="list-style-type: none"> 1. Click Add new entry next to cflowd. 2. In the Name box, Enter the IP address or identifier of the host system (the workstation running the cflowd utility). 3. From the Port list, select the UDP port number on the cflowd host system. 4. From the Version list, select the version format of the aggregated flows exported to a cflowd server. 5. From the Autonomous System Type, select the type of AS numbers that cflowd exports. <ul style="list-style-type: none"> • origin—Export origin AS numbers of the packet source address in the Source Autonomous System cflowd field. • peer—Export peer AS numbers through which the packet passed in the Source Autonomous System cflowd field. Default: origin 6. Click Aggregation next to cflowd. 7. Select Autonomous System check box to aggregate by autonomous system (AS) type. 8. Select the Protocol Port check box to aggregate by protocol and port number. 9. Select the Source Prefix check box to aggregate by source prefix. 10. Select the Destination Prefix check box to aggregate by destination prefix. 11. Expand Aggregation. 12. Click Source Destination Prefix next to Aggregation. 13. Select the Caida Compliant check box to record source and destination mask length values in compliance with the Version 2.1b1 release of the cflowd application from the Cooperative Association for Internet Data Analysis (CAIDA).
Configure the output interface.	<ol style="list-style-type: none"> 1. Expand Output. 2. Click Interface next to Output. 3. Click Add new entry next to Interface. 4. In the Name box, enter the name of the accounting interfaces. 5. In the Comment box, enter the comment for the interface. 6. From the Engine Id list, select the identity of the accounting interface. 7. From the Engine Type list, select the type of this accounting interface. 8. In the Source Address box, enter the address used for generating packets.

- Related Documentation**
- [Configuring the Extended DHCP Agent \(NSM Procedure\) on page 183](#)
 - [Specifying Address Family for Filters \(NSM Procedure\) on page 191](#)
 - [Configuring Load Balancing Using Hash Key \(NSM Procedure\) on page 192](#)

Configuring the Extended DHCP Agent (NSM Procedure)

See the following sections for details on configuring the extended Dynamic Host Configuration Protocol agent.

- [Configuring Authentication Support for the DHCP Relay Agent \(NSM Procedure\) on page 183](#)
- [Configuring Group \(NSM Procedure\) on page 184](#)
- [Overriding the Default Configuration Settings for the Extended DHCP Relay Agent \(NSM Procedure\) on page 185](#)
- [Configuring Relay Option 60 Information for Forwarding Client Traffic to Specific DHCP Servers \(NSM Procedure\) on page 187](#)
- [Configuring Relay Option 82 for a DHCP Server \(NSM Procedure\) on page 188](#)
- [Specifying the Name of a Group of DHCP Server Addresses for Use by the Extended DHCP Relay Agent \(NSM Procedure\) on page 189](#)
- [Configuring Operations for Extended DHCP Relay Agent Processes \(NSM Procedure\) on page 190](#)

Configuring Authentication Support for the DHCP Relay Agent (NSM Procedure)

You can configure the parameters the router sends to the external Authentication, Authorization, and Accounting server. A group configuration takes precedence over a global DHCP relay or DHCP local server configuration.

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Forwarding Options > DHCP Relay**.
4. Select **Authentication**.
5. Add or modify Authentication settings as specified in [Table 87 on page 184](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 87: Authentication Configuration Details

Task	Your Action
Configure the password.	<ol style="list-style-type: none"> 1. Expand Authentication. 2. In the Comment box, enter the comment for authentication. 3. In the Password box, enter the password to be sent to the external AAA authentication server for subscriber authentication.
Configure the username.	<ol style="list-style-type: none"> 1. Click Username Include next to Authentication. 2. In the Comment box, enter the comment. 3. In the Delimiter box, enter the character used as the delimiter between the concatenated components of the username. You cannot use the semicolon (;) as a delimiter. 4. In the Domain Name box, enter the domain name that is concatenated with the username during the subscriber authentication process. 5. In the User prefix box, enter the user prefix concatenated with the username during the subscriber authentication process. <ul style="list-style-type: none"> • Select Mac Address check box if the MAC address from the client PDU be concatenated with the username during the subscriber authentication process. • Select Logical System Name check box if the logical system name be concatenated with the username during the subscriber authentication process. • Select Routing Instance Name check box if the routing instance name be concatenated with the username during the subscriber authentication process. • Select Option 60 check box if the payload of the Option 60 (Vendor Class Identifier) from the client PDU be concatenated with the username during the subscriber authentication process. • Select Circuit Type check box if the circuit type be concatenated with the username during the subscriber authentication process. 6. Click Option 82 next to Username Include. 7. Select the Circuit-id or remote id check box to select the string for the agent circuit ID suboption.

Configuring Group (NSM Procedure)

You can specify the name of a group of interfaces that have a common DHCP relay agent configuration. A group must contain at least one interface.

To configure group of interfaces:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Forwarding Options > DHCP Relay**.
4. Select **Group**.

5. Add or modify settings as specified in [Table 88 on page 185](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 88: Group Configuration Details

Task	Your Action
Configuring authentication support for the DHCP relay agent.	See “Configuring Authentication Support for the DHCP Relay Agent (NSM Procedure)” on page 183
Specify one or more interfaces, or a range of interfaces, that are within a specified group on which the DHCP local server is enabled.	<ol style="list-style-type: none"> 1. Click Add new entry next to Group. 2. Expand Group. 3. Click Interface next to group. 4. Click Add new entry next to Interface. 5. From the Name list, select the name of the interface. 6. In the Comment box, enter the comment. 7. From the Upto list, select the upper end of the range of interfaces. 8. Select the Exclude check box to exclude an interface or a range of interfaces from the group.
Overriding the default configuration settings for the extended DHCP relay agent.	See “Overriding the Default Configuration Settings for the Extended DHCP Relay Agent (NSM Procedure)” on page 185 .
Configuring relay option 60 Information for forwarding client traffic to specific DHCP servers.	See “Configuring Relay Option 60 Information for Forwarding Client Traffic to Specific DHCP Servers (NSM Procedure)” on page 187 .
Configuring relay option 82 for a DHCP server.	See “Configuring Relay Option 82 for a DHCP Server (NSM Procedure)” on page 188 .

Overriding the Default Configuration Settings for the Extended DHCP Relay Agent (NSM Procedure)

You can override the default configuration settings for the extended DHCP relay agent. Specifying the overrides statement with no subordinate statements removes all DHCP relay agent overrides at that hierarchy level.

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, select **Forwarding Options > DHCP Relay**.
4. Select **Overrides**.

5. Add or modify settings as specified in [Table 89 on page 186](#).

6. Click one:

- OK—Saves the changes.
- Cancel—Cancels the modifications.

Table 89: Overrides Configuration Details

Option	Function	Your Action
Comment	Specifies the comment for the override.	In the Comment box, enter the comment.
always-write-giaddr	Overwrites the gateway IP address (giaddr) of every DHCP packet with the gateway IP address of the DHCP relay agent before forwarding the packet to the DHCP server.	Select the Always Write Giaddr check box.
always-write-option-82	Overrides the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server.	Select the Always Write Option 82 check box.
layer2-unicast-replies	Overrides the setting of the broadcast bit in DHCP request packets and instead use the Layer 2 unicast transmission method to transmit DHCP Offer reply packets and DHCP ACK reply packets from the DHCP server to DHCP clients during the discovery process.	Select the Layer2 Unicast Replies check box.
trust-option-82	Enables processing of DHCP client packets that have a gateway IP address (giaddr) of 0 (zero) and contain option 82 information.	Select the Trust Option 82 check box.
disable-relay	Disables DHCP relay on specific interfaces in a group.	Select the disable-relay check box.
Interface client limit	Specifies the interface client limit.	From the Interface Client Limit list, select the interface client limit.
No Arp	Disable Address Resolution Protocol entry for this client.	Select the No Arp check box to drop the unwanted ARP requests.

Configuring Relay Option 60 Information for Forwarding Client Traffic to Specific DHCP Servers (NSM Procedure)

You can configure the extended DHCP relay agent to use the DHCP vendor class identifier option (option 60) in DHCP client packets to forward client traffic to specific DHCP servers or to drop selected DHCP client packets. This feature is useful in network environments where DHCP clients access services provided by multiple vendors and DHCP servers.

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the tree, expand **Forwarding Options > DHCP Relay**.
4. Select **Relay Option 60**.
5. Add or modify settings as specified in [Table 90 on page 187](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 90: Relay Option 60 Configuration Details

Task	Your Action
Configure the match criteria when you use the DHCP vendor class identifier option (option 60) in DHCP client packets to forward client traffic to specific DHCP servers.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment for the relay option 60. 2. Click Vendor Option next to Relay Option 60. 3. In the Comment box, enter the comment for Vendor Option. 4. Click Default Relay Server Group next to Vendor Option and select the name of the default DHCP relay server group. <ul style="list-style-type: none"> • Select Drop to drop DHCP client packets that contain an option 60 string that matches the ASCII or hexadecimal match string and match criteria.

Table 90: Relay Option 60 Configuration Details (*continued*)

Task	Your Action
Configure the match string using the Equals and Starts With options.	<ol style="list-style-type: none"> 1. Expand Equals and Starts With next to Default Relay Server Group. 2. Click Add new entry next to Equals and Starts With. 3. Expand ascii. 4. In the name box, enter the ASCII match string of 1 through 255 alphanumeric characters. 5. Click Relay Server Group next to ascii. 6. In the Comment box, enter the comment for the ASCII. 7. Select the name of the extended DHCP local server group and enter the group name in the box. <ul style="list-style-type: none"> • Select Drop to drop DHCP client packets that contain an option 60 string that matches the ASCII or hexadecimal match string and match criteria. 8. Click Hexadecimal next to ascii. 9. Click Add new entry next to Hexadecimal. 10. Expand hexadecimal. 11. In the Name box, enter the Hexadecimal match string. 12. Click Relay Server Group next to ascii. 13. In the Comment box, enter the comment for the ASCII. 14. Select the name of the extended DHCP local server group and enter the group name in the box. <ul style="list-style-type: none"> • Select Drop to drop DHCP client packets that contain an option 60 string that matches the ASCII or hexadecimal match string and match criteria.

Configuring Relay Option 82 for a DHCP Server (NSM Procedure)

You can enable or disable the insertion of the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server.

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Forwarding Options > DHCP Relay**.
4. Select **Relay Option 82**.
5. Add or modify settings as specified in [Table 91 on page 189](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 91: Relay option 82 Configuration Details

Task	Your Action
Enable or disable the insertion of the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server.	<ol style="list-style-type: none"> 1. Expand Relay Option 82. 2. In the Comment box, enter the comment for the relay option 82. 3. Click Circuit Id next to Relay Option 82. 4. In the Comment box, enter the comment. 5. Click Prefix next to Circuit Id. 6. In the Comment box, enter the comment. 7. Select the prefix to be added to the base option 82 agent circuit ID information in DHCP packets destined for a DHCP server. The prefix can consist of any combination of the hostname, logical system name, and routing instance name.

Specifying the Name of a Group of DHCP Server Addresses for Use by the Extended DHCP Relay Agent (NSM Procedure)

You can specify the name of a group of DHCP server addresses for use by the extended DHCP relay agent.

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Forwarding Options > DHCP Relay**.
4. Select **Server Group**.
5. Add or modify settings as specified in [Table 92 on page 190](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 92: Sever Group Configuration Details

Task	Your Action
Specify the name of a group of DHCP server addresses for use by the extended DHCP relay agent.	<ol style="list-style-type: none"> 1. Expand Server Group. 2. In the Comment box, enter the comment for the server group. 3. Click Server Group next to Server Group. 4. Click Add new entry next to Server Group. 5. Expand Server-Group. 6. In the Name box, enter the name of the group of DHCP server addresses. 7. In the Comment box, enter the comment for the server group. 8. Click Address next to Server-Group. 9. Click Add new entry next to Address. 10. In the Name box, enter the IP address of the DHCP server belonging to this named server group. You can configure a maximum of five IP addresses per named server group.

Configuring Operations for Extended DHCP Relay Agent Processes (NSM Procedure)

You can configure tracing operations for extended DHCP relay agent processes.

To configure tracing operations for DHCP relay agent in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Forwarding Options > DHCP Relay**.
4. Select **Traceoptions**.
5. Add or modify settings as specified in [Table 93 on page 190](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 93: DHCP Relay Traceoptions Configuration Details

Task	Your Action
Configure tracing operations for extended DHCP relay agent processes.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment for the traceoptions. 2. Select the No Remote Trace check box to disable remote tracing globally or for a specific tracing operation.

Table 93: DHCP Relay Traceoptions Configuration Details (*continued*)

Task	Your Action
Specify the name of the file to receive the output of the tracing operation and specifies the maximum number of trace files.	<ol style="list-style-type: none"> 1. Click File next to Traceoptions. 2. In the Comment box, enter the comment for the file. 3. In the Filename box, enter the name of the file to receive the output of the tracing operation. 4. In the Size box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). 5. From the Files list, select the maximum number of trace files. Range: 2 through 1000. 6. Select one of the following: <ul style="list-style-type: none"> • world-readable—To enable unrestricted file access • no-world-readable—To restrict file access to owner 7. In the Match box, enter the regular expression.
Specify the tracing operation to perform. To specify more than one tracing operation, include multiple flag statements.	<ol style="list-style-type: none"> 1. Click Flag next to Traceoptions. 2. Click Add new entry next to Flag. 3. From the Name list, select the flag. 4. In the Comment box, enter the comment for the flag.

Specifying Address Family for Filters (NSM Procedure)

You can specify address family for filters using this option. You can specify inet for IP version 4 (IPv4), inet6 for IP version 6 (IPv6), mpls for MPLS, or vpls for virtual private LAN service (VPLS).

To specify the address family for filters in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Forwarding Options > Family**.
4. Add or modify settings as specified in [Table 94 on page 191](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 94: Address Family Details

Task	Your Action
Apply a forwarding table filter to a forwarding table.	<ol style="list-style-type: none"> 1. Click Inet, Inet6, or Mpls. 2. Click Filter next to Inet, Inet6, or Mpls. 3. In the Comment box, enter the comment. 4. From the Input list, select the name of the applied filter. 5. From the Output list, select the name of the applied filter.

Table 94: Address Family Details (*continued*)

Task	Your Action
Apply a forwarding table filter for VPLS.	<ol style="list-style-type: none"> 1. Click Vpls next to Family. 2. Expand Vpls. 3. Click Filter next to Vpls. 4. In the Comment box, enter the comment. 5. From the Input list, select the name of the applied filter. 6. Click Flood next to Vpls. 7. In the Comment box, enter the comment. 8. From the Input list, select the name of the applied filter.

Related Documentation

- [Configuring the Extended DHCP Agent \(NSM Procedure\) on page 183](#)
- [Configuring Per-Flow and Per-Prefix Load Balancing \(NSM Procedure\) on page 202](#)
- [Configuring Port Mirroring \(NSM Procedure\) on page 203](#)

Configuring Load Balancing Using Hash Key (NSM Procedure)

When there are multiple equal-cost paths to the same destination for the active route, the Junos OS uses a hash algorithm to choose one of the next-hop addresses to install in the forwarding table. Whenever the set of next hops for a destination changes in any way, the next-hop address is rechosen using the hash algorithm.

You can select which packet header data to use for per-flow load balancing using the hash-key option.

To configure load balancing in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Forwarding Options > Hash Key**.
4. Add or modify settings as specified in [Table 95 on page 193](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 95: Load Balance Configuration Details

Task	Your Action
Configure layer information for the load-balancing specification. Only the IPv4 protocol is supported.	<ol style="list-style-type: none"> 1. Click Inet next to Family. 2. Click Layer 3 next to Inet. 3. In the Comment box, enter the comment. 4. Select the Destination Address check box to include the destination-address MAC information in the hash key. 5. Click Layer 4 next to Inet. 6. In the Comment box, enter the comment.
Configure load balancing based on MPLS labels. Only the IPv4 protocol is supported.	<ol style="list-style-type: none"> 1. Click Mpls next to Family. 2. Expand Mpls. 3. Click Payload next to Mpls. 4. In the Comment box, enter the comment. 5. Click IP next to Payload. 6. In the Comment box, enter the comment. 7. Expand IP. 8. Click Layer 3 Only next to IP. 9. Select layer-3-only to include only Layer 3 IP information. 10. Select port-data to include the source and destination port field information. <ol style="list-style-type: none"> a. In the Comment box, enter the comment. b. Select Source Msb to Include the most significant byte of the source port. c. Select Source Lsb to Include the least significant byte of the source port. d. Select Destination Msb to include the most significant byte of the destination port. e. Select Destination Lsb to Include the least significant byte of the destination port.
Configure load balancing based on Layer 2 media access control information.	<ol style="list-style-type: none"> 1. Click Multiservice next to Mpls. 2. In the Comment box, enter the comment. 3. Select Source Mac to include the source-address MAC information in the hash key. 4. Select Destination Mac to include the destination-address MAC information in the hash key.

Related Documentation

- [Configuring Accounting Options \(NSM Procedure\) on page 181](#)
- [Configuring Helpers \(NSM Procedure\) on page 193](#)
- [Configuring Per-Flow and Per-Prefix Load Balancing \(NSM Procedure\) on page 202](#)

Configuring Helpers (NSM Procedure)

You can enable Trivial File Transfer Protocol (TFTP) or Domain Name System (DNS) request packet forwarding, or configure the router or interface to act as a Dynamic Host

Configuration Protocol (DHCP) or Bootstrap Protocol (BOOTP) relay agent. You use only one server address per interface or global configuration. See the following topics:

- [Configuring a Router or Interface to Act as a Bootstrap Protocol Relay Agent on page 194](#)
- [Enabling DNS Request Packet Forwarding on page 197](#)
- [Configuring a Port for a DHCP or BOOTP Relay Agent on page 199](#)
- [Configuring Tracing Operations for BOOTP, DNS, and TFTP Packet Forwarding on page 201](#)

Configuring a Router or Interface to Act as a Bootstrap Protocol Relay Agent

You can configure a router or interface to act as a Dynamic Host Configuration Protocol (DHCP) or bootstrap protocol (BOOTP) relay agent using this option.

To configure a BOOTP relay agent in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Forwarding Options > Helpers > BOOTP**.
4. Add or modify settings as specified in [Table 96 on page 194](#).
5. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 96: BOOTP Configuration Details

Task	Your Action
Configures a router or interface to act as a DHCP or BOOTP relay agent.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment. 2. Select the Relay Agent check box to configure router as a BOOTP relay agent. 3. From the Maximum Hop Count list, select the maximum number of hops allowed. Default: 4 hops 4. From the Minimum Wait Time list, select the minimum time allowed. Default: 3 seconds 5. From the Client Response Ttl list, select the IIP time-to-live (TTL) value in DHCP response packets sent to a DHCP client.

Table 96: BOOTP Configuration Details (*continued*)

Task	Your Action
Configure DHCP option 82.	<ol style="list-style-type: none"> 1. Click Dhcp Option82 next to Bootp. 2. In the Comment box, enter the comment. 3. Select the Disable check box to disable DHCP option 82 on this VLAN. 4. Click Circuit Id next to Dhcp Option82. 5. In the Comment box, enter the comment. 6. From the Prefix list, select the prefix <ul style="list-style-type: none"> • hostname—Set hostname as the prefix. 7. Select the Use Interface Description check box to use interface description instead of name. 8. Select the Use Vlan Id check box to use vlan id. 9. Click Remote Id next to Dhcp Option82. 10. In the Comment box, enter the comment. 11. From the Prefix list, select the prefix <ul style="list-style-type: none"> • none—Set no prefix. • hostname—Set hostname as the prefix. • mac—Set chassis MAC as the prefix. 12. Select the Use Interface Description check box to use interface description instead of name. 13. In the Use String check box, enter the raw string instead of the default remote ID. 14. Click Vendor Id next to Dhcp Option82. 15. In the Comment box, enter the comment. 16. In the Use String check box, enter the raw string instead of the default remote ID.

Table 96: BOOTP Configuration Details (*continued*)

Task	Your Action
Specify the interface for a DHCP and BOOTP relay agent.	<ol style="list-style-type: none"> 1. Click Interface next to BOOTP. 2. Click Add new entry next to Interface. 3. Expand Interface. 4. In the Name box, enter the interface for a DHCP and BOOTP relay agent. 5. In the Comment box, enter the comment. 6. Select the No Listen check box to disable recognition of DNS requests or stop packets from being forwarded on a logical interface, a group of logical interfaces, or a router. 7. Select the Broadcast check box to issue the DHCP or BOOTP request as a broadcast message. 8. In the Descriptions box, enter the description of BOOTP, DHCP, Domain Name System (DNS), or Trivial File Transfer Protocol (TFTP) service, or of an interface that is configured for the service. 9. From the Maximum Hop Count list, select the maximum number of hops allowed. Default: 4 hops 10. From the Minimum Wait Time list, select the minimum time allowed. Default: 3 seconds 11. From the Client Response Ttl list, select the IIP time-to-live (TTL) value in DHCP response packets sent to a DHCP client.

Table 96: BOOTP Configuration Details (*continued*)

Task	Your Action
Configure the router to act as a DHCP and BOOTP relay agent.	<ol style="list-style-type: none"> 1. Click Server next to Interface. 2. Click Add new entry next to Server. 3. Expand Server. 4. In the Name box, enter the server identifier. 5. In the Comment box, enter the comment. 6. Click Logical System next to Server. 7. Click Add new entry next to Logical System. 8. Expand logical-system. 9. In the Name box, enter the logical system name. 10. In the Comment box, enter the comment. 11. Click Routing Instance next to logical-system. 12. Click Add new entry next to Routing Instance. 13. In the New routing-instance window, enter the routing instance name. 14. Click Routing Instance next to server. 15. Click Add new entry next to Routing Instance. 16. In the New routing-instance window, enter the routing instance name. 17. Click Server next to BOOTP. 18. Click Add new entry next to Server. 19. Expand Server. 20. Click Logical System next to Server. 21. Click Add new entry next to Logical System. 22. In the Name box, enter the logical system name. 23. In the Comment box, enter the comment. 24. Click Routing Instance next to logical-system. 25. Click Add new entry next to Routing Instance. 26. In the New routing-instance window, enter the routing instance name. 27. Click Routing Instance next to server. 28. Click Add new entry next to Routing Instance. 29. In the New routing-instance window, enter the routing instance name.

Enabling DNS Request Packet Forwarding

You can configure the router to support Domain Name System (DNS) and Trivial File Transfer Protocol (TFTP) packet forwarding for IPv4 traffic, which allows clients to send DNS or TFTP requests to the router. The responding DNS or TFTP server recognizes the client address and sends a response directly to that address. By default, the router ignores DNS and TFTP request packets.

To enable DNS request packet forwarding in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Forwarding Options > Helpers > Domain**.



NOTE: For configuring TFTP, expand **Forwarding Options > Helpers > TFTP**.

4. Add or modify settings as specified in [Table 97 on page 199](#).
5. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 97: DNS and TFTP Configuration Details

Task	Your Action
Specify the interface for monitoring and forwarding DNS or TFTP requests.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment. 2. In the Description box, enter the description of BOOTP, DHCP, Domain Name System (DNS), or Trivial File Transfer Protocol (TFTP) service, or of an interface that is configured for the service. 3. Click Interface next to Domain. 4. Click Add new entry next to Interface. 5. Expand Interface. 6. In the Name box, enter the interface for a DHCP and BOOTP relay agent. 7. In the Comment box, enter the comment. 8. Select the No Listen check box to disable recognition of DNS requests or stop packets from being forwarded on a logical interface, a group of logical interfaces, or a router. 9. Select the Broadcast check box to issue the DHCP or BOOTP request as a broadcast message. 10. In the Descriptions box, enter the description of BOOTP, DHCP, Domain Name System (DNS), or Trivial File Transfer Protocol (TFTP) service, or of an interface that is configured for the service. 11. Click Server next to Interface. 12. In the Comment box, enter the comment. 13. In the Address box, enter the address of the server. 14. Expand Server. 15. Click Logical System next to Server. 16. Select logical-system or routing-instance. 17. Click Server next to Domain. 18. In the Comment box, enter the comment. 19. In the Address box, enter the address of the server. 20. Expand Server. 21. Click Logical System next to Server. 22. Select logical-system or routing-instance.

Configuring a Port for a DHCP or BOOTP Relay Agent

You can configure a port for a DHCP or BOOTP relay agent using this option.

To configure a port for a DHCP or BOOTP relay agent in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Forwarding Options > Helpers**.
4. Select **Port**.

5. Add or modify settings as specified in [Table 98 on page 200](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 98: Port Configuration Details

Task	Your Action
Configuring a Port.	<ol style="list-style-type: none"> 1. From the Name list, select the port number. 2. In the Comment box, enter the comment. 3. In the Description box, enter the description of BOOTP, DHCP, Domain Name System (DNS), or Trivial File Transfer Protocol (TFTP) service, or of an interface that is configured for the service. 4. Expand Port. 5. Click Interface next to Domain. 6. Click Add new entry next to Interface. 7. Expand Interface. 8. In the Name box, enter the interface for a DHCP and BOOTP relay agent. 9. In the Comment box, enter the comment. 10. Select the No Listen check box to disable recognition of DNS requests or stop packets from being forwarded on a logical interface, a group of logical interfaces, or a router. 11. Select the Broadcast check box to issue the DHCP or BOOTP request as a broadcast message. 12. In the Descriptions box, enter the description of BOOTP, DHCP, Domain Name System (DNS), or Trivial File Transfer Protocol (TFTP) service, or of an interface that is configured for the service. 13. Click Server next to Interface. 14. Expand Server. 15. In the Comment box, enter the comment. 16. In the Address box, enter the address of the server. 17. Click Logical System next to Server. 18. Select the corresponding logical system. 19. Click Server next to Port. 20. In the Comment box, enter the comment. 21. In the Address box, enter the address of the server. 22. Click Logical System next to Server. 23. Select the corresponding logical system.

Configuring Tracing Operations for BOOTP, DNS, and TFTP Packet Forwarding

You can configure tracing operations for BOOTP, DNS, and TFTP packet forwarding using this option. BOOTP, DNS, and TFTP forwarding tracing operations track all BOOTP, DNS, and TFTP operations and record them in a log file. The logged error descriptions provide detailed information to help you solve problems faster.

To configure tracing operations in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Forwarding Options > Helpers > TFTP**.
4. Select **Traceoptions**.
5. Add or modify settings as specified in [Table 99 on page 201](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 99: Traceoptions Configuration Details

Task	Your Action
Define tracing operations for event policy.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment for the traceoptions. 2. Select the No Remote Trace check box to disable remote tracing globally or for a specific tracing operation. 3. From the Level list, select the level.
Specify the name of the file to receive the output of the tracing operation and the maximum number of trace files.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment for the file. 2. In the Filename box, enter the name of the file to receive the output of the tracing operation. 3. In the Size box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). 4. From the Files list, select the maximum number of trace files. Range: 2 through 1000. Default: 3 5. Select one of the following: <ul style="list-style-type: none"> • world-readable—To enable unrestricted file access • no-world-readable—To restrict file access to owner. This is the default setting. 7. In the Matchbox, enter the regular expression.
Specify the tracing operation to perform	<ol style="list-style-type: none"> 1. Click Add new entry next to Flag. 2. From the Name list, select the flag. 3. In the Comment box, enter the comment for the flag.

Configuring Per-Flow and Per-Prefix Load Balancing (NSM Procedure)

You can enable per-prefix or per-flow load balancing so that the router elects a next hop independently of the route selected by other routers.

To configure load balancing in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Forwarding Options > Load Balance**.
4. Add or modify settings as specified in [Table 100 on page 202](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 100: Load Balancing Configuration Details

Task	Your Action
Enable per-flow load balancing based on hash values.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment. 2. Select the Indexed Next Hop check box to generate a permuted index of next-hop entries for unicast and aggregate next hops. 3. Click Per Flow next to Load Balance. 4. In the Comment box, enter the comment for per-flow. 5. Select the Hash Seed check box to configure based on the hash value.
Configure the hash parameter for per-prefix load balancing.	<ol style="list-style-type: none"> 1. Click Per Prefix next to Load Balance. 2. In the Comment box, enter the comment for per prefix. 3. From the Hash Seed list, select the hash value. Range: 0 through 65,535 Default: 0

Related Documentation

- [Configuring Port Mirroring \(NSM Procedure\) on page 203](#)
- [Configuring Helpers \(NSM Procedure\) on page 193](#)
- [Configuring Load Balancing Using Hash Key \(NSM Procedure\) on page 192](#)

Configuring Port Mirroring (NSM Procedure)

On all M Series, T Series, and MX Series routers, you can send a copy of an IPv4 or IPv6 packet from the routers to an external host address or a packet analyzer for analysis. This is known as port mirroring. In addition, on the M7i, M10i, M120, M320 and MX Series routers only, you can configure port mirroring for VPLS traffic. VPLS port mirroring is supported only on M7i and M10i routers with Enhanced CFEB (CFEB-E). In addition, on M320 routers, VPLS port mirroring is supported only on Enhanced III Flexible PIC Concentrators (FPCs).

To configure port mirroring in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Forwarding Options > Port Mirroring**.
4. Add or modify settings as specified in [Table 101 on page 204](#).
5. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 101: Port Mirroring Configuration Details

Task	Your Action
Configure the address type family to sample for port mirroring.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment for the port mirroring. 2. Select the Mirror Once check box to configure the router to mirror packets only once. 3. Click Family next to Port Mirroring. 4. Expand Family. 5. Click Inet or Inet6 next to Family. 6. Click Output. 7. In the Comment box, enter the comment. 8. Select the No Filter Check check box to disable filter checking on the port-mirroring interface. 9. Click Interface next to Output. 10. Click Add new entry next to Interface. 11. Expand Interface. 12. In the Name box, enter the name of the interface. 13. In the Comment box, enter the comment. 14. Click Next Hop next to interface. 15. Click Add new entry next to Next Hop. 16. In the Name box, enter the IP address of the next-hop router. 17. In the Comment box, enter the comment. 18. Click Vpls next to Family. 19. In the Comment box, enter the comment. 20. Click Output next to Vpls. 21. In the Comment box, enter the comment. 22. In the Interface box, enter the name of the interface. 23. Select the No Filter Check check box to disable filter checking on the port-mirroring interface.
Configure input packet properties for port mirroring.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment for input. 2. From the Rate list, select the ratio of the number of packets to be sampled. For example, if you specify a rate of 10, every tenth packet (1 packet out of 10) is sampled. Range: 1 through 65,535 3. From the Run Length list, select the number of samples following the initial trigger event. This allows you to sample packets following those already being sampled. Range: 0 through 20 Default: 0
Configure a port-mirroring instance.	<ol style="list-style-type: none"> 1. Click Instance next to Port Mirroring. 2. Click Add new entry next to Instance. 3. In the Name box, enter the name of the port-mirroring instance. 4. To configure the address type family to sample for port mirroring, refer Table 101 on page 204. 5. To configure input packet properties for port mirroring, refer Table 101 on page 204.

Table 101: Port Mirroring Configuration Details (*continued*)

Task	Your Action
Configure traffic sampling tracing operations.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment for traceoptions. 2. Click File next to Traceoptions. 3. In the Comment box, enter the comment for the file. 4. In the Filename box, enter the name of the file containing the trace information. Default: /var/log/sampled 5. In the Size box, enter the maximum size of each traffic sampling file or trace log file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). Syntax: xk to specify KB, xm to specify MB, or xg to specify GB Range: 10 KB through the maximum file size supported on your router Default: 1 MB for sampling data; 128 KB for log information 6. From the Files list, select the maximum number of traffic sampling or trace log files. Range: 1 through 100 files Default: 5 files for sampling output; 10 files for trace log information 7. Select one of the following: <ul style="list-style-type: none"> • world-readable—To enable unrestricted file access. • no-world-readable—To restrict file access to owner.

Related Documentation

- [Configuring Per-Flow and Per-Prefix Load Balancing \(NSM Procedure\) on page 202](#)
- [Configuring Load Balancing Using Hash Key \(NSM Procedure\) on page 192](#)
- [Specifying Address Family for Filters \(NSM Procedure\) on page 191](#)

Configuration of Interfaces

- [Configuring Interfaces on the Routing Platform \(NSM Procedure\) on page 207](#)
- [Configuring Interface set on the Routing Platform \(NSM Procedure\) on page 235](#)
- [Configuring Trace Options on the Routing Platform \(NSM Procedure\) on page 236](#)

Configuring Interfaces on the Routing Platform (NSM Procedure)

You can configure the interfaces on the router using this option. See the following topics:

- [Configuring Interface Properties \(NSM Procedure\) on page 207](#)
- [Damping Interface Transitions \(NSM Procedure\) on page 209](#)
- [Configuring Receive Bucket Properties on Interfaces \(NSM Procedure\) on page 210](#)
- [Configuring Tracing Operations of an Individual Router Interface \(NSM Procedure\) on page 210](#)
- [Configuring Transmit Leaky Bucket Properties \(NSM Procedure\) on page 211](#)
- [Configuring Logical Interface Properties \(NSM Procedure\) on page 212](#)
- [Configuring Protocol Family Information for the Logical Interface \(NSM Procedure\) on page 215](#)
- [Configuring the Traffic Shaping Profile \(NSM Procedure\) on page 233](#)

Configuring Interface Properties (NSM Procedure)

You can configure interfaces on the router using this option. The management and internal Ethernet interfaces are automatically configured. You must configure all other interfaces.

To configure interfaces in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.



NOTE: You can also configure interfaces through the Quick Configuration tab. Also, you can configure interfaces in a Config group and apply them to the interface node.

5. Add or modify settings as specified in [Table 102 on page 208](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 102: Interface Properties Configuration Details

Task	Your Action
Configure Interfaces.	<ol style="list-style-type: none"> 1. Click Add Interface next to Interface. 2. In the Add Interface Dialog box, enter the interface name. 3. From the Name list, select the interface name. 4. In the Comment box, enter the comment. 5. In the Description box, enter the text to describe the interface. If the text includes spaces, enclose the entire text in quotation marks. 6. From the Accounting Profile list, select the name of the accounting profile. 7. Select per-unit-scheduler to enable association of scheduler map names with logical interfaces. 8. Select Hierarchical-scheduler to enable the use of hierarchical scheduler. 9. From the Native Vlan Id list, select the VLAN ID number. 10. From the Speed list, select the speed. 11. From the Mtu list, select the maximum transmission unit (MTU) size for the media or protocol. 12. From the Encapsulation list, select the encapsulation type. 13. In the Bandwidth box, enter the peak rate. 14. Select one of the following: <ul style="list-style-type: none"> • traps—To enable the sending of Simple Network Management Protocol (SNMP) notifications when the state of the connection changes. • no-traps—To disable the sending of Simple Network Management Protocol (SNMP) notifications when the state of the connection changes. 15. From the Accounting Profile list, select the accounting profile.

Damping Interface Transitions (NSM Procedure)

When an interface changes from being up to being down, or from down to up, this transition is advertised immediately to the hardware and the Junos OS. In some situations you might want to damp interface transitions. This means not advertising the interface's transition until a certain period of time called the hold time has passed. When you have damped interface transitions and the interface goes from up to down, the interface is not advertised to the rest of the system as being down until it has remained down for the hold-time period. Similarly when an interface goes from down to up, it is not advertised as being up until it has remained up for the hold-time period.

To configure hold time value to use to damp interface transitions:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in [Table 103 on page 209](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 103: Hold Time Configuration Details

Task	Your Action
Configure hold-time value to use to damp interface transitions.	<ol style="list-style-type: none"> 1. Click Add Interface next to Interface. 2. In the Add Interface Dialog box, enter the interface name. 3. Click Hold Time next to interface. 4. In the Comment box, enter the comment. 5. From the Up list, select the hold time to use when an interface transitions from down to up. Range: 0 through 4,294,967,295 milliseconds Default: 0 milliseconds 6. From the Down list, select the hold time to use when an interface transitions from up to down Range: 0 through 4,294,967,295 milliseconds Default: 0 milliseconds

Configuring Receive Bucket Properties on Interfaces (NSM Procedure)

For all interface types except ATM, Fast Ethernet, Gigabit Ethernet, and channelized IQ and IQE, you can configure leaky bucket properties, which allow you to limit the amount of traffic received on a particular interface. You effectively specify what percentage of the interface's total capacity can be used to receive packets. You might want to set leaky bucket properties to limit the traffic flow from a link that is known to transmit a high volume of traffic.

To configure receive bucket properties in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in [Table 104 on page 210](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 104: Receive Bucket Configuration Details

Task	Your Action
Configure receive bucket properties.	<ol style="list-style-type: none"> 1. Click Add Interface next to Interface. 2. In the Add Interface Dialog box, enter the interface name. 3. Click Receive Bucket next to interface. 4. In the Comment box, enter the comment. 5. From the Overflow list, select how to handle packets that exceed the threshold for the receive leaky bucket. <ul style="list-style-type: none"> • Select tag to tag, count, and process received packets that exceed the threshold. • Select discard to discard received packets that exceed the threshold. 6. From the Rate list, select the percentage of the interface line rate that is available to receive or transmit packets. Range: 0 through 100 7. From the Threshold list, select the maximum size, in bytes, for traffic bursts. Range: 0 through 65,535 bytes

Configuring Tracing Operations of an Individual Router Interface (NSM Procedure)

You can define tracing operations for individual interfaces using this option. To specify more than one tracing operation, include multiple **flag** statements.

To configure tracing operations of an router interface in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in [Table 105 on page 211](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 105: Trace Options Configuration Details

Task	Your Action
Define tracing operations for individual interfaces.	<ol style="list-style-type: none"> 1. Click Add Interface next to Interface. 2. In the Add Interface Dialog box, enter the interface name. 3. Click Traceoptions next to interface. 4. In the Comment box, enter the comment. 5. Expand Traceoptions. 6. Click Flag next to Traceoptions. 7. Click Add new entry next to Flag. 8. From the Name list, select the tracing operation to perform. 9. In the Comment box, enter the comment.

Configuring Transmit Leaky Bucket Properties (NSM Procedure)

For all interface types except ATM, channelized E1, E1, Fast Ethernet, Gigabit Ethernet, and channelized IQ, you can configure leaky bucket properties, which allow you to limit the amount of traffic transmitted by a particular interface. You effectively specify what percentage of the interface's total capacity can be used to transmit packets. You might want to set leaky bucket properties to limit the traffic flow from a link that is known to transmit a high volume of traffic.

To configure transmit leaky bucket properties in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in [Table 106 on page 212](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 106: Transmit Bucket Configuration Details

Task	Your Action
Configure transmit bucket properties.	<ol style="list-style-type: none"> 1. Click Add Interface next to interface. 2. In the Add Interface Dialog box, enter the interface name. 3. Click Transmit Bucket next to interface. 4. In the Comment box, enter the comment. 5. From the Overflow list, select how to handle packets that exceed the threshold for the transmit leaky bucket. <ul style="list-style-type: none"> • Select discard to discard packets that exceed the threshold for the transmit leaky bucket. 6. From the Rate list, select the percentage of the interface line rate that is available to receive or transmit packets. Range: 0 through 100 7. From the Threshold list, select the maximum size, in bytes, for traffic bursts. Range: 0 through 65,535 bytes

Configuring Logical Interface Properties (NSM Procedure)

The following sections describes the configuration of logical interface properties:

- [Configuring Logical Unit Properties \(NSM Procedure\) on page 212](#)
- [Configuring an IP Demux Underlying Interface \(NSM Procedure\) on page 213](#)
- [Configuring the Logical Demux Source Family Type on the IP Demux Underlying Interface \(NSM Procedure\) on page 214](#)
- [Configuring Epd Threshold for the Logical Interface \(NSM Procedure\) on page 214](#)

Configuring Logical Unit Properties (NSM Procedure)

To configure logical unit properties in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in [Table 107 on page 213](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 107: Logical Unit Configuration Details

Task	Your Action
Configure logical unit properties.	<ol style="list-style-type: none"> 1. Click Add Interface next to Interface. 2. In the Add Interface Dialog box, enter the interface name. 3. Click Unit next to interface. 4. Click Add new entry next to Unit. 5. From the Name list, select the interface name. 6. In the Comment check box, enter the comment. 7. Select the Disable check box to disable a physical or a logical interface, effectively unconfiguring it. 8. Select the Reassemble Packets check box to enable reassembly of fragmented tunnel packets on generic routing encapsulation (GRE) tunnel interfaces. 9. In the Description box, enter the text to describe the interface. If the text includes spaces, enclose the entire text in quotation marks. 10. From the Encapsulation list, select the encapsulation type. 11. In the Bandwidth box, enter the peak rate. 12. Select one of the following: <ul style="list-style-type: none"> • traps—To enable the sending of Simple Network Management Protocol (SNMP) notifications when the state of the connection changes. • no-traps—To disable the sending of Simple Network Management Protocol (SNMP) notifications when the state of the connection changes. 13. From the Accounting Profile list, select the accounting profile.

Configuring an IP Demux Underlying Interface (NSM Procedure)

You can configure the logical demultiplexing (demux) destination family type on the IP demux underlying interface.

To configure an IP demux underlying interface in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in [Table 108 on page 214](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 108: IP Demux Configuration Details

Task	Your Action
Configure the logical demultiplexing (demux) destination family type.	<ol style="list-style-type: none"> 1. Click Add Interface next to Interface. 2. In the Add Interface Dialog box, enter the interface name. 3. Click Unit next to interface. 4. Click Add new entry next to Unit. 5. Click Demux Destination next to Unit. 6. Click Add new entry next to Demux Destination. 7. From the New demux-destination window, select the family type.

Configuring the Logical Demux Source Family Type on the IP Demux Underlying Interface (NSM Procedure)

You can configure the logical demultiplexing (demux) source family type on the IP demux underlying interface using this option.

To configure logical demux source family type in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in [Table 109 on page 214](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 109: IP Demux Source Configuration Details

Task	Your Action
Configure the logical demultiplexing (demux) source family type on the IP demux underlying interface.	<ol style="list-style-type: none"> 1. Click Add Interface next to Interface. 2. In the Add Interface Dialog box, enter the interface name. 3. Click Unit next to interface. 4. Click Add new entry next to Unit. 5. Click Demux Source next to Unit. 6. Click Add new entry next to Demux Source. 7. From the New demux-destination window, select the family type.

Configuring Epd Threshold for the Logical Interface (NSM Procedure)

To configure Epd threshold for the logical interface in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in [Table 110 on page 215](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 110: Epd Threshold Configuration Details

Task	Your Action
Define the EPD threshold on a virtual circuit (VC).	<ol style="list-style-type: none"> 1. Click Add Interface next to Interface. 2. In the Add Interface Dialog box, enter the interface name. 3. Click Unit next to interface. 4. Click Add new entry next to Unit. 5. Click Epd Threshold next to Unit. 6. In the Comment box, enter the comment. 7. In the Epd Threshold plp0 box, enter the early packet discard threshold value. 8. In the Plp1 box, enter the maximum number of cells. Range: For 1-port and 2-port OC12 interfaces, 1 through 425,984 cells

Configuring Protocol Family Information for the Logical Interface (NSM Procedure)

You can configure the family information for the logical interface for different protocols using the following options:

1. [Configuring Protocol Family \(Ccc\) Information for the Logical Interface \(NSM Procedure\) on page 216](#)
2. [Configuring Protocol Family \(Inet\) Information for the Logical Interface \(NSM Procedure\) on page 217](#)
3. [Configuring Protocol Family \(Inet6\) Information for the Logical Interface \(NSM Procedure\) on page 223](#)
4. [Configuring Protocol Family \(ISO\) Information for the Logical Interface \(NSM Procedure\) on page 230](#)
5. [Configuring Protocol Family \(MPLS\) Information for the Logical Interface \(NSM Procedure\) on page 231](#)
6. [Configuring Protocol Family \(TCC\) Information for the Logical Interface \(NSM Procedure\) on page 233](#)

Configuring Protocol Family (Ccc) Information for the Logical Interface (NSM Procedure)

To configure Ccc family information in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in [Table 111 on page 216](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 111: Ccc Family Configuration Details

Task	Your Action
Apply a filter to an interface.	<ol style="list-style-type: none"> 1. Click Add Interface next to Interface. 2. In the Add Interface Dialog box, enter the interface name. 3. Click Unit next to interface. 4. Click Add new entry next to Unit. 5. Click Family next to Unit. 6. Expand Family. 7. Click Ccc next to Family. 8. In the Comment box, enter the comment. 9. Click Filter next to Ccc. 10. In the Comment box, enter the comment. 11. From the Group list, select the filter group number. Range: 0 through 255
Configure input filter.	<ol style="list-style-type: none"> 1. Click Input next to Filter. 2. Select one of the following: <ul style="list-style-type: none"> • Input—To configure name of one filter to evaluate when packets are received on the interface. Enter the input filter name. • Input-list—To apply a group of filters to evaluate when packets are received on an interface. <ol style="list-style-type: none"> a. Click Add new entry next to input-list. b. In the New input-list window, enter the filter names. Up to 16 filters can be included in a filter input list.

Table 111: Ccc Family Configuration Details (*continued*)

Task	Your Action
Configure output filter.	<ol style="list-style-type: none"> 1. Click Output next to Filter. 2. Select one of the following: <ul style="list-style-type: none"> • output—To configure name of one filter to evaluate when packets are transmitted on the interface. Enter the output filter name. • output-list — To apply a group of filters to evaluate when packets are transmitted on an interface. <ol style="list-style-type: none"> a. Click Add new entry next to output-list. b. In the New output-list window, enter the filter names. Up to 16 filters can be included in a filter input list.
Apply a policer to an interface.	<ol style="list-style-type: none"> 1. Click Policer next to Filter. 2. In the Comment box, enter the comment. 3. In the Input box, enter the name of one policer to evaluate when packets are received on the interface. 4. In the Output box, enter the name of one policer to evaluate when packets are transmitted on the interface.

Configuring Protocol Family (Inet) Information for the Logical Interface (NSM Procedure)

To configure inet family information in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in [Table 112 on page 218](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 112: Inet Family Configuration Details

Task	Your Action
Configure Inet information.	<ol style="list-style-type: none"> 1. Click Add Interface next to Interface. 2. In the Add Interface Dialog box, enter the interface name. 3. Click Unit next to interface. 4. Click Add new entry next to Unit. 5. Click Family next to Unit. 6. Expand Family. 7. Click Inet next to Family. 8. In the Comment box, enter the comment. 9. From the Mac Validate list, select one of the following: <ul style="list-style-type: none"> • strict—Forwards incoming packets when both the IP source address and the MAC source address match one of the trusted address tuples. Drops packets when the MAC address does not match the tuple's MAC source address, or when IP source address of the incoming packet does not match any of the trusted IP addresses. • loose—Forwards incoming packets when both the IP source address and the MAC source address match one of the trusted address tuples. Drops packets when the IP source address matches one of the trusted tuples, but the MAC address does not match the MAC address of the tuple. Continues to forward incoming packets when the source address of the incoming packet does not match any of the trusted IP addresses. 10. From the Mtu list, select the MTU size. Range: 0 through 4,294,967,295 11. Select the No Redirects check box to disable the sending of protocol redirect messages for the entire routing platform. 12. Select the No Arp Learn check box to disable ARP mappings. 13. Select the Primary check box to configure the address to be the primary address of the protocol on the interface.
Enable IP packet counters on an interface.	<ol style="list-style-type: none"> 1. Click Accounting next to Inet. 2. In the Comment box, enter the comment. 3. Select the Destination Class Usage check box to enable packet counters on an interface that count packets that arrive from specific customers and are destined for specific prefixes on the provider core router. 4. Click Source Class Usage next to Accounting. 5. In the Comment box, enter the comment. 6. Select the Input check box to configure at least one expected ingress point. 7. Select the Output check box to configure at least one expected egress point.

Table 112: Inet Family Configuration Details (*continued*)

Task	Your Action
Configure the interface address.	<ol style="list-style-type: none"> 1. Click Address next to Inet. 2. Click Add new entry next to Address. 3. Expand address. 4. In the Name box, enter the interface name. 5. In the Comment box, enter the comment. 6. Select the Primary check box to configure this address to be the primary address of the protocol on the interface. If the logical unit has more than one address, the primary address is used by default as the source address when packets originate from the interface and the destination does not indicate the subnet. 7. Select the Preferred check box to configure this address to be the preferred address on the interface. If you configure more than one address on the same subnet, the preferred source address is chosen by default as the source address when you originate packets to destinations on the subnet.
Configure VRRP IPv4 group.	<ol style="list-style-type: none"> 1. Click Vrrp Group next to address. 2. Click Add new entry next to Vrrp Group. 3. In the Name box, enter the interface name. 4. In the Comment box, enter the comment. 5. In the Virtual Link Local Address box, enter the virtual link local address. 6. From the priority list, select the router's priority for being elected to be the master router in the VRRP group. A larger value indicates a higher priority for being elected. Range: 1 through 255 Default: 100 (for backup routers) 7. Select one of the following: <ul style="list-style-type: none"> • accept-data—To enable the interface to accept packets destined for the virtual IP address. • no-accept-data—To prevent the interface from accepting packets destined for the virtual IP address. 8. From the Authentication Type list, select the authentication type. 9. In the Authentication Key box, enter the authentication password. 10. Select Advertise-Interval next to vrrp-group. 11. Select one of the following: <ul style="list-style-type: none"> • advertise-interval—To configure the interval between Virtual Router Redundancy Protocol (VRRP) IPv4 advertisement packets. Range: 1 through 255 seconds • fast-interval—To configure the interval, in milliseconds, between Virtual Router Redundancy Protocol (VRRP) advertisement packets. Range: 100 through 999 milliseconds • inet6-advertise-interval—To configure the interval between Virtual Router Redundancy Protocol (VRRP) IPv6 advertisement packets Range: 100 to 40,950 milliseconds (ms)

Table 112: Inet Family Configuration Details (*continued*)

Task	Your Action
Configure a backup router to preempt the master router.	<ol style="list-style-type: none"> 1. Click Preempt next to vrrp-group. 2. Select preempt to allow the master router to be preempted. <ol style="list-style-type: none"> a. In the Comment box, enter the comment. b. From the Hold Time list, select the hold time before a higher-priority backup router preempts the master router. 3. Select no-preempt to prohibit the preemption of the master router. 4. Click Track next to vrrp-group. 5. In the Comment box, enter the comment. 6. From the Priority Hold Time list, select the minimum length of time that must elapse between dynamic priority changes. Range: 1 through 3600 seconds 7. Click Interface next to Track. 8. Click Add new entry next to Interface. 9. In the Name box, enter the interface name. 10. In the Comment box, enter the comment. 11. From the Priority Cost list, select the VRRP routers' priority cost for becoming the master default router. The router with the highest priority within the group becomes the master. Range: 1 through 254

Table 112: Inet Family Configuration Details (*continued*)

Task	Your Action
Specify the bandwidth threshold for VRRP.	<ol style="list-style-type: none"> 1. Click Bandwidth Threshold next to interface. 2. Click Add new entry next to Bandwidth Threshold. 3. In the Name box, enter the interface name. 4. In the Comment box, enter the comment. 5. From the Priority Cost list, select the VRRP router's priority cost for becoming the master default router. The router with the highest priority within the group becomes the master. Range: 1 through 254 6. Click Route next to Track. 7. In the Route_address box, enter the address. 8. In the Routing Instances box, enter the routing instance in which the route is to be tracked. 9. From the Priority Cost list, select the VRRP router's priority cost for becoming the master default router. The router with the highest priority within the group becomes the master. 10. Click Virtual Address next to vrrp-group. 11. Select one of the following: <ul style="list-style-type: none"> • virtual-address—To configure the addresses of the virtual routers in a Virtual Router Redundancy Protocol (VRRP) IPv4 group. You can configure up to eight addresses. <ol style="list-style-type: none"> a. Click Add new entry and in the New virtual-address window, enter the addresses of one or more virtual routers. b. In the New virtual-address window, enter the addresses of one or more virtual routers. • virtual-inet6-address—To configure the addresses of the virtual routers in a Virtual Router Redundancy Protocol (VRRP) IPv6 group. You can configure up to eight addresses. <ol style="list-style-type: none"> a. Click Add new entry b. In the New virtual-address window, enter the addresses of one or more virtual routers.
Configure input filter.	<ol style="list-style-type: none"> 1. Click Input next to Filter. 2. Select one of the following: <ul style="list-style-type: none"> • input—To configure name of one filter to evaluate when packets are received on the interface. Enter the input filter name. • input-list—To apply a group of filters to evaluate when packets are received on an interface. <ol style="list-style-type: none"> a. Click Add new entry next to input-list. b. In the New input-list window, enter the filter names. Up to 16 filters can be included in a filter input list.

Table 112: Inet Family Configuration Details (*continued*)

Task	Your Action
Configure output filter.	<ol style="list-style-type: none"> 1. Click Output next to Filter. 2. Select one of the following: <ul style="list-style-type: none"> • output—To configure name of one filter to evaluate when packets are transmitted on the interface. Enter the output filter name. • output-list —To apply a group of filters to evaluate when packets are transmitted on an interface. <ol style="list-style-type: none"> a. Click Add new entry next to output-list. b. In the New output-list window, enter the filter names. Up to 16 filters can be included in a filter input list.
Apply a policer to an interface.	<ol style="list-style-type: none"> 1. Click Policer next to Filter. 2. In the Comment box, enter the comment. 3. In the Input box, enter the name of one policer to evaluate when packets are received on the interface. 4. In the Output box, enter the name of one policer to evaluate when packets are transmitted on the interface.
Check whether traffic is arriving on an expected path.	<ol style="list-style-type: none"> 1. Click Rpf Check next to Inet. 2. In the Comment box, enter the comment. 3. In the Fail Filter box, enter the filter name to evaluate when packets are received on the interface. 4. Click Mode next to Rpf Check. 5. In the Comment box, enter the comment. 6. Select the loose check box to check whether the packet has a source address with a corresponding prefix in the routing table.
Configure the direction of traffic to be sampled.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment. 2. Select the Input check box to configure at least one expected ingress point. 3. Select the Output check box to configure at least one expected egress point.

Table 112: Inet Family Configuration Details (*continued*)

Task	Your Action
Define one or more service sets to be applied to an interface.	<ol style="list-style-type: none"> 1. Click Service next to Inet. 2. In the Comment box, enter the comment. 3. Click Input next to Service. 4. In the Comment box, enter the comment. 5. In the Post Service Filter box, enter the filter to be applied to traffic after service processing. 6. Expand Input. 7. Click Service Set next to Input. 8. Click Add new entry next to Service Set. 9. From the Name list, select the service set name. 10. In the Comment box, enter the comment. 11. In the Service Filter box, enter the filter name. 12. Click Output next to Service. 13. In the Comment box, enter the comment. 14. Expand Output. 15. Click Service Set next to Output. 16. Click Add new entry next to Service Set. 17. From the Name list, select the service set name. 18. In the Comment box, enter the comment. 19. In the Service Filter box, enter the filter name.
Configure an Ethernet or demultiplexing interface to be unnumbered.	<ol style="list-style-type: none"> 1. Click Unnumbered Address next to Inet. 2. In the Comment box, enter the comment. 3. In the Source box, enter the secondary IP address of the donor loopback interface.

Configuring Protocol Family (Inet6) Information for the Logical Interface (NSM Procedure)

To configure inet6 family information in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in [Table 113 on page 224](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 113: Inet6 Family Configuration Details

Task	Your Action
Configure Inet6 information.	<ol style="list-style-type: none"> 1. Click Add Interface next to Interface. 2. In the Add Interface Dialog box, enter the interface name. 3. Click Unit next to interface. 4. Click Add new entry next to Unit. 5. Click Family next to Unit. 6. Expand Family. 7. Click Inet next to Family. 8. In the Comment box, enter the comment. 9. From the Mac Validate list, select one of the following: <ul style="list-style-type: none"> • strict—Forwards incoming packets when both the IP source address and the MAC source address match one of the trusted address tuples. Drops packets when the MAC address does not match the tuple's MAC source address, or when IP source address of the incoming packet does not match any of the trusted IP addresses. • loose—Forwards incoming packets when both the IP source address and the MAC source address match one of the trusted address tuples. Drops packets when the IP source address matches one of the trusted tuples, but the MAC address does not match the MAC address of the tuple. Continues to forward incoming packets when the source address of the incoming packet does not match any of the trusted IP addresses. 10. From the Mtu list, select the MTU size. Range: 0 through 4,294,967,295 11. Select the No Redirects check box to disable the sending of protocol redirect messages for the entire routing platform. 12. Select the No Arp Learn check box to disable arp. 13. Select the Primary check box to configure the address to be the primary address of the protocol on the interface.
Enable IP packet counters on an interface.	<ol style="list-style-type: none"> 1. Click Accounting next to Inet. 2. In the Comment box, enter the comment. 3. Select Destination Class Usage check box to enable packet counters on an interface that count packets that arrive from specific customers and are destined for specific prefixes on the provider core router. 4. Click Source Class Usage next to Accounting. 5. In the Comment box, enter the comment. 6. Select the Input check box to configure at least one expected ingress point. 7. Select the Output check box to configure at least one expected egress point.

Table 113: Inet6 Family Configuration Details (*continued*)

Task	Your Action
Configure the interface address.	<ol style="list-style-type: none">1. Click Address next to Inet.2. Click Add new entry next to Address.3. Expand address.4. In the Name box, enter the interface name.5. In the Comment box, enter the comment.6. Select the Primary check box to configure this address to be the primary address of the protocol on the interface. If the logical unit has more than one address, the primary address is used by default as the source address when packets originate from the interface and the destination does not indicate the subnet.7. Select the Preferred check box to configure this address to be the preferred address on the interface. If you configure more than one address on the same subnet, the preferred source address is chosen by default as the source address when you originate packets to destinations on the subnet.

Table 113: Inet6 Family Configuration Details (*continued*)

Task	Your Action
Configure VRRP IPV6 Group.	<ol style="list-style-type: none"> 1. Click Vrrp Group next to address. 2. Click Add new entry next to Vrrp Group. 3. In the Name box, enter the interface name. 4. In the Comment box, enter the comment. 5. In the Virtual Link Local Address box, enter the virtual link local address. 6. From the priority list, select the router's priority for being elected to be the master router in the VRRP group. A larger value indicates a higher priority for being elected. Range: 1 through 255 Default: 100 (for backup routers) 7. Select one of the following: <ul style="list-style-type: none"> • accept-data—To enable the interface to accept packets destined for the virtual IP address. • no-accept-data—To prevent the interface from accepting packets destined for the virtual IP address. 8. From the Authentication Type list, select the authentication type. 9. In the Authentication Key box, enter the authentication password. 10. Select Advertise-Interval next to vrrp-group. 11. Select one of the following: <ul style="list-style-type: none"> • advertise-interval—To configure the interval between Virtual Router Redundancy Protocol (VRRP) IPv4 advertisement packets. Range: 1 through 255 seconds • fast-interval—To configure the interval, in milliseconds, between Virtual Router Redundancy Protocol (VRRP) advertisement packets. Range: 100 through 999 milliseconds • inet6-advertise-interval—To configure the interval between Virtual Router Redundancy Protocol (VRRP) IPv6 advertisement packets Range: 100 to 40,950 milliseconds (ms)

Table 113: Inet6 Family Configuration Details (*continued*)

Task	Your Action
Configure a backup router to preempt the master router.	<ol style="list-style-type: none"> Click Preempt next to vrrp-group. Select one of the following: <ul style="list-style-type: none"> preempt—To allow the master router to be preempted. <ol style="list-style-type: none"> In the Comment box, enter the comment. From the Hold Time list, select the hold time before a higher-priority backup router preempts the master router. Range: 0 through 3600 no-preempt—To prohibit the preemption of the master router. Click Track next to vrrp-group. In the Comment box, enter the comment. From the Priority Hold Time list, select the minimum length of time that must elapse between dynamic priority changes. Range: 1 through 3600 seconds Click Interface next to Track. Click Add new entry next to Interface. In the Name box, enter the interface name. In the Comment box, enter the comment. From the Priority Cost list, select the VRRP router's priority cost for becoming the master default router. The router with the highest priority within the group becomes the master. Range: 1 through 254

Table 113: Inet6 Family Configuration Details (*continued*)

Task	Your Action
Specify the bandwidth threshold for VRRP.	<ol style="list-style-type: none"> 1. Click Bandwidth Threshold next to interface. 2. Click Add new entry next to Bandwidth Threshold. 3. In the Name box, enter the interface name. 4. In the Comment box, enter the comment. 5. From the Priority Cost list, select the VRRP router's priority cost for becoming the master default router. The router with the highest priority within the group becomes the master. Range: 1 through 254 6. Click Route next to Track. 7. In the Route_address box, enter the address. 8. In the Routing Instances box, enter the routing instance in which the route is to be tracked. 9. From the Priority Cost list, select the VRRP router's priority cost for becoming the master default router. The router with the highest priority within the group becomes the master. 10. Click Virtual Address next to vrrp-group. 11. Select one of the following: <ul style="list-style-type: none"> • virtual-address—To configure the addresses of the virtual routers in a Virtual Router Redundancy Protocol (VRRP) IPv4 group. You can configure up to eight addresses. <ol style="list-style-type: none"> a. Click Add new entry and in the New virtual-address window, enter the addresses of one or more virtual routers. • virtual-inet6-address—To configure the addresses of the virtual routers in a Virtual Router Redundancy Protocol (VRRP) IPv6 group. You can configure up to eight addresses. <ol style="list-style-type: none"> a. Click Add new entry and in the New virtual-inet6-address window, enter the addresses of one or more virtual routers.
Configure input filter.	<ol style="list-style-type: none"> 1. Click Input next to Filter. 2. Select one of the following: <ul style="list-style-type: none"> • Select input to configure name of one filter to evaluate when packets are received on the interface. Enter the input filter name. • Select input-list to apply a group of filters to evaluate when packets are received on an interface. <ol style="list-style-type: none"> a. Click Add new entry next to input-list. b. In the New input-list window, enter the filter names. Up to 16 filters can be included in a filter input list.

Table 113: Inet6 Family Configuration Details (*continued*)

Task	Your Action
Configure output filter.	<ol style="list-style-type: none"> Click Output next to Filter. Select one of the following: <ul style="list-style-type: none"> Select output to configure name of one filter to evaluate when packets are transmitted on the interface. Enter the output filter name. <ol style="list-style-type: none"> Enter the output filter name. Select output-list to apply a group of filters to evaluate when packets are transmitted on an interface. <ol style="list-style-type: none"> Click Add new entry next to output-list. In the New output-list window, enter the filter names. Up to 16 filters can be included in a filter input list.
Apply a policer to an interface.	<ol style="list-style-type: none"> Click Policer next to Filter. In the Comment box, enter the comment. In the Input box, enter the name of one policer to evaluate when packets are received on the interface. In the Output box, enter the name of one policer to evaluate when packets are transmitted on the interface.
Check whether traffic is arriving on an expected path.	<ol style="list-style-type: none"> Click Rpf Check next to Inet. In the Comment box, enter the comment. In the Fail Filter box, enter the filter name to evaluate when packets are received on the interface. Click Mode next to Rpf Check. In the Comment box, enter the comment. Select the loose check box to check whether the packet has a source address with a corresponding prefix in the routing table.
Configure the direction of traffic to be sampled.	<ol style="list-style-type: none"> In the Comment box, enter the comment. Select the Input check box to configure at least one expected ingress point. Select the Output check box to configure at least one expected egress point.

Table 113: Inet6 Family Configuration Details (*continued*)

Task	Your Action
Define one or more service sets to be applied to an interface.	<ol style="list-style-type: none"> 1. Click Service next to Inet. 2. In the Comment box, enter the comment. 3. Click Input next to Service. 4. In the Comment box, enter the comment. 5. In the Post Service Filter box, enter the filter to be applied to traffic after service processing. 6. Expand Input. 7. Click Service Set next to Input. 8. Click Add new entry next to Service Set. 9. From the Name list, select the service set name. 10. In the Comment box, enter the comment. 11. In the Service Filter box, enter the filter name. 12. Click Output next to Service. 13. In the Comment box, enter the comment. 14. Expand Output. 15. Click Service Set next to Output. 16. Click Add new entry next to Service Set. 17. From the Name list, select the service set name. 18. In the Comment box, enter the comment. 19. In the Service Filter box, enter the filter name.

Configuring Protocol Family (ISO) Information for the Logical Interface (NSM Procedure)

To configure iso family information in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in [Table 114 on page 231](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 114: Iso Family Configuration Details

Task	Your Action
Configure Iso information.	<ol style="list-style-type: none"> 1. Click Add Interface next to Interface. 2. In the Add Interface Dialog box, enter the interface name. 3. Click Unit next to interface. 4. Click Add new entry next to Unit. 5. Click Family next to Unit. 6. Expand Family. 7. Click Iso next to Family. 8. In the Comment box, enter the comment. 9. From the Mtu list, select the MTU size. Range: 0 through 4,294,967,295
Configure the interface address.	<ol style="list-style-type: none"> 1. Click Address next to Inet. 2. Click Add new entry next to Address. 3. Expand address. 4. In the Name box, enter the interface name. 5. In the Comment box, enter the comment.

Configuring Protocol Family (MPLS) Information for the Logical Interface (NSM Procedure)

To configure mpls family information in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in [Table 115 on page 232](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 115: MPLS Family Configuration Details

Task	Your Action
Configure MPLS information.	<ol style="list-style-type: none"> 1. Click Add Interface next to Interface. 2. In the Add Interface Dialog box, enter the interface name. 3. Click Unit next to interface. 4. Click Add new entry next to Unit. 5. Click Family next to Unit. 6. Expand Family. 7. Click MPLS next to Family. 8. In the Comment box, enter the comment. 9. From the Mtu list, select the MTU size. Range: 0 through 4,294,967,295
Configure input filter.	<ol style="list-style-type: none"> 1. Click Input next to Filter. 2. Select one of the following: <ul style="list-style-type: none"> • input—To configure name of one filter to evaluate when packets are received on the interface. Enter the input filter name. • input-list—To apply a group of filters to evaluate when packets are received on an interface. <ol style="list-style-type: none"> a. Click Add new entry next to input-list. b. In the New input-list window, enter the filter names. Up to 16 filters can be included in a filter input list.
Configure output filter.	<ol style="list-style-type: none"> 1. Click Output next to Filter. 2. Select one of the following: <ul style="list-style-type: none"> • output—To configure name of one filter to evaluate when packets are transmitted on the interface. Enter the output filter name. • output-list—To apply a group of filters to evaluate when packets are transmitted on an interface. <ol style="list-style-type: none"> a. Click Add new entry next to output-list. b. In the New output-list window, enter the filter names. Up to 16 filters can be included in a filter input list.
Apply a policer to an interface.	<ol style="list-style-type: none"> 1. Click Policer next to Filter. 2. In the Comment box, enter the comment. 3. In the Input box, enter the name of one policer to evaluate when packets are received on the interface. 4. In the Output box, enter the name of one policer to evaluate when packets are transmitted on the interface.

Configuring Protocol Family (TCC) Information for the Logical Interface (NSM Procedure)

To configure tcc family information in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in [Table 116 on page 233](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 116: TCC Family Configuration Details

Task	Your Action
Configure tcc information.	<ol style="list-style-type: none"> 1. Click Add Interface next to Interface. 2. In the Add Interface Dialog box, enter the interface name. 3. Click Unit next to interface. 4. Click Add new entry next to Unit. 5. Click Family next to Unit. 6. Expand Family. 7. Click Tcc next to Family. 8. In the Comment box, enter the comment.
Apply a policer to an interface.	<ol style="list-style-type: none"> 1. Click Policer next to Tcc. 2. In the Comment box, enter the comment. 3. In the Input box, enter the name of one policer to evaluate when packets are received on the interface. 4. In the Output box, enter the name of one policer to evaluate when packets are transmitted on the interface.
Configure Ethernet TCC encapsulation.	<ol style="list-style-type: none"> 1. Click proxy next to TCC. 2. In the Comment box, enter the comment. 3. Click Remote next to TCC. 4. In the Comment box, enter the comment.

Configuring the Traffic Shaping Profile (NSM Procedure)

When you use an ATM encapsulation on ATM1 and ATM2 IQ interfaces, you can define bandwidth utilization, which consists of either a constant rate or a peak cell rate, with sustained cell rate and burst tolerance.

To configure traffic shaping profile in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in [Table 117 on page 234](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 117: Traffic Shaping Configuration Details

Task	Your Action
Define the traffic-shaping profile.	<ol style="list-style-type: none"> 1. Click Add Interface next to Interface. 2. In the Add Interface Dialog box, enter the interface name. 3. Click Unit next to interface. 4. Click Add new entry next to Unit. 5. Click Shaping next to Unit. 6. Expand Shaping. 7. In the Comment box, enter the comment. 8. From the Queue Length list, select the maximum number of packets the queue can contain. Range: 1 through 16383 packets Default: 16383 packets 9. Click Cbr next to Shaping. 10. Select one of the following: <ul style="list-style-type: none"> • cbr—To define a constant bit rate bandwidth utilization in the traffic-shaping profile for ATM encapsulation. <ol style="list-style-type: none"> a. In the Comment box, enter the comment b. In the Cbr Value box, enter the unspecified bit rate (UBR). • vbr—To define the variable bandwidth utilization in the traffic-shaping profile for ATM encapsulation. <ol style="list-style-type: none"> a. In the Comment box, enter the comment. b. In the Peak box, enter the peak rate c. In the Sustained box, enter the sustained rate. d. In the Burst box, enter the burst length. • rtvbr—To define the real-time variable bandwidth utilization in the traffic-shaping profile for ATM2 IQ PICs. <ol style="list-style-type: none"> a. In the Comment box, enter the comment. b. In the Peak box, enter the peak rate. c. In the Sustained box, enter the sustained rate. d. In the Burst box, enter the burst length.

Configuring Interface set on the Routing Platform (NSM Procedure)

You can configure an interface set on the routing platform using this option.

To configure interface set in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface Set**.
5. Add or modify settings as specified in [Table 118 on page 235](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 118: Interface Set Configuration Details

Task	Your Action
Define the interface set.	<ol style="list-style-type: none"> 1. Click Add new entry next to Interface Set. 2. Click interface-set. 3. In the Name box, enter the name for the interface set. 4. In the Comment box, enter the comment.
Apply the interface set to interfaces.	<ol style="list-style-type: none"> 1. Click interface next to interface-set. 2. Click Add new entry next to Interface. 3. In the Name box, enter the interface name. 4. In the Comment box, enter the comment. 5. Click Unit next to interface. 6. Click Add new entry next to Unit. 7. From the Name list, select the number of the logical unit. Range: 0 through 16,385 8. In the Comment box, enter the comment. 9. Click Vlan Tags Outer next to Interface. 10. Click Add new entry next to Vlan tags Outer. 11. From the Name list, select the outer VLAN ID. 12. In the Comment box, enter the comment.

Related Documentation

- [Configuring Interfaces on the Routing Platform \(NSM Procedure\) on page 207](#)
- [Configuring Trace Options on the Routing Platform \(NSM Procedure\) on page 236](#)

Configuring Trace Options on the Routing Platform (NSM Procedure)

You can configure the trace options using this option.

To configure trace options in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Traceoptions**.
5. Add or modify settings as specified in [Table 119 on page 236](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 119: Traceoption Configuration Details

Task	Your Action
Define tracing operations for the interface process.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment for the traceoptions. 2. Select No Remote Trace check box to disable remote tracing. 3. Click File next to Traceoptions. 4. In the Comment box, enter the comment for the filename. 5. In the Filename box, enter the name of the file to receive the output of the tracing operation. 6. In the Size box, enter the maximum trace file size. 7. From the Files list, select the maximum number of trace files. 8. Select one of the following: <ul style="list-style-type: none"> • no-world-readable—To restrict the file access to owner. • world-readable—To enable unrestricted access. 9. In the Match box, enter the regular expression. 10. Click Flag next to Traceoptions.
Define flag.	<ol style="list-style-type: none"> 1. Click Add new entry next to Flag. 2. From the Name list, select the flag to perform the trace operation. <ul style="list-style-type: none"> • Select kernel to log configuration IPC messages to kernel. • Select change-events to log changes that produce configuration events. • Select kernel-detail to log details of configuration messages to kernel. • Select config-states to log the configuration state machine changes. 3. Enter the comment for the flag. 4. Select the Disable check box to disable the tracing operation.

- Related Documentation**
- [Configuring Interfaces on the Routing Platform \(NSM Procedure\) on page 207](#)
 - [Configuring Interface set on the Routing Platform \(NSM Procedure\) on page 235](#)

Configuration of Multicast Snooping Options

- [Configuring Multicast Monitoring Options \(NSM Procedure\) on page 239](#)

Configuring Multicast Monitoring Options (NSM Procedure)

Multicast is a way for a Layer 2 device to monitor at the Layer 3 packet content to determine which actions are to be taken to process or forward a frame. There are specific forms of , such as IGMP or PIM . In all cases, monitoring involves a device configured to function at Layer 2 having access to Layer 3 (packet) information. Monitoring makes multicasting more efficient in these devices.

To configure multicast monitoring in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double click the device to select it.
3. In the **Configuration** tab, expand **Multicast Monitoring Options**.
4. Add or modify the settings as specified in [Table 120 on page 240](#).
5. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.

Table 120: Multicast Monitoring Options Configuration Details

Task	Your Action
Establish a list of flood group addresses for multicast monitoring.	<ol style="list-style-type: none"> 1. Click Flood Groups next to Multicast Monitoring Options. 2. Click Add new entry next to Flood Groups. 3. In the dialog box, enter the IP addresses.
Configure multicast forwarding cache properties.	<ol style="list-style-type: none"> 1. Click Forwarding Cache next to Multicast Monitoring Options. 2. In the Comment box, enter the comments. 3. Expand Forwarding Cache. 4. Click Threshold next to Forwarding Cache. 5. In the Comment box, enter the comments. 6. From the Suppress list, select the threshold value for a forwarding cache. Range: 1 through 200,000 7. From the Reuse list, select the reuse value for the threshold. The reuse value must be less than the suppression threshold value. Range: 1 through 200,000
Establish the graceful restart duration for multicast monitoring.	<ol style="list-style-type: none"> 1. Click Graceful Restart next to Multicast Monitoring Options. 2. In the Comment box, enter the comments. 3. From the Restart Duration list, select the duration for graceful restart. Range: 0 to 300 seconds Default : 180 seconds
Establish multicast monitoring option values.	<ol style="list-style-type: none"> 1. Click Option next to Multicast Monitoring Options. 2. In the Comment box, enter the comments. 3. Expand Options. 4. Click Syslog next to Options. 5. In the Comment box, enter the comments. 6. From the Upto list, select the level up to which severity the messages to be system logged. 7. From the Mark list, select the time interval in seconds to mark the trace file. Range : -2147483647 seconds to 2147483647 Seconds Default : 0 8. Expand Syslog. 9. Click Level next to Syslog. 10. Select the Level of severity to be logged.

Table 120: Multicast Monitoring Options Configuration Details (*continued*)

Task	Your Action
Configure tracing options.	<ol style="list-style-type: none"> 1. Click Traceoptions next to Multicast Monitoring Options. 2. In the Comment box, enter the comments. 3. Expand Traceoptions. 4. Click File next to Trace Options. 5. In the Comment box, enter the comments. 6. In the Filename box, enter the name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. 7. In the Size box, enter the maximum size of each trace file in bytes. Range : 10240 to 4,294,967,295 bytes 8. From the Files list, select the maximum number of files. 9. Select the world-readable option to enable log file access to all users. 10. Select the no-world-readable option to prevent all users from reading the log file. 11. Click Flag next to Trace Options. 12. Click Add new entry next to flag. 13. From the Name list, select a tracing operation to perform. 14. In the Comment box, enter the comments.

**Related
Documentation**

- [Configuring Interfaces on the Routing Platform \(NSM Procedure\) on page 207](#)

Configuration of Policy Options

- [Configuring an AS Path in a BGP Routing Policy \(NSM Procedure\) on page 243](#)
- [Configuring an AS Path Group in a BGP Routing Policy \(NSM Procedure\) on page 244](#)
- [Configuring a Community for use in BGP Routing Policy Conditions \(NSM Procedure\) on page 245](#)
- [Configuring a BGP Export Policy Condition \(NSM Procedure\) on page 246](#)
- [Configuring Flap Damping to Reduce the Number of BGP Update Messages \(NSM Procedure\) on page 247](#)
- [Configuring a Routing Policy Statement \(NSM Procedure\) on page 249](#)
- [Configuring Prefix List \(NSM Procedure\) on page 250](#)

Configuring an AS Path in a BGP Routing Policy (NSM Procedure)

An autonomous system (AS) path is a path to a destination. An AS path consists of the AS numbers of all the network devices that a packet traverses if it takes the associated route to a destination. The AS numbers are assembled in a sequence, or path, that is read from right to left. For example, for a packet to reach a destination using a route with an AS path 5 4 3 2 1, the packet first traverses AS 1 and so on until it reaches AS 5, which is the last AS before its destination.

You can define a match condition based on all of or portions of the AS path. You can create a named AS path and then include it in a BGP routing policy.

To configure an AS path for a BGP routing policy in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Policy Options**.
5. Select **As Path**.
6. Add or modify the parameters as specified in [Table 121 on page 244](#).
7. Click one:
 - **OK**—To save the changes.

- **Cancel**—To cancel the modifications.
- **Apply** — To apply the protocol settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 121: AS Path Configuration Details

Option	Function	Your Action
Name	Specifies the name of the AS path.	Enter a name.
Comment	Specifies the comment for the AS path.	Enters a comment.
Path	Specifies the AS path (as an AS number) to be included in the routing policy.	Enter an AS path.

Configuring an AS Path Group in a BGP Routing Policy (NSM Procedure)

Autonomous System (AS) path group consists of multiple AS paths. You can define match conditions based on the AS path groups. You can create named AS paths under an AS path group and then include the AS path group in a routing policy.

To configure an AS path group for a BGP routing policy in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Policy Options**.
5. Select **As Path Group**.
6. Add or modify the parameters as specified in [Table 122 on page 245](#).
7. Click one:
 - **OK**—To save the changes.
 - **Cancel**—To cancel the modifications.
 - **Apply** — To apply the protocol settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 122: AS Path Group Configuration Details

Option	Function	Your Action
Name	Specifies the name of the AS path group.	Enter a name.
Comment	Specifies the comment for the AS path group.	Enter a comment.
As Path	Specifies an AS path to be included in the AS path group. Specifies the name and comment for the AS path and specifies the path as an AS path number.	<ol style="list-style-type: none">1. Select As Path.2. Click the New button or select an AS path and click the Edit button.3. Specify the name, comment and path.4. Click OK, then click OK again.

Configuring a Community for use in BGP Routing Policy Conditions (NSM Procedure)

A community is a group of destinations that share a common property. You can define a community for use in a BGP routing policy match condition.

To configure a community for a BGP routing policy in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Policy Options**.
5. Select **Community**.
6. Add or modify the parameters as specified in [Table 123 on page 246](#).
7. Click one:
 - **OK**—To save the changes.
 - **Cancel**—To cancel the modifications.
 - **Apply** — To apply the protocol settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 123: Community Configuration Details

Option	Function	Your Action
Name	Specifies the name of the community.	Enter the name.
Comment	Specifies the comment for the community.	Enter the comment.
Invert Match	Enables you to invert the results for the community expression.	Select the check-box if you want to invert the results. Clear the check-box if you do not want to invert the results.
Members	Specifies one or more community members.	<ol style="list-style-type: none"> 1. Select Members. 2. Click the New button or select a member and click the Edit button. 3. Enter the member community. 4. Click OK, then click OK again.

Configuring a BGP Export Policy Condition (NSM Procedure)

You can define a routing policy condition based on the existence of routes in specific tables for use in a BGP export policy.

To configure condition in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Policy Options**.
5. Select **Condition**.
6. Add or modify the parameters as specified in [Table 124 on page 247](#).
7. Click one:
 - **OK**—To save the changes.
 - **Cancel**—To cancel the modifications.
 - **Apply** — To apply the protocol settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 124: Condition Configuration Details

Option	Function	Your Action
Name	Specifies the name of the condition.	Enter a name.
Comment	Specifies the comment for the condition.	Enter a comment.
Route Active On	Enables you to specify the policy condition based on the existing routes and the corresponding route tables.	<ol style="list-style-type: none"> 1. Select Route Active On. 2. Select one: <ul style="list-style-type: none"> • None—No policy condition based on routes need to be specified. • if-route-exists—Specify the policy condition based on the routes. Enter the comment, route and the corresponding routing table. 3. Click OK.

Configuring Flap Damping to Reduce the Number of BGP Update Messages(NSM Procedure)

To advertise network reachability information, BGP systems send an excessive number of update messages. You can use flap damping to reduce the number of update messages sent between BGP peers, thereby reducing the load on these peers without adversely affecting the route convergence time. Damping reduces the number of update messages by marking these routes as ineligible, so that they cannot be selected as active or preferable routes. Applying damping leads to some delay, or suppression, in the propagation of route information, but the result is increased network stability. You can define actions by creating a named set of damping parameters and including the set in a routing policy.

To configure damping for a BGP routing policy in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Policy Options**.
5. Select **Damping**.

6. Add or modify the parameters as specified in [Table 125 on page 248](#).
7. Click one:
 - **OK**—To save the changes.
 - **Cancel**—To cancel the modifications.
 - **Apply**—To apply the protocol settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 125: Damping Configuration Details

Option	Function	Your Action
Name	Specifies the name of the damping parameter setting.	Enter a name.
Comment	Specifies the comment for the damping parameter setting.	Enter a comment.
Disable	Enables you to disable damping on a per-prefix basis. Any damping state that is present in the routing table for a prefix is deleted if damping is disabled.	Select the check-box to disable damping. Clear the check-box to enable damping.
Half Life	Indicates the time in minutes interval after which the accumulated figure-of-merit value is reduced by half if the route remains stable. Figure-of-merit values correlate to the probability of future instability of a device. Routes with higher figure-of-merit values are suppressed for longer periods of time.	Enter the time limit in minutes or select it from the list.
Reuse	Indicates the figure-of-merit value below which a suppressed route can be used again.	Enter the value or select it from the list.
Suppress	Indicates the figure-of-merit value above which a route is suppressed for use or inclusion in advertisements.	Enter the value or select it from the list.
Max Suppress	Indicates the maximum time in minutes that a route can be suppressed no matter how unstable it has been.	<ol style="list-style-type: none"> 1. Enter the time limit or select it from the list. 2. Click OK.

Configuring a Routing Policy Statement (NSM Procedure)

You can configure policy statements for routing policies. Each policy statement is composed of from criteria, to criteria and then criteria. The from and to criteria comprise a set of match conditions for the routing policy. The then criteria specify the action to be taken when the from and to criteria are matched and when they are not matched.

To configure a routing policy statement in NSM :

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Policy Options**.
5. Select **Policy statement**.
6. Add/Modify the parameters as specified in [Table 126 on page 249](#).
7. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply — To apply the protocol settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 126: Configuring Policy Statement Fields

Option	Function	Your Action
Name	Specifies the name of the policy statement.	<ol style="list-style-type: none">1. Click the New button or select a policy statement and click Edit button.2. Select policy-statement .3. Specify the name.
Comment	Specifies the comment for the policy statement.	<ol style="list-style-type: none">1. Click the New button or select a policy statement and click Edit button.2. Select policy-statement .3. Specify the comment.

Table 126: Configuring Policy Statement Fields (*continued*)

Option	Function	Your Action
From	Enables you to define the criteria that an incoming route must match. You can specify one or more match conditions. If you specify more than one, all conditions must match the route for a match to occur.	<ol style="list-style-type: none"> 1. Click the New button or select a policy statement and click Edit button. 2. Expand policy-statement tree and select From. 3. Enter the From criteria. 4. Expand From tree and specify the match conditions.
Term	Indicates the term to be configured for the routing policy. You can create one or more terms for a routing policy. Each term comprises of match conditions and the corresponding actions.	<ol style="list-style-type: none"> 1. Click the New button or select a policy statement and click Edit button. 2. Expand policy-statement tree and select Term. 3. Click the New button or select a term and click Edit button. 4. Enter the term name, comment and the match conditions and actions.
Then	Enables you to define the action to be taken in the case of a match or mismatch between the packets and From and To conditions.	<ol style="list-style-type: none"> 1. Click the New button or select a policy statement and click Edit button. 2. Expand policy-statement tree and select Then. 3. Specify the parameters for Then criteria. 4. Expand Then tree and specify the actions for each match condition.
To	Enables you to define the criteria that an outgoing route must match. You can specify one or more match conditions. If you specify more than one, all conditions must match the route for a match to occur.	<ol style="list-style-type: none"> 1. Click the New button or select a policy statement and click Edit button. 2. Expand policy-statement tree and select To. 3. Enter the To criteria. 4. Expand To tree and specify the match conditions.

Configuring Prefix List (NSM Procedure)

A prefix list is a named list of IP addresses. You can specify an exact match with incoming routes and apply a common action to all matching prefixes in the list. This feature enables you to create a named prefix list and include it in a routing policy.

To configure prefix list in NSM:

1. In the navigation tree select **Device Manager > Devices** and select the device from the list.
2. In the configuration tree, expand **Policy Options**.
3. Select **Prefix List**.
4. Add/Modify the parameters as specified in [Table 127 on page 251](#).
5. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply — To apply the protocol settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 127: Configuring Prefix List Fields

Field	Function	Your Action
Name	Specifies the name of the prefix list.	<ol style="list-style-type: none"> 1. Click the New button or select a prefix list and click Edit button. 2. Select prefix-list. 3. Specify the name.
Comment	Specifies the comment for the prefix list.	<ol style="list-style-type: none"> 1. Click the New button or select a prefix list and click Edit button. 2. Select prefix-list. 3. Specify the comment.
Apply Path	Indicates that the prefix list should include all IP prefixes pointed to by a defined path.	<ol style="list-style-type: none"> 1. Click the New button or select a prefix list and click Edit button. 2. Select prefix-list. 3. Specify the path.
Prefix List Item	Specifies the prefix list item.	<ol style="list-style-type: none"> 1. Click the New button or select a prefix list and click Edit button. 2. Expand prefix-list tree and select Prefix List Item. 3. Specify the name and comment.

Configuration of Protocols

- [Configuring the BFD Protocol \(NSM Procedure\) on page 253](#)
- [Configuring BGP \(NSM Procedure\) on page 254](#)
- [Configuring the ILMI Protocol \(NSM Procedure\) on page 257](#)
- [Configuring Layer 2 Address Learning and Forwarding Properties \(NSM Procedure\) on page 258](#)
- [Configuring Layer 2 Circuit \(NSM Procedure\) on page 259](#)
- [Configuring Layer 2 Protocol Tunneling and BPDU Protection \(NSM Procedure\) on page 265](#)
- [Configuring Label Distribution Protocol \(NSM Procedure\) on page 267](#)
- [Configuring Link Management Protocol \(NSM Procedure\) on page 278](#)
- [Configuring MPLS Protocol \(NSM Procedure\) on page 282](#)
- [Configuring MSDP Protocol \(NSM Procedure\) on page 324](#)
- [Configuring MSTP \(NSM Procedure\) on page 332](#)
- [Configuring OSPF \(NSM Procedure\) on page 334](#)
- [Configuring RIP \(NSM Procedure\) on page 338](#)
- [Configuring RIPv6 Protocol \(NSM Procedure\) on page 340](#)
- [Configuring Router Advertisement \(NSM Procedure\) on page 350](#)
- [Configuring ICMP Router Discovery \(NSM Procedure\) on page 352](#)
- [Configuring VRRP \(NSM Procedure\) on page 355](#)
- [Configuring VSTP \(NSM Procedure\) on page 356](#)
- [Configuring RSVP \(NSM Procedure\) on page 358](#)

Configuring the BFD Protocol (NSM Procedure)

The Bidirectional Forwarding Detection (BFD) protocol is used to detect the failures in a network. The BFD protocol is independent of the underlying transport mechanisms and layers; hence the failure detection timers for BFD have shorter time limits than the failure detection mechanisms of other protocols like OSPF and IS-IS. Each session of the BFD operates in two modes, asynchronous mode and demand mode. In asynchronous mode, both endpoints periodically send Hello packets to each other. If a number of those packets are not received, the session is considered down. In demand mode, no Hello packets are

exchanged after the session is established; it is assumed that the endpoints have another way to verify connectivity to each other.

To configure BFD:

1. In the navigation tree select **Device Manager > Devices** and select the device from the list.
2. In the configuration tree, expand **Protocols**.
3. Select **Bfd**.
4. Add/Modify the parameters under the respective tabs as specified in [Table 128 on page 254](#).
5. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply — To apply the protocol settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 128: Configuring Bfd Fields

Field	Function	Your Action
Comment	Specifies the comment for Bfd.	Enter the comment.
Traceoptions	Enables you to define tracing operations that track all routing protocol functionality in the device. You can configure the tracing flag, filter, and the tracing policy.	<ol style="list-style-type: none"> 1. Expand the Bfd tree and select Traceoptions. 2. Expand the Traceoptions tree and set up the file and flag parameters.

Configuring BGP (NSM Procedure)

Border Gateway Protocol (BGP) is used for exchanging routing information between gateway hosts/internet service providers. The routing information refers to the routing tables containing information about the list of known devices, the addresses they can reach, and a cost metric associated with the path to each device so that the best available route is chosen. The primary function of a BGP speaking system is to exchange network reachability information with other BGP systems. This feature enables you to configure BGP peering sessions.

To configure BGP in NSM:

1. In the navigation tree select **Device Manager > Devices** and select the device from the list.
2. In the configuration tree, expand **Protocols**.
3. Select **BGP**.
4. Add/Modify the parameters under the respective tabs as specified in [Table 129 on page 255](#).
5. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply — To apply the protocol settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See [Updating Devices](#) for more information.

Table 129: BGP Configuration Fields

Field	Function	Your Action
General	The general parameters to be set up for applying BGP.	<ol style="list-style-type: none"> 1. Expand the Protocol tree. 2. Select BGP and select General tab. 3. Specify the general parameters like comment, description, local address, hold time, etc.
Path Selection	Enables you to specify the path selection criteria.	<ol style="list-style-type: none"> 1. Expand the Protocol tree. 2. Select BGP and select Path Selection tab. 3. Set up the path selection parameters and med plus IGP.
Traceoptions	Defines trace options for IGMP monitoring.	<ol style="list-style-type: none"> 1. Expand the Protocol tree. 2. Select BGP and select Traceoptions tab. 3. Set up the file and flag parameters.
Metric Out	Enables you to specify the metric value to add to the routes transmitted to the neighbor.	<ol style="list-style-type: none"> 1. Expand the Protocol tree. 2. Select BGP and select Metric Out tab. 3. Set up the metric value and minimum IGP.

Table 129: BGP Configuration Fields (*continued*)

Field	Function	Your Action
Multihop	If an EBGP peer is more than one hop away from the local router, you must specify the next hop to the peer so that the two systems can establish a BGP session. This type of session is called a multihop BGP session.	<ol style="list-style-type: none"> 1. Expand the Protocol tree. 2. Select BGP and select Multihop tab. 3. Set up the comment, Ttl and specify whether the next hop has to be changed.
Advertise	Enables you to specify whether BGP should advertise the best route even if the routing table did not select it to be an active route.	<ol style="list-style-type: none"> 1. Expand the Protocol tree. 2. Select BGP and select Advertise tab. 3. Specify whether Advertise has to be inactivated and set up the Advertise Peer As.
Import	Enables you to apply one or more routing policies to routes being imported into the Junos OS routing table from BGP .	<ol style="list-style-type: none"> 1. Expand the Protocol tree. 2. Select BGP and select Import tab. 3. Specify the export policies configured on the peer.
Family	Enables you to configure protocol family information for the logical interface.	<ol style="list-style-type: none"> 1. Expand the Protocol tree. 2. Select BGP and select Family tab. 3. Specify the Family and Inet parameters. 4. Expand the Inet tree and set up the parameters.
Authentication Settings	Enables you to specify the authentication settings for BGP.	<ol style="list-style-type: none"> 1. Expand the Protocol tree. 2. Select BGP and select Authentication Settings tab. 3. Specify the authentication key, algorithm and key chain.
Export	Enables you to apply one or more routing policies to routes being exported from the Junos OS routing table from BGP .	<ol style="list-style-type: none"> 1. Expand the Protocol tree. 2. Select BGP and select Export tab. 3. Specify the export policies configured on the peer.
Local As	Enables you to configure BGP with a different local autonomous session (AS) number for each BGP session	<ol style="list-style-type: none"> 1. Expand the Protocol tree. 2. Select BGP and select Local As tab. 3. Enter the comment, as number, loop and specify whether it is private.

Table 129: BGP Configuration Fields (*continued*)

Field	Function	Your Action
Graceful Restart	Enables you to specify the graceful restart parameters.	<ol style="list-style-type: none"> 1. Expand the Protocol tree. 2. Select BGP and select Graceful Restart tab. 3. Specify the graceful restart parameters.
Bfd Liveness Detection	Enables you to configure bidirectional forwarding detection (BFD) timers.	<ol style="list-style-type: none"> 1. Expand the Protocol tree. 2. Select BGP and select Bfd Liveness Detection tab. 3. Specify the Bfd Liveness Detection parameters, Detection Time and Transmit Interval.
Group	Enables you to configure BGP group.	<ol style="list-style-type: none"> 1. Expand the Protocol tree. 2. Select BGP and select Group tab. 3. Click the New button or select a group and click Edit button. 4. Enter all the group parameters.

Configuring the ILMI Protocol (NSM Procedure)

To configure the ILMI protocol in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > ilmi**.
4. Select **Traceoptions**.
5. Add or modify settings as specified in [Table 130 on page 257](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 130: Trace Options Configuration Details

Task	Your Action
Define tracing options.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment for the traceoptions. 2. Select the No Remote Trace check box to disable remote tracing globally or for a specific tracing operation.

Table 130: Trace Options Configuration Details (*continued*)

Task	Your Action
Specify the name of the file to receive the output of the tracing operation and the maximum number of trace files.	<ol style="list-style-type: none"> 1. Click File next to Traceoptions. 2. In the Comment box, enter the comment for the file. 3. In the Filename box, enter the name of the file to receive the output of the tracing operation. 4. In the Size box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). Range: 10240 through 1073741824 5. From the Files list, select the maximum number of trace files. Range: 2 through 1000. 6. Select one of the following: <ul style="list-style-type: none"> • world-readable—To enable unrestricted file access. • no-world-readable—To restrict file access to owner. This is the default setting.
Specify the tracing operation to perform.	<ol style="list-style-type: none"> 1. Click Add new entry next to Flag. 2. From the Name list, select the flag. <ul style="list-style-type: none"> • database—Trace database events. • routing-socket—Trace Routing socket events. • state—Trace state change events. • debug—Trace debug messages. • event—Trace event handler events. • packet—Trace packet events. • all—Trace all areas of code. 3. In the Comment box, enter the comment for the flag.

Related Documentation

- [Configuring Link Management Protocol \(NSM Procedure\) on page 278](#)
- [Configuring Layer 2 Address Learning and Forwarding Properties \(NSM Procedure\) on page 258](#)

Configuring Layer 2 Address Learning and Forwarding Properties (NSM Procedure)

On MX Series routers only, you can configure Layer 2 address learning and forwarding properties in support of Layer 2 bridging. The router learns unicast media access control (MAC) addresses to avoid flooding the packets to all the ports in a bridge domain. The router creates a source MAC entry in its source and destination MAC tables for each MAC address learned from packets received on ports that belong to the bridge domain.

To configure Layer 2 address learning in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > L2 Learning**.

4. Add or modify settings as specified in [Table 131 on page 259](#).
5. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 131: L2 Learning Configuration Details

Task	Your Action
Configure Layer 2 address learning and forwarding properties globally.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment. 2. From the Global Mac Table Aging Time list, select the time elapsed before MAC table entries are timed out and entries are deleted. Range : 10 through 1000000 3. Select one of the following: <ul style="list-style-type: none"> • Global No Mac Learning—To disable MAC learning for the entire router • Global Mac Statistics—To enable MAC accounting for the entire router.
Limit the number of media access control (MAC) addresses learned from the logical interfaces on the router.	<ol style="list-style-type: none"> 1. Click Global Mac Limit next to L2 Learning. 2. In the Comment box, enter the comment. 3. From the Mac Limit list, select the Number of MAC addresses that can be learned systemwide. Range: 20 through 1,048,575 4. From the Packet Action list, select drop to specify that packets for new source MAC addresses be dropped after the MAC address limit is reached.

Related Documentation

- [Configuring Layer 2 Circuit \(NSM Procedure\) on page 259](#)
- [Configuring Layer 2 Protocol Tunneling and BPDU Protection \(NSM Procedure\) on page 265](#)

Configuring Layer 2 Circuit (NSM Procedure)

You can enable a Layer 2 circuit using the L2 Circuit option. See the following topics:

- [Configuring Local Interface Switching \(NSM Procedure\) on page 259](#)
- [Configuring the Neighbor Interface for the Layer 2 Circuit \(NSM Procedure\) on page 260](#)
- [Tracing Layer 2 Circuit Creation and Changes \(NSM Procedure\) on page 264](#)

Configuring Local Interface Switching (NSM Procedure)

You can configure a virtual circuit entirely on the local router, terminating the circuit on a local interface. Possible uses for this feature include being able to enable switching between frame relay Data-Link Connection Identifier (DLCI)s.

To configure local interface switching in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > L2 Circuit**.
4. Select **Local Switching**.
5. Add or modify settings as specified in [Table 132 on page 260](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 132: Local Switching Configuration Details

Task	Your Action
Configure a local switching interface.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment.
Configure the interface over which Layer 2 circuit traffic travels.	<ol style="list-style-type: none"> 1. Click Interface next to Local Switching. 2. Click Add new entry next to Interface. 3. In the Name box, enter the name of the interface to be configured. 4. In the Protect Interface box, enter the name of the protect interface to be configured. 5. In the Description box, enter the text description for the Layer 2 circuit. If the text includes one or more spaces, enclose the entire text string in quotation marks (" "). 6. Select the Ignore Mtu Mismatch check box to ignore the MTU configuration set for the physical interface associated with the local switching interface or with the remote Provider Edge (PE) router.
Specify the end interface for a local interface switch.	<ol style="list-style-type: none"> 1. Click End Interface next to interface. 2. In the Comment box, enter the comment. 3. In the Interface box, enter the name of the interface. 4. In the Protect Interface box, enter the name of the protect interface to be configured.

Configuring the Neighbor Interface for the Layer 2 Circuit (NSM Procedure)

Each Layer 2 circuit is represented by the logical interface connecting the local provider edge (PE) router to the local customer edge (CE) router. All the Layer 2 circuits using a particular remote PE router designated for remote CE routers are listed under the neighbor statement (neighbor designates the PE router). Each neighbor is identified by its IP address and is usually the end-point destination for the Label Switched Path (LSP) tunnel (transporting the Layer 2 circuit).

To configure a neighbor interface in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > L2 Circuit**.
4. Select **Neighbor**.
5. Add or modify settings as specified in [Table 133 on page 261](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 133: Neighbor Interface Configuration Details

Task	Your Action
Configure a neighbor.	<ol style="list-style-type: none">1. In the Name box, enter the IP address of a neighboring router.2. In the Comment box, enter the comment.

Table 133: Neighbor Interface Configuration Details (*continued*)

Task	Your Action
Configure the interface over which Layer 2 circuit traffic travels.	<ol style="list-style-type: none"> 1. Click Interface next to neighbor. 2. Click Add new entry next to Interface. 3. In the Name box, enter the interface name. 4. In the Comment box, enter the comment. 5. In the Psn Tunnel Endpoint box, enter the address for the tunnel endpoint. 6. In the Protect Interface box, enter the name of the protect interface to be configured. 7. From the Virtual Circuit Id list, select the identifier. Range: 1 through 4,294,967,295 8. In the Description box, enter the text description for the Layer 2 circuit. If the text includes one or more spaces, enclose the entire text string in quotation marks (" "). 9. Select one of the following: <ul style="list-style-type: none"> • control-word—To enable the use of the control word. • no-control-word—To disable the use of the control word. 10. In the Community box, specify the community for the Layer 2 circuit. 11. From the Mtu list, select the MTU number to be advertised for the Layer 2 circuit. Range: 512 through 65535 12. From the Encapsulation Type list, select the encapsulation type. 13. Select the Ignore Encapsulation Mismatch check box to allow a Layer 2 circuit to be established even though the encapsulation configured on the CE device interface does not match the encapsulation configured on the Layer 2 circuit interface. 14. Select the Ignore Mtu Mismatch check box to ignore the MTU configuration set for the physical interface associated with the local switching interface or with the remote PE router. 15. From the Switchover Delay list, select the time to wait before switching to the backup pseudowire after the primary pseudowire fails. Range: 0 through 180,000 milliseconds Default: 10,000 milliseconds

Table 133: Neighbor Interface Configuration Details (*continued*)

Task	Your Action
Configure pseudowire redundancy for Layer 2 circuits and Virtual Private LAN Service (VPLS).	<ol style="list-style-type: none"> 1. Click Interface next to neighbor. 2. Click Add new entry next to Interface. 3. Click Backup Neighbor next to interface. 4. Click Add new entry next to Backup Neighbor. 5. In the Name box, enter the interface name. 6. In the Comment box, enter the comment. 7. From the Virtual Circuit Id list, select the identifier. Range: 1 through 4,294,967,295 8. In the Community box, specify the community for the Layer 2 circuit. 9. In the Psn Tunnel Endpoint box, enter the address for the tunnel endpoint. 10. Select the Standby check box to configure the pseudowire to the specified backup neighbor as the standby. 11. Click Static next to backup-neighbor. 12. In the Comment box, enter the comment. 13. From the Incoming Label list, select the incoming label for the static pseudowire. Range: 1000000 through 1048575 14. From the Outgoing Label list, select the outgoing label for the static pseudowire. Range: 299776 through 1048575
Specify bandwidth allocation for a Layer 2 circuit or for the class types of a Layer 2 circuit.	<ol style="list-style-type: none"> 1. Click Interface next to neighbor. 2. Click Add new entry next to Interface. 3. Click Bandwidth next to interface. 4. In the Comment box, enter the comment. 5. In the Per Traffic Class Bandwidth box, enter the bandwidth in bits per second for a class type on the Layer 2 circuit. 6. In the Ctnumber box, enter the bandwidth in bits per second for a class type on the Layer 2 circuit. You can configure bandwidth for up to 4 class types (ct0, ct1, ct2, ct3) per Layer 2 circuit. If you configure the class types, you must configure them in order, starting with class type ct0.
Configure static Layer 2 circuit pseudowires.	<ol style="list-style-type: none"> 1. Click Interface next to neighbor. 2. Click Add new entry next to Interface. 3. Click Static next to interface. 4. In the Comment box, enter the comment. 5. From the Incoming Label list, select the incoming label for the static pseudowire. Range: 1000000 through 1048575 6. From the Outgoing Label list, select the outgoing label for the static pseudowire. Range: 299776 through 1048575 7. Select the Send Oam check box to send OAM.

Tracing Layer 2 Circuit Creation and Changes (NSM Procedure)

You can trace traffic flowing through a Layer 2 circuit using the Traceoptions option.

To configure tracing operations in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **L2 Circuit**.
4. Select **Traceoptions**.
5. Add or modify settings as specified in [Table 134 on page 264](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 134: Layer2 Circuit Traceoption Configuration Details

Task	Your Action
Trace traffic flowing through a Layer 2 circuit.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment.
Specify the name of the file to receive the output of the tracing operation and specifies the maximum number of trace files	<ol style="list-style-type: none"> 1. Click File next to Traceoptions. 2. In the Comment box, enter the comment for the file. 3. In the Filename box, enter the name of the file to receive the output of the tracing operation. 4. In the Size box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). 5. From the Files list, select the maximum number of trace files. Range: 2 through 1000. 6. Select one of the following: <ul style="list-style-type: none"> • world-readable—To enable unrestricted file access. • no-world-readable—To restrict file access to owner. This is the default setting.
Specify the tracing operation to perform.	<ol style="list-style-type: none"> 1. Click Flag next to Traceoptions. 2. Click Add new entry next to Flag. 3. From the Name list, select the flag. 4. In the Comment box, enter the comment for the flag. 5. Select the modifier for the tracing flag. Select one the following check boxes. <ul style="list-style-type: none"> • Send—Packets being transmitted • Receive—Packets being received • Detail—Detailed trace information • Disable—Disable tracing

Configuring Layer 2 Protocol Tunneling and BPDU Protection (NSM Procedure)

Layer 2 protocol tunneling allows Layer 2 protocol data units (PDUs) to be tunneled through a network. This is useful to provide a single Spanning Tree Protocol (STP) domain for subscribers across a service provider network. On the MX Series routers only, you can configure Bridge Protocol Data Unit (BPDU) protection to ignore BPDUs received on interfaces where none should be expected (for example, a LAN interface on a network edge with no other bridges present). If a BPDU is received on a blocked interface, the interface is disabled and stops forwarding frames. By default, all BPDUs are accepted and processed on all interfaces.

To configure layer 2 protocol tunneling and BPDU protection in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Layer2 Control**.
4. Add or modify settings as specified in [Table 135 on page 265](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 135: Layer2 Circuit Configuration Details

Task	Your Action
Enable BPDU blocking on an interface.	<ol style="list-style-type: none"> 1. Click Bpdu Block next to Layer2 Control. 2. In the Comment box, enter the comment. 3. From the Disable Timeout list, select the disable timeout value. Range: 10 through 3600 Default: If this option is not configured, the interface is not periodically checked and remains disabled 4. Click Interface next to Bpdu Block. 5. Click Add new entry next to Interface. 6. In the Name box, enter the interface name. 7. In the Comment box, enter the comment.

Table 135: Layer2 Circuit Configuration Details (*continued*)

Task	Your Action
Enable rewriting of the MAC address for Layer 2 protocol tunneling.	<ol style="list-style-type: none"> 1. Click mac Rewrite next to Layer2 Control. 2. In the Comment box, enter the comment. 3. Click Interface next to Bpdu Block. 4. Click Add new entry next to Interface. 5. In the Name box, enter the interface name. 6. In the Comment box, enter the comment. 7. Click Protocol next to interface. 8. In the Comment box, enter the comment. 9. Click Cdp next to Protocol. 10. In the Comment box, enter the comment. 11. Click Stp next to Protocol. 12. In the Comment box, enter the comment. 13. Click Vtp next to Protocol. 14. In the Comment box, enter the comment.
Define tracing options.	<ol style="list-style-type: none"> 1. Click Traceoptions next to Layer2 Control. 2. In the Comment box, enter the comment for the traceoptions. 3. Click File next to Traceoptions. 4. In the Comment box, enter the comment for the file. 5. In the Filename box, enter the name of the file to receive the output of the tracing operation. 6. In the Size box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). 7. From the Files list, select the maximum number of trace files. Range: 2 through 1000. 8. Select one of the following: <ul style="list-style-type: none"> • world-readable—To enable unrestricted file access. • no-world-readable—To restrict file access to owner. This is the default setting. 9. In the Match box, enter the regular expression. 10. Click Add new entry next to Flag. 11. From the Name list, select the flag. 12. Select the Disable check box to disable the tracing operation.

- Related Documentation**
- [Configuring Link Management Protocol \(NSM Procedure\) on page 278](#)
 - [Configuring Layer 2 Address Learning and Forwarding Properties \(NSM Procedure\) on page 258](#)

Configuring Label Distribution Protocol (NSM Procedure)

The Label Distribution Protocol (LDP) is a protocol for distributing labels in non-traffic-engineered applications. LDP allows routers to establish label-switched paths (LSPs) through a network by mapping network-layer routing information directly to data link layer-switched paths.

To configure LDP in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Protocols > LDP**.
4. Add or modify the settings as specified in [Table 136 on page 268](#).
5. Click one:
 - OK — To save the changes
 - Cancel — To cancel the modifications

Table 136: LDP Configuration Details

Task	Your Action
Configure LDP.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment. 2. From the Preference list, select the route preference level for LDP routes. Range: 0 through 4,294,967,295 3. Select the No Forwarding check box to omit the Ingress routes from the inet.0 routing table. 4. Select the L2 Smart Policy check box to prevent LDP from exporting IPv6 FECs over sessions with layer 2 neighbors. 5. Select the Track IGP Metric check box to cause the IGP route metric to be used for the LDP routes instead of the default LDP route metric. 6. Select the Strict Targeted Hellos check box to prevent LDP sessions from being established with remote neighbors that have not been specifically configured. 7. Select one of the following: <ul style="list-style-type: none"> • deaggregate—To control forwarding equivalence class (FEC) deaggregation on the router. • no-deaggregate—To control forwarding equivalence class (FEC) aggregation on the router. 8. Select the Explicit Null check box to advertise label 0 to the egress router of a label-switched path (LSP). 9. From the Label Withdrawal Delay list, select the number of seconds to wait before withdrawing labels for the LDP LSPs. Default: 60 seconds Range: 0 through 120 seconds 10. From the Keep Alive Interval list, select a Keep Alive value. Range: 1 through 65,535 seconds Default: 10 seconds 11. From the Keep Alive Timeout list, select a Keep Alive Timeout value. Range: 1 through 65,535 seconds Default: 30 seconds
Configure the prefixes advertised into LDP from the routing table.	<ol style="list-style-type: none"> 1. Expand LDP. 2. Click Egress Policy next to LDP. 3. Click Add after selecting a policy member from the Non member list to add it to the Members list. 4. Click Remove after selecting a policy from the Members list to remove it from the Members list. 5. Click Add All to add all the Non members to the Members list. 6. Click Remove All to remove all the members from the Members list.

Table 136: LDP Configuration Details (*continued*)

Task	Your Action
Apply policy filters to outbound LDP label bindings.	<ol style="list-style-type: none"> 1. Click Export next to LDP. 2. Click Add after selecting a policy member from the Non-member list to add it to the Members list. 3. Click Remove after selecting the policy from the Members list to remove it from the Members list. 4. Click Add All to add all the Non-members to the Members list. 5. Click Remove All to remove all the members from the Members list.
Enable LDP graceful restart on the LDP master protocol instance or for a specific routing instance.	<ol style="list-style-type: none"> 1. Click Graceful Restart next to LDP. 2. Select the Disable check box to explicitly disable LDP on an interface, or explicitly disable LDP graceful restart. 3. Select the Helper Disable check box to disable helper mode for LDP graceful restart. 4. From the Recovery Time list, select the amount of time a router waits for LDP to restart gracefully. Range: 120 through 1800 seconds Default: 140 seconds 5. From the Maximum Neighbor Recovery Time list, select the maximum amount of time to wait before giving up an attempt to gracefully restart. Range: 120 through 1900 seconds Default: 140 seconds 6. From the Reconnect Time list, select the reconnect time. Range: 30 through 300 7. From the Maximum Neighbor Reconnect Time list, select the maximum time allowed for reconnection. Range: 30 through 300
Apply policy filters to received LDP label bindings.	<ol style="list-style-type: none"> 1. Click Import next to LDP. 2. Click Add after selecting a policy member from the Non-member list to add it to the Members list. 3. Click Remove after selecting a policy from the Members list to remove it from the Members list. 4. Click Add All to add all the Non-members to the Members list. 5. Click Remove All to remove all the members from the Members list.

Table 136: LDP Configuration Details (*continued*)

Task	Your Action
Enable LDP on one or more router interfaces.	<ol style="list-style-type: none"> Click Interface next to LDP. Click Add new entry next to Interface. In the Name box, enter the name of the interface. Select the Disable check box to disable LDP on the interface. From the Hello Interval list, select a value to control the rate at which hello messages are sent on the interface. Range: 1 through 65,535 seconds Default: 5 seconds for link hello messages, 15 seconds for targeted hello messages From the Hold Time list, select a hold time to specify how long an LDP node should wait for a hello message before declaring a neighbor to be down. Range: 1 through 65,535 seconds Default: 15 seconds for link hello messages, 45 seconds for targeted hello messages From the Transport Address list, select the transport address. Select one of the following: <ul style="list-style-type: none"> router-id—The router identifier is used as the transport address interface—The first IP address on the interface is used as the transport address Select one of the following: <ul style="list-style-type: none"> Allow-Subnet-Mismatch—To ignore the LDP subnet check. No-Allow-Subnet-Mismatch—To enable the LDP subnet check.
Disable LDP traps.	<ol style="list-style-type: none"> Click Log Updown next to LDP. In the Comment box, enter the comment. Click Trap next to Log Updown. In the Comment box, enter the comment. Select the Disable check box to disable LDP traps.

Table 136: LDP Configuration Details (*continued*)

Task	Your Action
Specify merged next-hop policy.	<ol style="list-style-type: none">1. Click Next Hop next to LDP.2. In the Comment box, enter the comment.3. Click Merged next to Next Hop.4. In the Comment box, enter the comment.5. Click Policy next to Merged.6. Click Add after selecting a policy member from the Non member list to add it to the Members list.7. Click Remove after selecting a policy from the Members list to remove it from the Members list.8. Click Add All to add all the Non members to the Members list.9. Click Remove All to remove all the members from the Members list.

Table 136: LDP Configuration Details (*continued*)

Task	Your Action
Enable OAM for all of the LDP LSPs or for a specific LDP LSP.	<ol style="list-style-type: none"> Click Oam next to LDP. In the Comment box, enter the comment. From the Lsp Ping Interval list, select the time interval between LSP ping messages. Range: 30 through 3600 Click Bfd Liveness Detection next to Oam. In the Comment box, enter the comment. From the Version list, select the BFD protocol version to detect. Range: 1 (BFD version 1), or automatic (autodetection) Default: automatic From the Minimum Interval list, select the minimum transmit and receive interval. Range: 1 through 255,000 From the Minimum Receive Interval list, select the minimum receive interval. Range: 1 through 255,000 From the Multiplier list, select the detection time multiplier. Range: 1 through 255 Default: 3 Select the No Adaptation check box to disable BFD adaptation. Select the Ecmp check box to cause RSVP to establish BFD sessions for all ECMP paths configured for the specified FEC. From the Holddown Interval list, select the time the BFD session must remain up before state change notification is sent. Range: 1 through 255000 Click Detection Time next to Bfd Liveness Detection. In the Comment box, enter the comment. From the Threshold list, select the time the BFD session must remain up before state change notification is sent. Range: 1 through 4294967295

Table 136: LDP Configuration Details (*continued*)

Task	Your Action
Configure route and next-hop properties in the event of a BFD session failure event on an LDP LSP.	<ol style="list-style-type: none"> Click Failure Action next to Bfd Liveness Detection. In the Comment box, enter the comment. Select one of the following: <ul style="list-style-type: none"> remove-route—To remove LDP route from the ribs remove-nexthop—To remove LDP nexthop from the route Click Transmit Interval next to Bfd Liveness Detection. In the Comment box, enter the comment. From the Minimum Interval list, select the minimum transmit and receive interval. Range: 1 through 255,000 From the Threshold list, select the time the BFD session must remain up before state change notification is sent. Range: 1 through 4294967295

Table 136: LDP Configuration Details (*continued*)

Task	Your Action
Enable Bidirectional Forwarding Detection (BFD) for all MPLS LSPs or for just a specific LSP.	<ol style="list-style-type: none"> 1. Click Fec next to Oam. 2. In the Name box, enter the forwarding equivalence class (FEC) address. 3. In the Comment box, enter the comment. 4. Click Bfd Liveness Detection next to Fec. 5. Select one of the following: <ul style="list-style-type: none"> • bfd-liveness-detection—To enable BFD for all MPLS LSPs or for just a specific LSP. • no-bfd-liveness-detection—To disable BFD for all MPLS LSPs or for just a specific LSP. 6. Click Periodic Traceroute next to fec. 7. In the Comment box, enter the comment. 8. From the Frequency list, select the interval between traceroute attempts. Range: 15 through 120 minutes 9. From the Ttl list, select the maximum time-to-live value. Range: 1 through 255 10. From the Retries list, select the number of attempts to send a probe to a specific node before giving up. Range: 1 through 9 11. From the Wait list, select the wait interval before resending a probe packet. Range: 5 though 15 seconds 12. From the Paths list, select the maximum number of paths to search. Range: 1 through 255 13. In the Source box, enter the IPv4 source address to use when sending probes. 14. From the Exp list, select the class of service to use when sending probes. Range: 0 through 7 15. From the Fanout list, select the maximum number of next hops to search per node. Range: 1 through 16 16. Select Disable check box to disable tracing for a specific FEC. Range: 1 through 16

Table 136: LDP Configuration Details (*continued*)

Task	Your Action
Enable an OAM ingress policy.	<ol style="list-style-type: none"> 1. Click Ingress Policy next to Oam. 2. Click Add after selecting a policy member from the Non member list to add it to the Members list. 3. Click Remove after selecting a policy from the Members list to remove it from the Members list. 4. Click Add All to add all the Non members to the Members list. 5. Click Remove All to remove all the members from the Members list.
Enable tracing of forwarding equivalence classes (FECs) for LDP LSPs.	<ol style="list-style-type: none"> 1. Click Periodic Traceroute next to Oam. 2. In the Comment box, enter the comment. 3. From the Frequency list, select the interval between traceroute attempts. Range: 15 through 120 minutes 4. From the Ttl list, select the maximum time-to-live value. Range: 1 through 255 5. From the Retries list, select the number of attempts to send a probe to a specific node before giving up. Range: 1 through 9 6. From the Wait list, select the wait interval before resending a probe packet. Range: 5 though 15 seconds 7. From the Paths list, select the maximum number of paths to search. Range: 1 through 255 8. In the Source box, enter the IPv4 source address to use when sending probes. 9. From the Exp list, select the class of service to use when sending probes. Range: 0 through 7 10. From the Fanout list, select the maximum number of next hops to search per node. Range: 1 through 16

Table 136: LDP Configuration Details (*continued*)

Task	Your Action
Enable policing of forwarding equivalence classes (FECs) for LDP.	<ol style="list-style-type: none"> 1. Click Policing next to Ldp. 2. In the Comment box, enter the comment. 3. Click Fec next to Policing. 4. Click Add new entry next to Fec. 5. In the Name box, enter the address for the FEC. 6. In the Comment box, enter the comment. 7. From the Ingress Traffic list, select the name of the filter for policing ingress FEC traffic. 8. From the Transit Traffic list, select the name of the filter for policing transit FEC traffic.
Specify the LDP session to which you want to attach the Transmission Control Protocol (TCP) MD5 signature.	<ol style="list-style-type: none"> 1. Click Session next to Ldp. 2. Click Add new entry next to Session. 3. In the Name box, enter the address for the remote end of the LDP session. 4. In the Comment box, enter the comment. 5. In the Authentication Key box, enter the authentication key. 6. From the Authentication Algorithm list, select the algorithm. 7. In the Authentication Key Chain box, enter the MD5 authentication signature. The maximum length of the authentication signature is 69 characters.
Configure session protection.	<ol style="list-style-type: none"> 1. Click Session Protection next to Ldp. 2. From the Timeout list, select the session protection timeout. Range: 1 through 65535
Specify parameters for targeted hellos.	<ol style="list-style-type: none"> 1. Click Targeted Hello next to Ldp. 2. In the Comment box, enter the comment. 3. From the Hello Interval list, select the hello interval in seconds. Range: 1 through 65535 4. From the Hold Time list, select the hold time interval in seconds. Range: 1 through 65535

Table 136: LDP Configuration Details (*continued*)

Task	Your Action
Configure LDP protocol-level trace options.	<ol style="list-style-type: none"> 1. Click Traceoptions next to Ldp. 2. In the Comment box, enter the comment for the traceoptions. 3. Click File next to Traceoptions. 4. In the Comment box, enter the comment for the file. 5. In the Filename box, enter the name of the file to receive the output of the tracing operation. 6. In the Size box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). 7. From the Files list, select the maximum number of trace files. Range: 2 through 1000 8. Select one of the following: <ul style="list-style-type: none"> • world-readable—To enable unrestricted file access. • no-world-readable—To restrict file access to owner. This is the default setting.
Configure LDP traffic statistics.	<ol style="list-style-type: none"> 1. Click Traffic Statistics next to Ldp. 2. In the Comment box, enter the comment. 3. From the Interval list, select the interval at which the statistics are polled and written to the file. Range: 60 through 65535 4. Select No Penultimate Hop check box to disable penultimate hop statistics collection. 5. Click File next to Traffic Statistics. 6. In the Comment box, enter the comment for the file. 7. In the Filename box, enter the name of the file to receive the output of the tracing operation. 8. In the Size box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). 9. From the Files list, select the maximum number of trace files. Range: 2 through 1000 10. Select one of the following: <ul style="list-style-type: none"> • world-readable—To enable unrestricted file access. • no-world-readable—To restrict file access to owner. This is the default setting.

Table 136: LDP Configuration Details (*continued*)

Task	Your Action
Allow control of the transport address used by LDP.	<ol style="list-style-type: none"> 1. Click Transport Address next to Ldp. 2. In the Comment box, enter the comment. 3. Click Router Id next to Transport Address. 4. Select one of the following: <ul style="list-style-type: none"> • router-id—The router identifier is used as the transport address. • interface—The first IP address on the interface is used as the transport address. • address—IP address to be advertised as the transport address.

- Related Documentation**
- [Configuring the ILMI Protocol \(NSM Procedure\) on page 257](#)
 - [Configuring RSVP \(NSM Procedure\) on page 358](#)
 - [Configuring Link Management Protocol \(NSM Procedure\) on page 278](#)

Configuring Link Management Protocol (NSM Procedure)

Link Management is a protocol used to define a forwarding adjacency between peers and to maintain and allocate resources on the traffic engineering links. It defines the data channel connection and the control channel connection between devices.

To configure link management in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Protocols > Link Management**.
4. Add or modify the settings as specified in [Table 137 on page 279](#).
5. Click one:
 - **OK**—To save the changes.
 - **Cancel**—To cancel the modifications.

Table 137: Link Management Protocol Configuration Details

Task	Your Action
Configure a network peer.	<ol style="list-style-type: none">1. Click Peer next to Link Management.2. Click Add new entry next to Peer.3. In the Name box, enter the name of the peer.4. In the Comment box, enter the comment.5. In the Address box, enter the ID of the peer.6. Expand Peer.7. Click Control Channel next to Peer.8. Click Add new entry next to Control Channel.9. In the dialog box, enter the name of the control channel interface.

Table 137: Link Management Protocol Configuration Details (*continued*)

Task	Your Action
Configure a Lmp Control Channel.	<ol style="list-style-type: none"> 1. Click Lmp Control Channel next to peer. 2. Click Add new entry next to Lmp Control Channel. 3. In the Name box, enter the peer name. 4. In the Comment box, enter the comment. 5. In the Remote Address box, enter the remote IP address for the Link Management Protocol (LMP) control channel interface. 6. Click Lmp Protocol next to peer. 7. In the Comment box, enter the comment. 8. From the Hello Interval list, select how often the router sends Link Management Protocol (LMP) hello packets. Range: 150 through 21845 Default: 150 milliseconds 9. From the Hello Dead Interval list, select how long the Link Management Protocol (LMP) waits before declaring the control channel to be dead. Range: 500 through 300,000 Default: 500 milliseconds (three times the hello interval) 10. From the Retransmission Interval list, select how often Link Management Protocol (LMP) sends Config and LinkSummary messages on the LMP control channel. Range: 500 through 300,000 Default: 500 milliseconds 11. From the Retry Limit list, select the maximum number of times messages are sent without receiving an acknowledgment. Range: 3 through 1000 Default: 3 12. Select Passive check box to specify the router to not configure the Link Management Protocol (LMP) control channels, but to wait for the remote peer to configure the LMP control channels. 13. Click Te-Link next to peer. 14. Click Add new entry next to Te-Link. 15. In the dialog box, enter the name of the te-link to be associated with this peer.

Table 137: Link Management Protocol Configuration Details (*continued*)

Task	Your Action
Represent a collection of physical ports or time slots.	<ol style="list-style-type: none"> 1. Click Add new entry next to Te Link. 2. In the Name box, enter the name of the collection of physical ports or the name of the time slots. 3. In the Comment box, enter the comment. 4. In the Local Address box, enter the local IP address associated with the traffic engineering link. 5. In the Remote Address box, enter the remote IP address for the traffic engineering link. 6. From the Remote ID list, select the ID assigned to a traffic engineering link or an interface on the peer node. Range: 1 through 4294967295 7. From the Te Metric list, select the metric value. Range: 1 through 65535 8. Select Disable check box to disable the traffic engineering link or an interface to a traffic engineering link. 9. Expand te-link. 10. Click Interface next to te-link. <ul style="list-style-type: none"> • Select interface to specify the egress router interface. • Select label-switched-path to specify the LSP to be used by the forwarding adjacency.
Specify trace options for the LMP protocol.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment. 2. Expand Traceoptions. 3. Click File next to Trace Options. 4. In the Comment box, enter the comment. 5. In the Filename box, enter the name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. 6. In the Size box, enter the maximum size of each trace file in kilobytes (KB), megabytes (MB) or gigabytes (GB). 7. From the Files list, select the maximum number of files. 8. Select world-readable to enable log file access to all users. 9. Select no-world-readable to prevent all users from reading the log file. 10. Click Flag next to Trace Options. 11. Click Add new entry next to flag. 12. From the Name list, select a tracing operation to perform. 13. In the Comment box, enter the comment.

Related Documentation

- [Configuring the ILMI Protocol \(NSM Procedure\) on page 257](#)

- [Configuring RSVP \(NSM Procedure\) on page 358](#)
- [Configuring Layer 2 Circuit \(NSM Procedure\) on page 259](#)

Configuring MPLS Protocol (NSM Procedure)

You can enable MPLS on the router using the MPLS option. See the following topics:

- [Enabling MPLS on the Router \(NSM Procedure\) on page 282](#)
- [Configuring Administrative Group \(NSM Procedure\) on page 285](#)
- [Configuring Administrative Groups \(NSM Procedure\) on page 285](#)
- [Configuring Bandwidth for the Reroute Path \(NSM Procedure\) on page 286](#)
- [Configuring DiffServ-Aware Traffic Engineering \(NSM Procedure\) on page 287](#)
- [Configuring MPLS on Interfaces \(NSM Procedure\) on page 288](#)
- [Configure a Label Switched Path \(LSP\) to Use in Dynamic MPLS on page 290](#)
- [Configuring System Log Messages and SNMP Traps for LSPs \(NSM Procedure\) on page 316](#)
- [Configuring BFD for MPLS IPv4 LSPs \(NSM Procedure\) on page 317](#)
- [Configuring Named Paths \(NSM Procedure\) on page 319](#)
- [Configuring MTU Signaling in RSVPs \(NSM Procedure\) on page 320](#)
- [Configuring static LSPs on the Ingress Router \(NSM Procedure\) on page 321](#)
- [Configuring MPLS Statistics \(NSM Procedure\) on page 322](#)
- [Tracing MPLS Packets and Operations \(NSM Procedure\) on page 323](#)

Enabling MPLS on the Router (NSM Procedure)

You can enable MPLS on the router using the MPLS option.

To enable MPLS on the router in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Mpls**.
5. Add or modify settings as specified in [Table 138 on page 283](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 138: MPLS Configuration Details

Task	Your Action
Enable MPLS on the router.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment. 2. Select the Disable check box to disable the functionality of the configured object. 3. From the Traffic Engineering list, select whether MPLS performs traffic engineering on BGP destinations only or on both BGP and IGP destinations. 4. From the Advertisement Hold Time list, select the hold time, in seconds. Range: 0 through 65,535 seconds Default: 5 seconds 5. From the Rsvp Error Hold Time list, select the amount of time MPLS retains RSVP PathErr messages and considers them for CSPF computations. Range: 0 through 240 seconds Default: 25 seconds 6. Select the Optimize Aggressive check box to enable aggressive optimization. 7. From the Smart Optimize Timer list, select the number of seconds to wait before switching an LSP back to its original path. Range: 0 through 65,535 seconds Default: 180 seconds 8. Select the No Propagate Ttl check box to disable normal time-to-live (TTL) decrementing. 9. Select the Explicit Null check box to advertise label 0 to the egress router of an LSP. 10. Select the IPv6 Tunneling check box to allow IPv6 routes to be resolved over an MPLS network. 11. Select the Icmp Tunneling check box to enable ICMP tunneling, which can be used for debugging and tracing purposes. 12. From the Revert Timer list, select the amount of time (in seconds) that an LSP must wait before traffic reverts to a primary path. Range: 0 through 65,535 seconds Default: 60 seconds

Table 138: MPLS Configuration Details (*continued*)

Task	Your Action
	<p>13. Select the Expand Loose Hop check box to allow an LSP to traverse multiple OSPF areas within a service provider's network.</p> <p>14. From the Class Of Service list, select the CoS value. Range: 0 through 7 Default: If you do not specify a CoS value, the IP precedence bits from the packet's IP header are used as the packet's CoS value.</p> <p>15. Select the No Decrement Ttl check box to disable normal time-to-live (TTL) decrementing.</p> <p>16. From the Hop Limit list, select the maximum number of hops. Range: 2 through 255 (for an LSP); 0 through 255 (for fast reroute) Default: 255 (for an LSP); 6 (for fast reroute)</p> <p>17. Select the No Cspf check box to disable constrained-path LSP computation.</p> <p>18. Select the Admin Down check box to indicate the administrative down status for an LSP.</p> <p>19. From the Optimize Timer list, select the length of the optimize timer, in seconds. Range: 0 through 65,535 seconds Default: 0 seconds (the optimize timer is disabled)</p> <p>20. From the Preference list, select the preference to assign to the route. A route with a lower preference value is preferred. Range: 0 through 4,294,967,295 Default: 5 for static MPLS LSPs, 7 for RSVP MPLS LSPs, 9 for LDP MPLS LSPs</p> <p>21. From the Setup Priority list, select the setup priority. Range: 0 through 7, where 0 is the highest and 7 is the lowest priority Default: 7 (The session cannot preempt any existing sessions.)</p> <p>22. From the Reservation Priority list, select the reservation priority, used to keep a reservation after it has been set up. Range: 0 through 7, where 0 is the highest and 7 is the lowest priority Default: 0 (Once the session is set up, no other session can preempt it.)</p> <p>23. Select one of the following:</p> <ul style="list-style-type: none"> • record—to specify whether an LSP should actively record the routes in the path. • no-record—to specify whether an LSP should not record the routes in the path. <p>24. Select the standby check box to have the path remain up at all times to provide instant switchover if connectivity problems occur.</p>

Configuring Administrative Group (NSM Procedure)

You can configure an administrative group constraint for each LSP or for each primary or secondary LSP path using the Admin Group option.

To configure an administrative group in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Mpls**.
5. Add or modify settings as specified in [Table 139 on page 285](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 139: Administrative Group Configuration Details

Task	Your Action
Configure administrative group.	<ol style="list-style-type: none"> 1. Click Admin Group next to Mpls. 2. In the Comment box, enter the comment.
Define the administrative groups to exclude for an LSP or for a path's primary and secondary paths.	<ol style="list-style-type: none"> 1. Click Exclude next to Admin Group. 2. Click Add new entry next to Exclude. 3. In the New exclude window, enter the names of one or more groups.
Require the LSP to traverse links that include all of the defined administrative groups.	<ol style="list-style-type: none"> 1. Click Include All next to Admin Group. 2. Click Add new entry next to Include All. 3. In the New include-all window, enter the names of one or more groups.
Define the administrative groups to include for an LSP or for a path's primary and secondary paths.	<ol style="list-style-type: none"> 1. Click Include Any next to Admin Group. 2. Click Add new entry next to Include Any. 3. In the New include-any window, enter the names of one or more groups.

Configuring Administrative Groups (NSM Procedure)

You can configure administrative groups to implement link coloring of resource classes using the Admin Groups option.

To configure administrative groups in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.

3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Mpls**.
5. Add or modify settings as specified in [Table 140 on page 286](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 140: Administrative Groups Configuration Details

Task	Your Action
Configure administrative groups.	<ol style="list-style-type: none"> 1. Click Admin Groups next to Mpls. 2. Click Add new entry next to Admin Groups. 3. In the Name box, enter the name of the group. You can assign up to 32 names. 4. In the Comment box, enter the comment. 5. From the Group Value list, select the value assigned to the group. Range: 0 through 31
Define the administrative groups to exclude for an LSP or for a path's primary and secondary paths.	<ol style="list-style-type: none"> 1. Click Exclude next to Admin Group. 2. Click Add new entry next to Exclude. 3. In the New exclude window, enter the names of one or more groups.
Require the LSP to traverse links that include all of the defined administrative groups.	<ol style="list-style-type: none"> 1. Click Include All next to Admin Group. 2. Click Add new entry next to Include All. 3. In the New include-all window, enter the names of one or more groups.
Define the administrative groups to include for an LSP or for a path's primary and secondary paths.	<ol style="list-style-type: none"> 1. Click Include Any next to Admin Group. 2. Click Add new entry next to Include Any. 3. In the New include-any window, enter the names of one or more groups.

Configuring Bandwidth for the Reroute Path (NSM Procedure)

When configuring fast reroute, allocate bandwidth for the reroute path. By default, no bandwidth is reserved for the rerouted path. The fast reroute bandwidth does not need to be identical to that allocated for the LSP itself.

To configure bandwidth for the reroute path in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Mpls**.

5. Add or modify settings as specified in [Table 141 on page 287](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 141: Automatic Policers Configuration Details

Task	Your Action
Allocate bandwidth for the reroute path.	<ol style="list-style-type: none"> 1. Click Bandwidth next to Mpls. 2. In the Comment box, enter the comment. 3. In the Per Traffic Class Bandwidth box, enter the bandwidth, in bits per second. 4. In the Ct0 box, enter the bandwidth, for the specified class. 5. In the Ct1 box, enter the bandwidth, for the specified class. 6. In the Ct2 box, enter the bandwidth, for the specified class. 7. In the Ct3 box, enter the bandwidth, for the specified class.
Apply the same policer action to all the class types.	<ol style="list-style-type: none"> 1. Click Class next to Automatic Policing. 2. Click Add new entry next to Class. 3. From the Name list, select the class type to which the policer action is to be applied. 4. In the Comment box, enter the comment. 5. Select one of the policer actions. <ul style="list-style-type: none"> • drop—Drop all packets. • loss-priority-high—Set the packet loss priority (PLP) to high. • loss-priority-low—Set the PLP to low.

Configuring DiffServ-Aware Traffic Engineering (NSM Procedure)

Differentiated Services (DiffServ)-aware traffic engineering provides a way to guarantee a specified level of service over an MPLS network. The routers providing DiffServ-aware traffic engineering are part of a differentiated services network domain. All routers participating in a differentiated services domain must have DiffServ-aware traffic engineering enabled.

To configure DiffServ-aware traffic engineering in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Mpls**.
5. Add or modify settings as specified in [Table 142 on page 288](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 142: DiffServ-Aware Traffic Engineering Configuration Details

Task	Your Action
Configure DiffServ-aware traffic engineering.	<ol style="list-style-type: none"> 1. Click Diffserv Te next to Mpls. 2. In the Comment box, enter the comment. 3. In the Per Traffic Class Bandwidth box, enter the bandwidth, in bits per second. 4. From the Bandwidth Model list, select the bandwidth model for differentiated services. <ul style="list-style-type: none"> • extended-mam—The extended maximum allocation model (MAM) is a bandwidth model based on MAM. • mam—The MAM is defined in RFC 4125, Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering. • rdm—The Russian dolls bandwidth allocation model (RDM) is defined in RFC 4127, <i>Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering</i>.
Specify the traffic engineering class matrix for a multiclass label switched path (LSP) or a DiffServ-aware traffic engineering LSP.	<ol style="list-style-type: none"> 1. Click Te Class Matrix next to Diffserv Te. 2. In the Comment box, enter the comment. 3. For the traffic engineering classes, configure the following: <ol style="list-style-type: none"> a. In the Comment box, enter the comment. b. From the Traffic Class list, select the traffic class for the traffic engineering class. c. From the Priority list, select the priority of the class type. Range: 0 through 7

Configuring MPLS on Interfaces (NSM Procedure)

To configure MPLS on interfaces in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Mpls**.
5. Add or modify settings as specified in [Table 143 on page 289](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 143: Interface Configuration Details

Task	Your Action
Enable MPLS on one or more interfaces.	<ol style="list-style-type: none"> 1. Click Interface next to Mpls. 2. Click Add new entry next to Interface. 3. In the Name box, enter the Name of the interface on which to configure MPLS. 4. In the Comment box, enter the comment. 5. Select the Disable check box to disable the functionality of the configured object.
Define administrative groups for an interface.	<ol style="list-style-type: none"> 1. Click Admin Group next to interface. 2. In the Comment box, enter the comment. 3. Click Add new entry next to Admin Group. 4. In the New admin-group window, enter one or more names of groups.
Label MPLS packets.	<ol style="list-style-type: none"> 1. Click Label Map next to interface. 2. Click Add new entry next to Label Map. 3. In the Name box, enter the interface name. 4. From the Swap list, select the label value. Range: 1,000,000 through 1,048,575. Labels 0 through 999,999 are for internal use. Labels 1,000,000 through 1,048,575 are unassigned by the Junos OS and are available for static label switched paths (LSPs). When you configure static LSPs, you can use only this range of labels. 5. From the Swap Label list, select the label value. 6. From the Push Label list, select the label value. Range: 0 through 1,048,575 7. Select the Pop check box to remove the label from the top of the label stack. 8. From the Preference list, select the preference to be assigned to the route. Range: 0 through 4,294,967,295 Default: 5 for static MPLS LSPs, 7 for RSVP MPLS LSPs, 9 for LDP MPLS LSPs 9. From the Class of Service list, select the CoS value. Range: 0 through 7 Default: If you do not specify a CoS value, the IP precedence bits from the packet's IP header are used as the packet's CoS value
Configure IP address of the next hop to the destination.	<ol style="list-style-type: none"> 1. Select one of the following: <ul style="list-style-type: none"> • next-hop—to configure the IP address of the next hop to the destination. <ol style="list-style-type: none"> a. Enter the IP address of the next-hop router. • reject—to reject the packet. • discard—to discard the packet.

Configure a Label Switched Path (LSP) to Use in Dynamic MPLS

- [Configuring Label Switched Path \(NSM Procedure\) on page 290](#)
- [Configuring Administrative Group \(NSM Procedure\) on page 293](#)
- [Configuring Automatic Bandwidth Allocation for LSPs \(NSM Procedure\) on page 294](#)
- [Configuring Bandwidth for the Reroute Path \(NSM Procedure\) on page 295](#)
- [Configuring Fast Reroute \(NSM Procedure\) on page 296](#)
- [Adding LSP-Related Routes to the inet.3 Routing Table \(NSM Procedure\) on page 297](#)
- [Configuring MPLS LSPs for GMPLS \(NSM Procedure\) on page 298](#)
- [Configuring BFD for MPLS IPv4 LSPs \(NSM Procedure\) on page 299](#)
- [Configuring the Primary Point-to-Multipoint LSP \(NSM Procedure\) on page 301](#)
- [Configuring Policers for LSPs \(NSM Procedure\) on page 302](#)
- [Configuring Primary Paths for an LSP \(NSM Procedure\) on page 303](#)
- [Configuring Secondary Paths for an LSP \(NSM Procedure\) on page 308](#)

Configuring Label Switched Path (NSM Procedure)

You can configure a label switched path (LSP) to use in dynamic MPLS.

To configure a LSP in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in [Table 144 on page 291](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 144: LSP Configuration Details

Task	Your Action
Configure label switched path.	<ol style="list-style-type: none"> 1. Click Add new entry next to Label Switched Path. 2. In the Name box, enter the name that identifies the LSP. 3. In the Comment box, enter the comment. 4. Select the Disable check box to disable the functionality of the configured object. 5. Select the No Install To Address check box to prevent the egress router address configured using the <code>to</code> statement from being installed into the inet.3 and inet.0 routing tables. 6. Select the Backup check box to configure a backup provider edge (PE) group for ingress PE router redundancy when point-to-multipoint LSP are used for multicast distribution. 7. In the From box, enter the source address to use for the LSP.
	<ol style="list-style-type: none"> 8. Select the Ldp Tunneling check box to enable the LSP to be used for LDP tunneling. 9. From the Metric list, select the LSP metric value Default: No metric assigned (dynamic) Range: 1 through 16,777,215 10. From the Retry Timer list, select the amount of time between attempts to connect to the primary path. Default: 30 seconds Range: 1 through 600 seconds 11. From the Retry Limit list, select the maximum number of tries to establish the primary path. Default: 0 (The ingress node never stops trying to establish the primary path.) Range: 0 through 10,000 12. From the Revert Timer list, select the amount of time (in seconds) that an LSP must wait before traffic reverts to a primary path. Default: 60 seconds Range: 0 through 65,535 seconds 13. From the Class Of Service list, select the CoS value. Range: 0 through 7. Default: If you do not specify a CoS value, the IP precedence bits from the packet's IP header are used as the packet's CoS value. 14. Select the No Decrement Ttl check box to disable normal time-to-live (TTL) decrementing. 15. From the Hop Limit list, select the maximum number of hops. Range: 2 through 255 (for an LSP); 0 through 255 (for fast reroute) Default: 255 (for an LSP); 6 (for fast reroute) 16. Select the No Cspf check box to disable constrained-path LSP computation.

Table 144: LSP Configuration Details (*continued*)

Task	Your Action
	17. Select the Admin Down check box to set the A-bit in the Admin Status object.
	18. From the Optimize Timer list, select the length of the optimize timer, in seconds. Range: 0 through 65,535 seconds Default: 0 seconds (the optimize timer is disabled)
	19. From the Preference list, select the preference to assign to the route. Range: 1 through 255 Default: 5 for static MPLS LSPs, 7 for RSVP MPLS LSPs, 9 for LDP MPLS LSPs
	20. From the Setup Priority list, select the setup priority. Range: 0 through 7, where 0 is the highest and 7 is the lowest priority. Default: 7 (The session cannot preempt any existing sessions.)
	21. From the Reservation Priority list, select the reservation priority. Range: 0 through 7, where 0 is the highest and 7 is the lowest priority. Default: 0 (Once the session is set up, no other session can preempt it.)

Table 144: LSP Configuration Details (*continued*)

Task	Your Action
	<p>22. Select one of the following:</p> <ul style="list-style-type: none"> • record—Record routes • no-record—Does not record routes <p>23. Select the Standby check box to have the path remain up at all times to provide instant switchover if connectivity problems occur.</p> <p>24. Select one of the following options:</p> <ul style="list-style-type: none"> • random—Choose the path at random. • least-fill—Prefer the path with the most available bandwidth (with the largest minimum available bandwidth ratio). • most-fill—Prefer the path with the least available bandwidth (with the minimum available bandwidth ratio). The minimum available bandwidth ratio of a path is the smallest available bandwidth ratio belonging to any of the links in the path. <p>25. In the Description box, enter the textual description of the LSP.</p> <p>26. Select one of the following options:</p> <ul style="list-style-type: none"> • link-protection—Enable link protection. • node-link-protection—Enable node and link protection on the specified LSP. • most-fill—Prefer the path with the least available bandwidth (with the minimum available bandwidth ratio). The minimum available bandwidth ratio of a path is the smallest available bandwidth ratio belonging to any of the links in the path. <p>27. Select the Adaptive check box for RSVP to use shared explicit (SE) reservation styles and assists in smooth transition during rerouting.</p> <p>28. Select the Associate backup Pe Groups check box to enable an LSP to monitor the status of its destination PE router.</p>

Configuring Administrative Group (NSM Procedure)

You can configure an administrative group constraint for each Label Switched Path (LSP) or for each primary or secondary LSP path using the Admin Group option.

To configure an administrative group in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > MPLS**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in [Table 145 on page 294](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 145: Administrative Group Configuration Details

Task	Your Action
Configure administrative group.	<ol style="list-style-type: none"> 1. Click Add new entry next to Label Switched Path. 2. Click Admin Group next to label-switched-path. 3. In the Comment box, enter the comment.
Define the administrative groups to exclude for an LSP or for a path's primary and secondary paths.	<ol style="list-style-type: none"> 1. Click Exclude next to Admin Group. 2. Click Add new entry next to Exclude. 3. In the New exclude window, enter the names of one or more groups.
Require the LSP to traverse links that include all of the defined administrative groups.	<ol style="list-style-type: none"> 1. Click Include All next to Admin Group. 2. Click Add new entry next to Include All. 3. In the New include-all window, enter the names of one or more groups.
Define the administrative groups to include for an LSP or for a path's primary and secondary paths.	<ol style="list-style-type: none"> 1. Click Include Any next to Admin Group. 2. Click Add new entry next to Include Any. 3. In the New include-any window, enter the names of one or more groups.

Configuring Automatic Bandwidth Allocation for LSPs (NSM Procedure)

Automatic bandwidth allocation allows an MPLS tunnel to automatically adjust its bandwidth allocation based on the volume of traffic flowing through the tunnel. You can configure an LSP with minimal bandwidth, and this feature can dynamically adjust the LSP's bandwidth allocation based on current traffic patterns.

To configure automatic bandwidth allocation in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > MPLS**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in [Table 146 on page 295](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 146: Automatic Bandwidth Configuration Details

Task	Your Action
Configure automatic bandwidth.	<ol style="list-style-type: none"> 1. Click Add new entry next to Label Switched Path. 2. Click Auto Bandwidth next to label-switched-path. 3. Select the Enable Feature check box to enable the option. 4. In the Comment box, enter the comment. 5. From the Adjust Interval list, select the bandwidth reallocation interval, in seconds. Range: 300 through 4,294,967,295 seconds Default: 86,400 seconds 6. From the Adjust Threshold list, select the threshold for automatic bandwidth adjustment. 7. In the Minimum Bandwidth box, enter the minimum bandwidth in bits per second (bps) for an LSP with automatic bandwidth allocation enabled. 8. In the Maximum Bandwidth box, enter the maximum amount of bandwidth in bits per second (bps). 9. Select the Monitor Bandwidth check box to configure passive bandwidth utilization monitoring. 10. From the Adjust Threshold Overflow Limit list, select the number of consecutive bandwidth overflow samples. Range: 1 through 65,535

Configuring Bandwidth for the Reroute Path (NSM Procedure)

When configuring fast reroute, allocate bandwidth for the reroute path. By default, no bandwidth is reserved for the rerouted path. The fast reroute bandwidth does not need to be identical to that allocated for the LSP itself.

To configure bandwidth for the reroute path in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in [Table 147 on page 296](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 147: Bandwidth Configuration Details

Task	Your Action
Allocate bandwidth for the reroute path.	<ol style="list-style-type: none"> 1. Click Add new entry next to Label Switched Path. 2. Click Bandwidth next to label-switched-path. 3. In the Comment box, enter the comment. 4. In the Per Traffic Class Bandwidth box, enter the bandwidth, in bits per second. 5. In the Ct0 box, enter the bandwidth, for the specified class. 6. In the Ct1 box, enter the bandwidth, for the specified class. 7. In the Ct2 box, enter the bandwidth, for the specified class. 8. In the Ct3 box, enter the bandwidth, for the specified class.

Configuring Fast Reroute (NSM Procedure)

Fast reroute provides a mechanism for automatically rerouting traffic on an LSP if a node or link in an LSP fails, thus reducing the loss of packets traveling over the LSP.

To configure fast reroute in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in [Table 148 on page 296](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 148: Fast Reroute Configuration Details

Task	Your Action
Configure fast reroute.	<ol style="list-style-type: none"> 1. Click Fast Reroute next to Label Switched Path. 2. Select the Enable Feature check box to enable the option. 3. In the Comment box, enter the comment. 4. From the Hop Limit list, select the maximum number of hops. Range: 2 through 255 (for an LSP); 0 through 255 (for fast reroute) Default: 255 (for an LSP); 6 (for fast reroute)

Table 148: Fast Reroute Configuration Details (*continued*)

Task	Your Action
Allocate bandwidth for the reroute path.	<ol style="list-style-type: none"> Click Bandwidth next to Fast Reroute. Select one of the following: <ul style="list-style-type: none"> bandwidth—specify the traffic rate associated with the LSP and enter the bandwidth. bandwidth-percent—configure the percentage of bandwidth to reserve for the detour path in case the primary path for a traffic engineered LSP or a multiclass LSP fails and select the bandwidth percentage.
Control exclusion of administrative groups.	<ol style="list-style-type: none"> Select one of the following: <ul style="list-style-type: none"> exclude—Define the administrative groups to exclude for fast reroute. <ol style="list-style-type: none"> Click Add new entry next to exclude. In the New exclude window, enter the names of one or more groups. no-exclude—Disable administrative group exclusion.
Control inclusion of administrative groups.	<ol style="list-style-type: none"> Select one of the following: <ul style="list-style-type: none"> include-all—Define the administrative groups that must all be included for fast reroute. <ol style="list-style-type: none"> Click Add new entry next to include-all. In the New include-all window, enter the names of one or more groups. no-include-all—Disable administrative group inclusion.
Control inclusion of administrative groups.	<ol style="list-style-type: none"> Select one of the following: <ul style="list-style-type: none"> include-any—Define the administrative groups to include for fast reroute. <ol style="list-style-type: none"> Click Add new entry next to include-any. In the New include-any window, enter the names of one or more groups. no-include-any—Disable administrative group inclusion.

Adding LSP-Related Routes to the inet.3 Routing Table (NSM Procedure)

By default, a host route toward the egress router is installed in the inet.3 routing table. Installing the host route allows BGP to perform next-hop resolution. It also prevents the host route from interfering with prefixes learned from dynamic routing protocols and stored in the inet.0 routing table.

To add additional routes into the inet.3 routing table in NSM:

- In the NSM navigation tree, select **Device Manager > Devices**.
- Click the **Device Tree** tab, and then double-click the device to select it.
- Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
- Select **Label Switched Path**.

5. Add or modify settings as specified in [Table 149 on page 298](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 149: Install Configuration Details

Task	Your Action
Associate one or more prefixes with an LSP.	<ol style="list-style-type: none"> 1. Click Add new entry next to Label Switched Path. 2. Click Install next to label-switched-path. 3. Click Add new entry next to Install. 4. In the Name box, enter the routing table. 5. In the Comment box, enter the comment. 6. Select the Active check box to install the route into the inet.0 routing table. This allows you to issue a ping or traceroute command on this address.

Configuring MPLS LSPs for GMPLS (NSM Procedure)

To enable the proper GMPLS switching parameters you can use the Lsp Attributes option.

To configure the LSP attributes in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in [Table 150 on page 299](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 150: Lsp Attributes Configuration Details

Task	Your Action
Define the parameters signaled during LSP setup.	<ol style="list-style-type: none"> 1. Click Add new entry next to Label Switched Path. 2. Click Lsp Attributes next to label-switched-path. 3. In the Comment box, enter the comment. 4. From the Signal Bandwidth list, select the type of bandwidth encoding used on the LSP. The options available for selection are 10gigether, ds1, ds3, e1, e3, ethernet, fastether, gigether, stm-1, stm-4, stm-16, stm-64, stm-256, sts-1, vt1-5, or vt2. 5. From the Switching Type list, select the switching method for the LSP. Select one of the following: <ul style="list-style-type: none"> • fiber—Fiber switching • lambda—Lambda switching • psc-1—Packet switching • tdm—Time-division multiplexing (TDM) switching 6. From the Encoding Type list, select the encoding type of payload carried by the LSP. Select one of the following: <ul style="list-style-type: none"> • ethernet—Ethernet • packet—Packet • pdh—Plesiochronous digital hierarchy (PDH) • sonet-sdh—SONET/SDH 7. From the Gpid list, select the type of payload carried by the LSP. Select one of the following: <ul style="list-style-type: none"> • ethernet—Ethernet (GPID value: 33) • hdlc—High-level Data Link Control (HDLC) (GPID value: 44) • ipv4—IP version 4 (GPID value: 0x0800) • pos-no-scrambling-crc-16—for interoperability with other vendors' equipment (GPID value: 29) • pos-no-scrambling-crc-32—for interoperability with other vendors' equipment (GPID value: 30) • pos-scrambling-crc-16—for interoperability with other vendors' equipment (GPID value: 31) • pos-scrambling-crc-32—for interoperability with other vendors' equipment (GPID value: 32) • ppp—Point-to-Point Protocol (PPP) (GPID value: 50)

Configuring BFD for MPLS IPv4 LSPs (NSM Procedure)

You can configure BFD for LSPs that use either LDP or RSVP as the signaling protocol using the Oam option.

To configure BFD for LSPs in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.

5. Add or modify settings as specified in [Table 151 on page 300](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 151: Oam Configuration Details

Task	Your Action
Enable OAM for RSVP-signaled LSPs.	<ol style="list-style-type: none"> 1. Click Add new entry next to Label Switched Path. 2. Click Oam next to label-switched-path. 3. In the Comment box, enter the comment. 4. From the Lsp Ping Interval list, select the duration of the LSP ping interval in seconds. Range: 30 through 3,600 seconds
Enable Bidirectional Forwarding Detection (BFD) for all of the MPLS LSPs or for just a specific LSP.	<ol style="list-style-type: none"> 1. Click Bfd Liveness Detection next to Oam. 2. In the Comment box, enter the comment. 3. From the Version list, select the BFD version to be used for detection. 4. From the Minimum Interval list, select the minimum transmit and receive interval. Range: 1 through 255,000 milliseconds 5. From the Minimum Receive Interval list, select the minimum receive interval. Range: 1 through 255,000 milliseconds 6. From the Multiplier list, select the detection time multiplier. Range: 1 through 255 Default: 3 7. Select the No Adaptation check box to disable BFD adaptation.
Specify the threshold for the adaptation of the detection time.	<ol style="list-style-type: none"> 1. Click Detection Time next to Bfd Liveness Detection. 2. In the Comment box, enter the comment. 3. From the Threshold list, select the threshold for detecting the adaptation of the transmit interval.
Configure route and next-hop properties in the event of a BFD protocol session failure event on an RSVP label-switched path.	<ol style="list-style-type: none"> 1. Click Failure Action next to Bfd Liveness Detection. 2. In the Comment box, enter the comment. 3. Click Teardown next to Failure Action. 4. Select one of the following: <ul style="list-style-type: none"> • teardown—when a BFD session fails for an RSVP LSP, the associated LSP path is taken down and resigaled immediately. • make-before-break—when a BFD session fails for an RSVP LSP, an attempt is made to signal a new LSP path before tearing down the old LSP path. <ol style="list-style-type: none"> a. In the Comment box, enter the comment. b. From the Teardown Timeout list, select the time in seconds.

Table 151: Oam Configuration Details (*continued*)

Task	Your Action
Specify the minimum transmit interval for failure detection.	<ol style="list-style-type: none"> 1. Click Transmit Interval next to Failure Action Detection. 2. In the Comment box, enter the comment. 3. From the Minimum Interval list, select the minimum interval at which the local router transmits hello packets to the neighbor with which it has established a BFD session. 4. From the Threshold list, select the threshold for detecting the adaptation of the transmit interval. Range: 0 to 4,294,967,295
Configure MPLS tracing options.	<ol style="list-style-type: none"> 1. Click Traceoptions next to Oam. 2. In the Comment box, enter the comment. 3. Select the No Remote Trace check box to disable remote tracing globally or for a specific tracing operation. 4. Click File next to Traceoptions. 5. In the Filename box, enter the name of the file to receive the output of the tracing operation. 6. In the Size box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). 7. From the Files list, select the maximum number of trace files. Range: 2 through 1000 8. Select one of the following: <ul style="list-style-type: none"> • world-readable—To enable unrestricted file access. • no-world-readable—To restrict file access to owner. 9. In the Match box, enter the regular expression. 10. Click Flag next to Traceoptions. 11. Click Add new entry next to Flag 12. From the Name list, select the flag. 13. In the Comment box, enter the comment.

Configuring the Primary Point-to-Multipoint LSP (NSM Procedure)

A point-to-multipoint LSP must have a configured primary point-to-multipoint LSP to carry traffic from the ingress router. The configuration of the primary point-to-multipoint LSP is similar to a signaled LSP. You can specify an LSP as either a point-to-multipoint LSP or as a branch LSP of a point-to-multipoint LSP by specifying the point-to-multipoint LSP path name.

To configure the primary Point-to-Multipoint LSP in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in [Table 152 on page 302](#).
6. Click one:

- OK—Saves the changes.
- Cancel—Cancels the modifications.

Table 152: Point-to-Multipoint Configuration Details

Task	Your Action
Configure the primary Point-to-Multipoint LSP.	<ol style="list-style-type: none"> 1. Click Add new entry next to Label Switched Path. 2. Click P2mp next to label-switched-path. 3. Select the Enable Feature check box to enable the option. 4. In the Comment box, enter the comment. 5. In the Path_name box, enter the name of the point-to-multipoint LSP path that identifies the sequence of nodes that form the point-to-multipoint LSP.

Configuring Policers for LSPs (NSM Procedure)

MPLS LSP policing allows you to control the amount of traffic forwarded through a particular LSP. Policing helps to ensure that the amount of traffic forwarded through an LSP never exceeds the requested bandwidth allocation. LSP policing is supported on regular LSPs, LSPs configured with DiffServ-aware traffic engineering, and multiclass LSPs. You can configure multiple policers for each multiclass LSP. For regular LSPs, each LSP policer is applied to all of the traffic traversing the LSP. The policer's bandwidth limitations become effective as soon as the total sum of traffic traversing the LSP exceeds the configured limit.

To configure policers for LSPs in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in [Table 153 on page 302](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 153: Policer Configuration Details

Task	Your Action
Specify the policing filter for the LSP.	<ol style="list-style-type: none"> 1. Click Add new entry next to Label Switched Path. 2. Click Policing next to label-switched-path. 3. In the Comment box, enter the comment. 4. From the Filter list, select the name of the policing filter. 5. Select the No Auto Policing check box to disable automatic policing on this LSP.

Configuring Primary Paths for an LSP (NSM Procedure)

- [Configuring Primary Paths for an LSP \(NSM Procedure\) on page 303](#)
- [Configuring Administrative Group \(NSM Procedure\) on page 304](#)
- [Configuring Class-Type Bandwidth Constraints for Multiclass LSPs \(NSM Procedure\) on page 305](#)
- [Configuring BFD for MPLS IPv4 LSPs \(NSM Procedure\) on page 306](#)

Configuring Primary Paths for an LSP (NSM Procedure)

You can specify the primary path to use for an LSP using the Primary option. You can configure only one primary path. You can optionally specify preference, CoS, and bandwidth values for the primary path, which override any equivalent values that you configure for the LSP.

To configure primary paths for an LSP in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in [Table 154 on page 303](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 154: Primary Paths Configuration Details

Task	Your Action
Configure the primary paths for an LSP.	<ol style="list-style-type: none"> 1. Click Add new entry next to Label Switched Path. 2. Click Primary next to label-switched-path. 3. Click Add new entry next to Primary. 4. In the Name box, enter the name of a path. 5. In the Comment box, enter the comment. 6. From the Class Of Service list, select the CoS value. Range: 0 through 7. Default: If you do not specify a CoS value, the IP precedence bits from the packet's IP header are used as the packet's CoS value. 7. Select the No Decrement Ttl check box to disable normal time-to-live (TTL) decrementing. 8. From the Hop Limit list, select the maximum number of hops. Range: 2 through 255 (for an LSP); 0 through 255 (for fast reroute) 9. Select the No Cspf check box to disable constrained-path LSP computation.

Table 154: Primary Paths Configuration Details (*continued*)

Task	Your Action
	<ol style="list-style-type: none"> 10. Select the Admin Down check box to set the A-bit in the Admin Status object. 11. From the Optimize Timer list, select the length of the optimize timer, in seconds. Range: 0 through 65,535 seconds Default: 0 seconds (the optimize timer is disabled) 12. From the Preference list, select the preference to assign to the route. Range: 0 to 4,294,967,295 Default: 5 for static MPLS LSPs, 7 for RSVP MPLS LSPs, 9 for LDP MPLS LSPs 13. From the Setup Priority list, select the setup priority. Range: 0 through 7, where 0 is the highest and 7 is the lowest priority.
	<ol style="list-style-type: none"> 14. From the Reservation Priority list, select the reservation priority. Range: 0 through 7, where 0 is the highest and 7 is the lowest priority. 15. Select one of the following: <ul style="list-style-type: none"> • record—Record routes • no-record—Does not record routes 16. Select the Standby check box to have the path remain up at all times to provide instant switchover if connectivity problems occur. 17. Select the Adaptive check box for RSVP to use shared explicit (SE) reservation styles and assists in smooth transition during rerouting. 18. From the Select list, select the conditions under which the path is selected to carry traffic. Select one the following: <ul style="list-style-type: none"> • manual—The path is selected for carrying traffic if it is up and stable for at least the revert timer window (potentially before the revert timer has elapsed). Traffic is sent to other working paths if the current path is down or degraded (receiving errors). • unconditional—The path is always selected for carrying traffic, even if it is currently down or degraded (receiving errors).

Configuring Administrative Group (NSM Procedure)

You can configure an administrative group constraint for each LSP or for each primary or secondary LSP path using the Admin Group option.

To configure administrative group in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Group**.

5. Add or modify settings as specified in [Table 155 on page 305](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 155: Administrative Group Configuration Details

Task	Your Action
Configure administrative group.	<ol style="list-style-type: none"> 1. Click Add new entry next to Label Switched Path. 2. Click Primary next to label-switched-path. 3. Click Add new entry next to Primary. 4. Click Admin Group next to Primary. 5. In the Comment box, enter the comment.
Define the administrative groups to exclude for an LSP or for a path's primary and secondary paths.	<ol style="list-style-type: none"> 1. Click Exclude next to Admin Group. 2. Click Add new entry next to Exclude. 3. In the New exclude window, enter the names of one or more groups.
Require the LSP to traverse links that include all of the defined administrative groups.	<ol style="list-style-type: none"> 1. Click Include All next to Admin Group. 2. Click Add new entry next to Include All. 3. In the New include-all window, enter the names of one or more groups.
Define the administrative groups to include for an LSP or for a path's primary and secondary paths.	<ol style="list-style-type: none"> 1. Click Include Any next to Admin Group. 2. Click Add new entry next to Include Any. 3. In the New include-any window, enter the names of one or more groups.

Configuring Class-Type Bandwidth Constraints for Multiclass LSPs (NSM Procedure)

You configure a multiclass LSP by using the Bandwidth option.

To configure bandwidth for the multiclass LSP in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in [Table 156 on page 306](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 156: Bandwidth Configuration Details

Task	Your Action
Configure an LSP as a multiclass LSP.	<ol style="list-style-type: none"> 1. Click Add new entry next to Label Switched Path. 2. Click Primary next to label-switched-path. 3. Click Add new entry next to primary. 4. Click Bandwidth next to Primary. 5. In the Comment box, enter the comment. 6. In the Per Traffic Class Bandwidth box, enter the bandwidth, in bits per second. 7. In the Ct0 box, enter the bandwidth, for the specified class. 8. In the Ct1 box, enter the bandwidth, for the specified class. 9. In the Ct2 box, enter the bandwidth, for the specified class. 10. In the Ct3 box, enter the bandwidth, for the specified class.

Configuring BFD for MPLS IPv4 LSPs (NSM Procedure)

You can configure BFD for LSPs that use either LDP or RSVP as the signaling protocol using the Oam option.

To configure BFD for LSPs in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in [Table 157 on page 306](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 157: Oam Configuration Details

Task	Your Action
Enable OAM for RSVP-signaled LSPs.	<ol style="list-style-type: none"> 1. Click Add new entry next to Label Switched Path. 2. Click Primary next to label-switched-path. 3. Click Add new entry next to Primary. 4. Click Oam next to primary. 5. In the Comment box, enter the comment. 6. From the Lsp Ping Interval list, select the duration of the LSP ping interval in seconds.

Table 157: Oam Configuration Details (*continued*)

Task	Your Action
Enable Bidirectional Forwarding Detection (BFD) for all of the MPLS LSPs or for just a specific LSP.	<ol style="list-style-type: none"> 1. Click Bfd Liveness Detection next to Oam. 2. In the Comment box, enter the comment. 3. From the Version list, select the BFD version to be used for detection. 4. From the Minimum Interval list, select the minimum transmit and receive interval. Range: 1 through 255,000 milliseconds 5. From the Minimum Receive Interval list, select the minimum receive interval. Range: 1 through 255,000 milliseconds 6. From the Multiplier list, select the detection time multiplier. Range: 1 through 255 Default: 3 7. Select the No Adaptation check box to disable BFD adaptation.
Specify the threshold for the adaptation of the detection time.	<ol style="list-style-type: none"> 1. Click Detection Time next to Bfd Liveness Detection. 2. In the Comment box, enter the comment. 3. From the Threshold list, select the threshold for detecting the adaptation of the transmit interval.
Configure route and next-hop properties in the event of a BFD protocol session failure event on an RSVP label-switched path.	<ol style="list-style-type: none"> 1. Click Failure Action next to Bfd Liveness Detection. 2. In the Comment box, enter the comment. 3. Click Teardown next to Failure Action. 4. Select one of the following: <ul style="list-style-type: none"> • teardown—when a BFD session fails for an RSVP LSP, the associated LSP path is taken down and resigaled immediately. • make-before-break—when a BFD session fails for an RSVP LSP, an attempt is made to signal a new LSP path before tearing down the old LSP path. <ol style="list-style-type: none"> a. In the Comment box, enter the comment. b. From the Teardown Timeout list, select the time in seconds.
Specify the minimum transmit interval for failure detection.	<ol style="list-style-type: none"> 1. Click Transmit Interval next to Failure Action. 2. In the Comment box, enter the comment. 3. From the Minimum Interval list, select the minimum interval at which the local router transmits hello packets to the neighbor with which it has established a BFD session. Range: 1 through 255,000 milliseconds 4. From the Threshold list, select the threshold for detecting the adaptation of the transmit interval. Range: 0 through 4,294,967,295 milliseconds

Table 157: Oam Configuration Details (*continued*)

Task	Your Action
Configure MPLS tracing options.	<ol style="list-style-type: none"> 1. Click Traceoptions next to Oam. 2. In the Comment box, enter the comment. 3. Select the No Remote Trace check box to disable remote tracing globally or for a specific tracing operation. 4. Click File next to Traceoptions. 5. In the Filename box, enter the name of the file to receive the output of the tracing operation. 6. In the Size box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). 7. From the Files list, select the maximum number of trace files. Range: 2 through 1000 8. Select one of the following: <ul style="list-style-type: none"> • world-readable—To enable unrestricted file access. • no-world-readable—To restrict file access to owner. 9. In the Match box, enter the regular expression. 10. Click Flag next to Traceoptions. 11. Click Add new entry next to Flag 12. From the Name list, select the flag. 13. In the Comment box, enter the comment.

Configuring Secondary Paths for an LSP (NSM Procedure)

- [Configuring Secondary Paths for an LSP \(NSM Procedure\) on page 308](#)
- [Configuring Administrative Group \(NSM Procedure\) on page 310](#)
- [Configuring Class-Type Bandwidth Constraints for Multiclass LSPs \(NSM Procedure\) on page 311](#)
- [Configuring BFD for MPLS IPv4 LSPs \(NSM Procedure\) on page 312](#)
- [Configuring the Egress Router Address for LSPs \(NSM Procedure\) on page 314](#)
- [Tracing LSP Packets and Operations \(NSM Procedure\) on page 315](#)

Configuring Secondary Paths for an LSP (NSM Procedure)

You can specify one or more secondary paths to use for the LSP. You can configure more than one secondary path. All secondary paths are equal, and the first one that is available is chosen. You can specify secondary paths even if you have not specified any primary paths. Optionally, you can specify preference, CoS, and bandwidth values for the secondary path, which override any equivalent values that you configure for the LSP.

To configure secondary paths for an LSP in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.

5. Add or modify settings as specified in [Table 158 on page 309](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 158: Secondary Paths Configuration Details

Task	Your Action
Configure the secondary paths for an LSP.	<ol style="list-style-type: none"> 1. Click Add new entry next to Label Switched Path. 2. Click Secondary next to label-switched-path. 3. Click Add new entry next to Secondary. 4. In the Name box, enter the name of a path. 5. In the Comment box, enter the comment. 6. From the Class Of Service list, select the CoS value. Range: 0 through 7. Default: If you do not specify a CoS value, the IP precedence bits from the packet's IP header are used as the packet's CoS value. 7. Select the No Decrement Ttl check box to disable normal time-to-live (TTL) decrementing. 8. From the Hop Limit list, select the maximum number of hops. Range: 2 through 255 (for an LSP); 0 through 255 (for fast reroute) Default: 255 (for an LSP); 6 (for fast reroute) 9. Select the No Cspf check box to disable constrained-path LSP computation.

Table 158: Secondary Paths Configuration Details (*continued*)

Task	Your Action
	<ol style="list-style-type: none"> 10. Select the Admin Down check box to set the A-bit in the Admin Status object. 11. From the Optimize Timer list, select the length of the optimize timer, in seconds. Range: 0 through 65,535 seconds Default: 0 seconds (the optimize timer is disabled) 12. From the Preference list, select the preference to assign to the route. Range: 0 to 4,294,967,295 Default: 5 for static MPLS LSPs, 7 for RSVP MPLS LSPs, 9 for LDP MPLS LSPs 13. From the Setup Priority list, select the setup priority. Range: 0 through 7, where 0 is the highest and 7 is the lowest priority. 14. From the Reservation Priority list, select the reservation priority. Range: 0 through 7, where 0 is the highest and 7 is the lowest priority. 15. Select one of the following: <ul style="list-style-type: none"> • record—Record routes • no-record—Does not record routes 16. Select the Standby check box to have the path remain up at all times to provide instant switchover if connectivity problems occur. 17. Select the Adaptive check box for RSVP to use shared explicit (SE) reservation styles and assists in smooth transition during rerouting. 18. From the Select list, select the conditions under which the path is selected to carry traffic. Select one the following: <ul style="list-style-type: none"> • manual—The path is selected for carrying traffic if it is up and stable for at least the revert timer window (potentially before the revert timer has elapsed). Traffic is sent to other working paths if the current path is down or degraded (receiving errors). • unconditional—The path is always selected for carrying traffic, even if it is currently down or degraded (receiving errors).

Configuring Administrative Group (NSM Procedure)

You can configure an administrative group constraint for each LSP or for each primary or secondary LSP path using the Admin Group option.

To configure administrative group in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Group**.

5. Add or modify settings as specified in [Table 159 on page 311](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 159: Administrative Group Configuration Details

Task	Your Action
Configure administrative group.	<ol style="list-style-type: none"> 1. Click Add new entry next to Label Switched Path. 2. Click Secondary next to label-switched-path. 3. Click Add new entry next to Secondary. 4. Click Admin Group next to secondary. 5. In the Comment box, enter the comment.
Define the administrative groups to exclude for an LSP or for a path's secondary paths.	<ol style="list-style-type: none"> 1. Click Exclude next to Admin Group. 2. Click Add new entry next to Exclude. 3. In the New exclude window, enter the names of one or more groups.
Require the LSP to traverse links that include all of the defined administrative groups.	<ol style="list-style-type: none"> 1. Click Include All next to Admin Group. 2. Click Add new entry next to Include All. 3. In the New include-all window, enter the names of one or more groups.
Define the administrative groups to include for an LSP or for a path's primary and secondary paths.	<ol style="list-style-type: none"> 1. Click Include Any next to Admin Group. 2. Click Add new entry next to Include Any. 3. In the New include-any window, enter the names of one or more groups.

Configuring Class-Type Bandwidth Constraints for Multiclass LSPs (NSM Procedure)

You configure a multiclass LSP by using the Bandwidth option.

To configure bandwidth for the multiclass LSP in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in [Table 160 on page 312](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 160: Bandwidth Configuration Details

Task	Your Action
Configure an LSP as a multiclass LSP.	<ol style="list-style-type: none"> 1. Click Add new entry next to Label Switched Path. 2. Click Secondary next to label-switched-path. 3. Click Add new entry next to Secondary. 4. Click Bandwidth next to secondary. 5. In the Comment box, enter the comment. 6. In the Per Traffic Class Bandwidth box, enter the bandwidth, in bits per second. 7. In the Ct0 box, enter the bandwidth, for the specified class. 8. In the Ct1 box, enter the bandwidth, for the specified class. 9. In the Ct2 box, enter the bandwidth, for the specified class. 10. In the Ct3 box, enter the bandwidth, for the specified class.

Configuring BFD for MPLS IPv4 LSPs (NSM Procedure)

You can configure BFD for LSPs that use either LDP or RSVP as the signaling protocol using the Oam option.

To configure BFD for LSPs in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in [Table 161 on page 312](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 161: Oam Configuration Details

Task	Your Action
Enable OAM for RSVP-signaled LSPs.	<ol style="list-style-type: none"> 1. Click Add new entry next to Label Switched Path. 2. Click Secondary next to label-switched-path. 3. Click Add new entry next to Secondary. 4. Click Oam next to secondary. 5. In the Comment box, enter the comment. 6. From the Lsp Ping Interval list, select the duration of the LSP ping interval in seconds.

Table 161: Oam Configuration Details (*continued*)

Task	Your Action
Enable Bidirectional Forwarding Detection (BFD) for all of the MPLS LSPs or for just a specific LSP.	<ol style="list-style-type: none"> 1. Click Bfd Liveness Detection next to Oam. 2. In the Comment box, enter the comment. 3. From the Version list, select the BFD version to be used for detection. 4. From the Minimum Interval list, select the minimum transmit and receive interval. Range: 1 through 255,000 milliseconds 5. From the Minimum Receive Interval list, select the minimum receive interval. Range: 1 through 255,000 milliseconds 6. From the Multiplier list, select the detection time multiplier. Range: 1 through 255 Default: 3 7. Select the No Adaptation check box to disable BFD adaptation.
Specify the threshold for the adaptation of the detection time.	<ol style="list-style-type: none"> 1. Click Detection Time next to Bfd Liveness Detection. 2. In the Comment box, enter the comment. 3. From the Threshold list, select the threshold for detecting the adaptation of the transmit interval.
Configure route and next-hop properties in the event of a BFD protocol session failure event on an RSVP label-switched path.	<ol style="list-style-type: none"> 1. Click Failure Action next to Bfd Liveness Detection. 2. In the Comment box, enter the comment. 3. Click Teardown next to Failure Action. 4. Select one of the following: <ul style="list-style-type: none"> • teardown—when a BFD session fails for an RSVP LSP, the associated LSP path is taken down and resigaled immediately. • make-before-break—when a BFD session fails for an RSVP LSP, an attempt is made to signal a new LSP path before tearing down the old LSP path. <ol style="list-style-type: none"> a. In the Comment box, enter the comment. b. From the Teardown Timeout list, select the time in seconds.
Specify the minimum transmit interval for failure detection.	<ol style="list-style-type: none"> 1. Click Transmit Interval next to Failure Action. 2. In the Comment box, enter the comment. 3. From the Minimum Interval list, select the minimum interval at which the local router transmits hello packets to the neighbor with which it has established a BFD session. 4. From the Threshold list, select the threshold for detecting the adaptation of the transmit interval. Range: 0 to 4,294,967,295

Table 161: Oam Configuration Details (*continued*)

Task	Your Action
Configure LSP tracing options.	<ol style="list-style-type: none"> 1. Click Traceoptions next to Oam. 2. In the Comment box, enter the comment. 3. Select the No Remote Trace check box to disable remote tracing globally or for a specific tracing operation. 4. Click File next to Traceoptions. 5. In the Filename box, enter the name of the file to receive the output of the tracing operation. 6. In the Size box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). 7. From the Files list, select the maximum number of trace files. Range: 2 through 1000 8. Select one of the following: <ul style="list-style-type: none"> • world-readable—To enable unrestricted file access. • no-world-readable—To restrict file access to owner. 9. In the Match box, enter the regular expression. 10. Click Flag next to Traceoptions. 11. Click Add new entry next to Flag 12. From the Name list, select the flag. 13. In the Comment box, enter the comment.

Configuring the Egress Router Address for LSPs (NSM Procedure)

When configuring an LSP, you must specify the address of the egress router by using the To option.

To configure the egress router of a dynamic LSP in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in [Table 162 on page 315](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 162: Egress Router Address Configuration Details

Task	Your Action
Specify the address of the egress router.	<ol style="list-style-type: none"> 1. Click Add new entry next to Label Switched Path. 2. Click To next to label-switched-path. 3. Select one of the following: <ul style="list-style-type: none"> • To—Specify the egress router of a dynamic LSP and enter the address of the egress router. • Template—Configure an LSP template.

Tracing LSP Packets and Operations (NSM Procedure)

You can trace LSP packets and operations using the Traceoptions option.

To trace LSP packets and operations in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in [Table 163 on page 315](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 163: LSP Traceoptions Configuration Details

Task	Your Action
Trace LSP packets and operations.	<ol style="list-style-type: none"> 1. Click Add new entry next to Label Switched Path. 2. Click Traceoptions next to label-switched-path. 3. In the Comment box, enter the comment. 4. Click File next to Traceoptions. 5. In the Comment box, enter the comment. 6. In the Filename box, enter the name of the file to receive the output. 7. In the Size box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). 8. From the Files list, select the maximum number of trace files. Range: 2 through 1000 9. Select one of the following: <ul style="list-style-type: none"> • world-readable—To enable unrestricted file access. • no-world-readable—To restrict file access to owner.

Table 163: LSP Traceoptions Configuration Details (*continued*)

Task	Your Action
Specify the tracing operation to perform.	<ol style="list-style-type: none"> 1. Click Flag next to Traceoptions. 2. Click Add new entry next to Flag. 3. In the Comment box, enter the comment. 4. From the Name list, select the tracing operation to be performed. 5. In the Comment box, enter the comment.

Configuring System Log Messages and SNMP Traps for LSPs (NSM Procedure)

Whenever a label switched paths (LSPs) makes a transition from up to down, or down to up, and whenever an LSP switches from one active path to another, the ingress router generates a system log message and sends an SNMP trap.

To configure system log messages and SNMP traps for LSPs in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Mpls**.
5. Add or modify settings as specified in [Table 164 on page 316](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 164: Log Updown Configuration Details

Task	Your Action
Log a message or send an SNMP trap whenever an LSP makes a transition from up to down, or vice versa.	<ol style="list-style-type: none"> 1. Click Log Updown next to Mpls. 2. In the Comment box, enter the comment. 3. Select one of the following: <ul style="list-style-type: none"> • syslog—To log a message to the system log file. • no-syslog—Does not log a message to the system log file. 4. Select the Trap Path Down check box to generate SNMP traps whenever an LSP path goes down. 5. Select the Trap Path Up check box to generate SNMP traps whenever an LSP path goes up.

Table 164: Log Updown Configuration Details (*continued*)

Task	Your Action
Send an SNMP trap.	<ol style="list-style-type: none"> Click Trap next to Log Updown. Select one of the following: <ul style="list-style-type: none"> trap—To send an SNMP trap. no-trap—Does not send an SNMP trap. <ol style="list-style-type: none"> In the Comment box, enter the comment. Select the Mpls Lsp Traps check box to block the MPLS LSP traps defined in the jnx-mpls.mib but to allow the rfc3812.mib traps. Select the Rfc3812 Traps check box to block the traps defined in the rfc3812.mib but to allow the MPLS LSP traps defined in the jnx-mpls.mib.

Configuring BFD for MPLS IPv4 LSPs (NSM Procedure)

You can configure BFD for label switched paths (LSPs) that use either LDP or RSVP as the signaling protocol using the Oam option.

To configure BFD for LSPs in NSM:

- In the NSM navigation tree, select **Device Manager > Devices**.
- Click the **Device Tree** tab, and then double-click the device to select it.
- Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
- Select **Mpls**.
- Add or modify settings as specified in [Table 165 on page 317](#).
- Click one:
 - OK**—Saves the changes.
 - Cancel**—Cancels the modifications.

Table 165: Oam Configuration Details

Task	Your Action
Enable OAM for RSVP-signaled LSPs.	<ol style="list-style-type: none"> Click Oam next to Mpls. In the Comment box, enter the comment. From the Lsp Ping Interval list, select the duration of the LSP ping interval in seconds.

Table 165: Oam Configuration Details (*continued*)

Task	Your Action
Enable Bidirectional Forwarding Detection (BFD) for all of the MPLS LSPs or for just a specific LSP.	<ol style="list-style-type: none"> 1. Click Bfd Liveness Detection next to Oam. 2. In the Comment box, enter the comment. 3. From the Version list, select the BFD version to be used for detection. 4. From the Minimum Interval list, select the minimum transmit and receive interval. Range: 1 through 255,000 milliseconds 5. From the Minimum Receive Interval list, select the minimum receive interval. Range: 1 through 255,000 milliseconds 6. From the Multiplier list, select the detection time multiplier. Range: 1 through 255 Default: 3 7. Select the No Adaptation check box to disable BFD adaptation.
Specify the threshold for the adaptation of the detection time.	<ol style="list-style-type: none"> 1. Click Detection Time next to Bfd Liveness Detection. 2. In the Comment box, enter the comment. 3. From the Threshold list, select the threshold for detecting the adaptation of the transmit interval.
Configure route and next-hop properties in the event of a BFD protocol session failure event on an RSVP label-switched path.	<ol style="list-style-type: none"> 1. Click Failure Action next to Bfd Liveness Detection. 2. In the Comment box, enter the comment. 3. Click Teardown next to Failure Action. 4. Select one of the following: <ul style="list-style-type: none"> • teardown—when a BFD session fails for an RSVP LSP, the associated LSP path is taken down and resigaled immediately. • make-before-break—when a BFD session fails for an RSVP LSP, an attempt is made to signal a new LSP path before tearing down the old LSP path. <ol style="list-style-type: none"> a. In the Comment box, enter the comment. b. From the Teardown Timeout list, select the time in seconds.
Specify the minimum transmit interval for failure detection.	<ol style="list-style-type: none"> 1. Click Transmit Interval next to Failure Action. 2. In the Comment box, enter the comment. 3. From the Minimum Interval list, select the minimum interval at which the local router transmits hello packets to the neighbor with which it has established a BFD session. Range: 1 to 255,000 milliseconds 4. From the Threshold list, select the threshold for detecting the adaptation of the transmit interval. Range: 0 to 4,294,967,295

Table 165: Oam Configuration Details (*continued*)

Task	Your Action
Configure MPLS tracing options.	<ol style="list-style-type: none"> 1. Click Traceoptions next to Oam. 2. In the Comment box, enter the comment. 3. Select the No Remote Trace check box to disable remote tracing globally or for a specific tracing operation. 4. Click File next to Traceoptions. 5. In the Filename box, enter the name of the file to receive the output of the tracing operation. 6. In the Size box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). 7. From the Files list, select the maximum number of trace files. Range: 2 through 1000 8. Select one of the following: <ul style="list-style-type: none"> • world-readable—To enable unrestricted file access. • no-world-readable—To restrict file access to owner. 9. In the Match box, enter the regular expression. 10. Click Flag next to Traceoptions. 11. Click Add new entry next to Flag 12. From the Name list, select the flag. 13. In the Comment box, enter the comment.

Configuring Named Paths (NSM Procedure)

To configure signaled label switched paths (LSPs), you must first create one or more named paths on the ingress router. For each path, you can specify some or all transit routers in the path, or you can leave it empty. Each pathname can contain up to 32 characters and can include letters, digits, periods, and hyphens. The name must be unique within the ingress router.

To configure named paths in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Mpls**.
5. Add or modify settings as specified in [Table 166 on page 320](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 166: Named Path Configuration Details

Task	Your Action
Create a named path.	<ol style="list-style-type: none"> 1. Click Path next to Mpls. 2. Click Add new entry next to Path. 3. In the Name box, enter the hostname. 4. In the Comment box, enter the comment.
Specify the sequence of explicit routers that form the path.	<ol style="list-style-type: none"> 1. Click Path List next to Path. 2. In the Name box, enter the Name that identifies the sequence of nodes that form an LSP. 3. In the Comment box, enter the comment. 4. Select one of the following: <ul style="list-style-type: none"> • loose—indicate that the next address in the path statement is a loose link. This means that the LSP can traverse through other routers before reaching this router. • strict—indicate that the LSP must go to the next address specified in the path statement without traversing other nodes.

Configuring MTU Signaling in RSVPs (NSM Procedure)

To configure maximum transmission unit (MTU) signaling in RSVP, you need to configure MPLS to allow IP packets to be fragmented before they are encapsulated in MPLS. You also need to configure MTU signaling in RSVP. For troubleshooting purposes, you can configure MTU signaling alone without enabling packet fragmentation.

To configure MTU signaling in RSVP in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Mpls**.
5. Add or modify settings as specified in [Table 167 on page 320](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 167: Path MTU Configuration Details

Task	Your Action
Configure MTU options for MPLS paths, including packet fragmentation and MTU signaling.	<ol style="list-style-type: none"> 1. Click Path Mtu next to Mpls. 2. Select the Enable Feature check box to enable the option. 3. In the Comment box, enter the comment. 4. Select the Allow Fragmentation check box to allow IP packets to be fragmented before they are encapsulated in MPLS.

Table 167: Path MTU Configuration Details (*continued*)

Task	Your Action
Configure MTU signaling in RSVP.	<ol style="list-style-type: none"> 1. Click Rsvp next to Path Mtu. 2. Select the Enable Feature check box to enable the option. 3. In the Comment box, enter the comment. 4. Select the Mtu Signaling check box to enable MTU signaling in RSVP.

Configuring static LSPs on the Ingress Router (NSM Procedure)

You can configure static LSPs on the ingress router using the Static Path option.

To configure static path in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Mpls**.
5. Add or modify settings as specified in [Table 168 on page 321](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 168: Static Path Configuration Details

Task	Your Action
Configure static path.	<ol style="list-style-type: none"> 1. Click Static Path next to Mpls. 2. Click Add new entry next to Static Path. 3. From the Name list, select the routing table. 4. In the Comment box, enter the comment.
Configure static LSPs on the ingress router.	<ol style="list-style-type: none"> 1. Click Path next to static-path. 2. Click Add new entry next to Path. 3. In the Name box, enter the name of the routing table. 4. In the Comment box, enter the comment. 5. In the Next Hop box, enter the IP address of the next hop to the destination.

Table 168: Static Path Configuration Details (*continued*)

Task	Your Action
	6. From the Push list, select the out-label value. Range: 0 through 1,048,575
	7. From the Double Push Bottom list, select the bottom-label value. Range: Labels 0 through 999,999 are for internal use. Labels 1,000,000 through 1,048,575 are unassigned by the Junos OS and are available for static LSPs.
	8. From the Double Push Top list, select the top-label value. Range: Labels 0 through 999,999 are for internal use. Labels 1,000,000 through 1,048,575 are unassigned by the Junos OS and are available for static LSPs.
	9. From the Triple Push Bottom list, select the bottom-label value. Range: 0 through 1,048,575. Labels 0 through 999,999 are for internal use. Labels 1,000,000 through 1,048,575 are unassigned by the Junos OS and are available for static LSPs.
	10. From the Triple Push Middle list, select the middle-label value. Range: 0 through 1,048,575. Labels 0 through 999,999 are for internal use. Labels 1,000,000 through 1,048,575 are unassigned by the Junos OS and are available for static LSPs.
	11. From the Triple Push Top list, select the top-label value. Range: 0 through 1,048,575. Labels 0 through 999,999 are for internal use. Labels 1,000,000 through 1,048,575 are unassigned by the Junos OS and are available for static LSPs.
	12. From the Preference list, select the preference to be assigned to the route.
	13. From the Class Of Service list, select the CoS value. Range: 0 through 7 Default: If you do not specify a CoS value, the IP precedence bits from the packet's IP header are used as the packet's CoS value.

Configuring MPLS Statistics (NSM Procedure)

You can enable MPLS statistics collection and reporting using the Statistics option.

To configure static path in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Mpls**.
5. Add or modify settings as specified in [Table 169 on page 323](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 169: MPLS Statistics Configuration Details

Task	Your Action
Enable MPLS statistics collection and reporting.	<ol style="list-style-type: none"> 1. Click Statistics next to Mpls. 2. In the Comment box, enter the comment. 3. From the Interval list, select the interval at which to periodically collect statistics. Range: 1 through 65,535 Default: none 4. Select the Auto Bandwidth check box to collect statistics related to automatic bandwidth.
Configure the file.	<ol style="list-style-type: none"> 1. Click File next to Statistics. 2. In the Comment box, enter the comment. 3. In the Filename box, enter the name of the file to receive the output. 4. In the Size box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). 5. From the Files list, select the maximum number of trace files. Range: 2 through 1000 6. Select one of the following: <ul style="list-style-type: none"> • world-readable—To enable unrestricted file access. • no-world-readable—To restrict file access to owner.

Tracing MPLS Packets and Operations (NSM Procedure)

You can trace MPLS packets and operations using the Traceoptions option.

To trace MPLS packets and operations in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Mpls**.
5. Add or modify settings as specified in [Table 170 on page 324](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 170: Traceoptions Configuration Details

Task	Your Action
Trace MPLS packets and operations.	<ol style="list-style-type: none"> 1. Click Traceoptions next to Mpls. 2. In the Comment box, enter the comment. 3. Click File next to Traceoptions. 4. In the Comment box, enter the comment. 5. In the Filename box, enter the name of the file to receive the output. 6. In the Size box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). 7. From the Files list, select the maximum number of trace files. Range: 2 through 1000 8. Select one of the following: <ul style="list-style-type: none"> • world-readable—To enable unrestricted file access. • no-world-readable—To restrict file access to owner.
Specify the tracing operation to perform.	<ol style="list-style-type: none"> 1. Click Flag next to Traceoptions. 2. Click Add new entry next to Flag. 3. In the Comment box, enter the comment. 4. From the Name list, select the tracing operation to be performed. 5. In the Comment box, enter the comment.

Configuring MSDP Protocol (NSM Procedure)

The Multicast Source Discovery Protocol (MSDP) is used to connect multicast routing domains. It typically runs on the same router as the Protocol Independent Multicast (PIM) sparse-mode rendezvous point (RP). Each MSDP router establishes adjacencies with internal and external MSDP peers similar to the Border Gateway Protocol (BGP). These peer routers inform each other about active sources within the domain. When they detect active sources, the routers can send PIM sparse-mode explicit join messages to the active source. You can enable MSDP on the router using the MSDP option. See the following topics.

- [Configuring MSDP on the Router \(NSM Procedure\) on page 324](#)
- [Configuring the MSDP Active Source Limit \(NSM Procedure\) on page 325](#)
- [Configuring Export Policy \(NSM Procedure\) on page 326](#)
- [Configuring MSDP Peer Group on page 327](#)

Configuring MSDP on the Router (NSM Procedure)

You can enable multicast source discovery protocol (MSDP) on the router using the MSDP option.

To enable MSDP on the router in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **MSDP**.
5. Add or modify settings as specified in [Table 171 on page 325](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 171: MSDP Configuration Details

Task	Your Action
Enable MSDP on the router.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment. 2. From the Data Encapsulation list, select one of the following: <ul style="list-style-type: none"> • disable—Do not use MSDP data encapsulation. • enable—Use MSDP data encapsulation. 3. Select the Disable check box to disable MSDP. 4. In the Local Address box, enter the IP address of the local end of the connection.

Configuring the MSDP Active Source Limit (NSM Procedure)

A router interested in MSDP messages, such as a rendezvous point (RP), might have to process a large number of MSDP messages, especially source-active messages, arriving from other routers. Because of the potential need for a router to examine, process, and create state tables for many MSDP packets, there is a possibility of an MSDP-based DoS attack on a router running MSDP. To minimize this possibility, you can configure the router to limit the number of source active messages the router accepts. Also, you can configure a threshold for applying random early discard (RED) to drop some but not all MSDP active source messages.

To configure the MSDP active source limit on the router in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Msdp**.
5. Add or modify settings as specified in [Table 172 on page 326](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 172: Active Source Limit Configuration Details

Task	Your Action
Configure active source limit.	<ol style="list-style-type: none"> 1. Click Active Source Limit next to Msdp. 2. In the Comment box, enter the comment. 3. From the Maximum list, select the maximum number of active source messages. Range: 1 through 1,000,000 Default: 25,000 4. From the Threshold list, select the RED threshold for active source messages. Range: 1 through 1,000,000 Default: 24,000

Configuring Export Policy (NSM Procedure)

To apply policies to source-active messages being exported from the source-active cache into MSDP, use the Export option.

To configure export policy in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Msdp**.
5. Add or modify settings as specified in [Table 173 on page 326](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 173: Export Policy Configuration Details

Task	Your Action
Apply one or more policies to routes being exported from the routing table into MSDP.	<ol style="list-style-type: none"> 1. Click Export Policy next to Msdp. 2. Use the following options to select the policies to export. <ul style="list-style-type: none"> • Click Add after selecting a policy member from the Non member list to add it to the Members list. • Click Remove after selecting a policy from the Members list to remove it from the Members list. • Click Add All to add all the Non members to the Members list. • Click Remove All to remove all the members from the Members list.

Configuring MSDP Peer Group

- [Configuring MSDP Peer Group \(NSM Procedure\) on page 327](#)
- [Configuring MSDP Peers \(NSM Procedure\) on page 328](#)
- [Configuring a Routing Table Group with MSDP \(NSM Procedure\) on page 330](#)
- [Configuring Per-Source Active Source Limit \(NSM Procedure\) on page 331](#)
- [Configuring MSDP Traceoptions \(NSM Procedure\) on page 332](#)

Configuring MSDP Peer Group (NSM Procedure)

You can define an MSDP peer group using the Group option.

To configure an MSDP peer group in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Msdp**.
5. Add or modify settings as specified in [Table 174 on page 327](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 174: Peer Group Configuration Details

Task	Your Action
Define an MSDP peer group.	<ol style="list-style-type: none"> 1. Click Group next to Msdp. 2. Click Add new entry next to Group. 3. In the Name box, enter the name of the MSDP group. 4. In the Comment box, enter the comment. 5. From the Mode list, select the mesh groups. 6. Select the Disable check box to disable MSDP. 7. In the Local Address box, enter the IP address of the local end of the connection.
Apply one or more policies to routes being exported from the routing table into MSDP.	<ol style="list-style-type: none"> 1. Click Export next to Group. 2. Use the following options to select the policies to export: <ul style="list-style-type: none"> • Click Add after selecting a policy member from the Non member list to add it to the Members list. • Click Remove after selecting a policy from the Members list to remove it from the Members list. • Click Add All to add all the Non members to the Members list. • Click Remove All to remove all the members from the Members list.

Table 174: Peer Group Configuration Details (*continued*)

Task	Your Action
Apply one or more policies to routes being imported into the routing table from MSDP.	<ol style="list-style-type: none"> 1. Click Import next to Group. 2. Use the following options to select the policies to import: <ul style="list-style-type: none"> • Click Add after selecting a policy member from the Non member list to add it to the Members list. • Click Remove after selecting a policy from the Members list to remove it from the Members list. • Click Add All to add all the Non members to the Members list. • Click Remove All to remove all the members from the Members list.

Configuring MSDP Peers (NSM Procedure)

An MSDP router must know which routers are its peers. You define the peer relationships explicitly by configuring the neighboring routers that are the MSDP peers of the local router. After peer relationships are established, the MSDP peers exchange messages to advertise active multicast sources. You must configure at least one peer for MSDP to function.

To configure MSDP peers in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Msdp**.
5. Add or modify settings as specified in [Table 175 on page 329](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 175: MSDP Peer Configuration Details

Task	Your Action
Configure MSDP peers.	<ol style="list-style-type: none"> 1. Click Group next to Msdp. 2. Click Add new entry next to Group. 3. Click Peer next to group. 4. Click Add new entry next to Peer. 5. In the Name box, enter the name of the MSDP group. 6. In the Comment box, enter the comment. 7. From the Mode list, select the mesh groups. 8. Select the Disable check box to disable MSDP. 9. In the Local Address box, enter the IP address of the local end of the connection. 10. Select the Default Peer check box to establish this peer as the default MSDP peer and accept source-active messages from the peer without the usual peer-reverse-path-forwarding (peer-RPF) check. 11. In the Authentication Key box, enter the MD5 authentication key.
Configure active source limit.	<ol style="list-style-type: none"> 1. Click Active Source Limit next to Peer. 2. In the Comment box, enter the comment. 3. From the Maximum list, select the maximum number of active source messages. Range: 1 through 1,000,000 Default: 25,000 4. From the Threshold list, select the RED threshold for active source messages. Range: 1 through 1,000,000 Default: 24,000
Apply one or more policies to routes being exported from the routing table into MSDP.	<ol style="list-style-type: none"> 1. Click Export next to Peer. 2. Use the following options to select the policies to export: <ul style="list-style-type: none"> • Click Add after selecting a policy member from the Non member list to add it to the Members list. • Click Remove after selecting a policy from the Members list to remove it from the Members list. • Click Add All to add all the Non members to the Members list. • Click Remove All to remove all the members from the Members list.

Table 175: MSDP Peer Configuration Details (*continued*)

Task	Your Action
Apply one or more policies to routes being imported into the routing table from MSDP.	<ol style="list-style-type: none"> 1. Click Import next to Peer. 2. Use the following options to select the policies to import: <ul style="list-style-type: none"> • Click Add after selecting a policy member from the Non member list to add it to the Members list. • Click Remove after selecting a policy from the Members list to remove it from the Members list. • Click Add All to add all the Non members to the Members list. • Click Remove All to remove all the members from the Members list.
Configure MSDP tracing options.	<ol style="list-style-type: none"> 1. Click Traceoptions next to Peer. 2. In the Comment box, enter the comment for the traceoptions. 3. Click File next to Traceoptions. 4. In the Comment box, enter the comment for the filename. 5. In the Filename box, enter the name of the file to receive the output of the tracing operation. 6. In the Size box, enter the maximum trace file size. 7. From the Files list, select the maximum number of trace files. 8. Select one of the following: <ul style="list-style-type: none"> • no-world-readable—To restrict the file access to owner. • world-readable—To enable unrestricted access. 9. Click Flag next to Traceoptions. 10. Click Add new entry next to Flag. 11. From the Name list, select the flag to perform the trace operation. 12. In the Comment box, enter the comment for the flag. 13. Select the corresponding modifier for the tracing flag.

Configuring a Routing Table Group with MSDP (NSM Procedure)

To associate with MSDP a routing table group that imports and exports routes into the specified routing table group, you can use the Rib Group option.

To associate a routing table group with MSDP in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Msdp**.
5. Add or modify settings as specified in [Table 176 on page 331](#).
6. Click one:
 - **OK**—Saves the changes.

- **Cancel**—Cancels the modifications.

Table 176: Rib Group Configuration Details

Task	Your Action
Associate a routing table group with MSDP.	<ol style="list-style-type: none"> 1. Click Rib Group next to Msdp. 2. In the Comment box, enter the comment. 3. In the Ribgroup Name box, enter the name of the routing table group.

Configuring Per-Source Active Source Limit (NSM Procedure)

You can configure an active source limit for an address range as well as for a specific peer. A per-source active source limit uses an IP prefix and prefix length instead of a specific address. You can configure more than one per-source active source limit. The longest match determines the limit.

To configure an active source limit for an address range as well as for a specific peer in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Msdp**.
5. Add or modify settings as specified in [Table 177 on page 331](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 177: Active Source Limit Configuration Details

Task	Your Action
Configure an active source limit for an address range as well as for a specific peer.	<ol style="list-style-type: none"> 1. Click Source next to Msdp. 2. Click Add new entry next to Source. 3. In the Name box, enter the IP address. 4. In the Comment box, enter the comment.
Configure active source limit.	<ol style="list-style-type: none"> 1. Click Active Source Limit next to source. 2. In the Comment box, enter the comment. 3. From the Maximum list, select the maximum number of active source messages. Range: 1 through 1,000,000 Default: 25,000 4. From the Threshold list, select the RED threshold for active source messages. Range: 1 through 1,000,000 Default: 24,000

Configuring MSDP Traceoptions (NSM Procedure)

You can configure the MSDP traceoption using the Traceoption option.

To configure traceoptions in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Msdp**.
5. Add or modify settings as specified in [Table 178 on page 332](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 178: MSDP Traceoption Configuration Details

Task	Your Action
Configure traceoptions.	<ol style="list-style-type: none"> 1. Click Traceoptions next to Msdp. 2. In the Comment box, enter the comment for the traceoptions. 3. Click File next to Traceoptions. 4. In the Comment box, enter the comment for the filename. 5. In the Filename box, enter the name of the file to receive the output of the tracing operation. 6. In the Size box, enter the maximum trace file size. 7. From the Files list, select the maximum number of trace files. 8. Select one of the following: <ul style="list-style-type: none"> • no-world-readable—To restrict the file access to owner. • world-readable—To enable unrestricted access. 9. Click Flag next to Traceoptions. 10. Click Add new entry next to Flag. 11. From the Name list, select the flag to perform the trace operation. 12. In the Comment box, enter the comment for the flag. 13. Select the corresponding modifier for the tracing flag.

Configuring MSTP (NSM Procedure)

Multiple Spanning Tree Protocol (MSTP) is used to create a loop-free topology in networks using multiple spanning tree regions, each region containing multiple spanning-tree instances (MSTIs). MSTIs provide different paths for different VLANs. This functionality facilitates better load sharing across redundant links.

MSTP supports up to 64 regions, each one capable of supporting 4094 MSTIs.

To configure MSTP:

1. In the navigation tree, select **Device Manager > Devices**. In Device Manager, select the device for which you want to configure a port mirror analyzer.
2. In the Configuration tree, expand **Protocols > MSTP**.
3. Add/modify MSTP settings as specified in [Table 179 on page 333](#).



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See [Updating Devices](#) for more information.

Table 179: MSTP Configuration Fields

Option	Function	Your Action
Disable	Specifies whether MSTP must be disabled on the port.	Click to select the option.
Configuration Name	Specifies the configuration name.	Type a name.
Revision Level	Specifies the configuration revision level.	Select a value.
Max Hops	Specifies the number of hops in a region before the BPDU is discarded.	Select a value.
Max Age	Specifies the maximum-aging time for all MST instances. The maximum aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.	Select a value.
Hello time	Specifies the hello time for all MST instances.	Select a value.
Forward Delay	Specifies the number of seconds a port waits before changing from its spanning-tree learning and listening states to the forwarding state.	Select a value.
Bridge Priority	Specifies the bridge priority.	Enter a value.
Bpdu Block on Edge	Specifies whether Bpdu blocks must be processed.	Select to enable the feature.

Table 179: MSTP Configuration Fields (*continued*)

Option	Function	Your Action
Interface	Specifies MSTP settings for the interface.	<ol style="list-style-type: none"> 1. Click the expand icon. 2. Specify the interface name. 3. Specify the port priority. 4. Specify the path cost. MSTP uses the path cost when selecting an interface to place into the forwarding state. A lower path cost represents higher-speed transmission. 5. Specify the mode. The link type can be shared or point-to-point. 6. Select Edge to enable the feature. 7. Select No root port if it is not specified. 8. Click OK. 9. Specify the Bpdu timeout action: <ul style="list-style-type: none"> • Block • Alarm
Msti	Specifies MST instances settings for an interface or VLAN.	<ol style="list-style-type: none"> 1. Specify the Msti ID. 2. Enter a comment. 3. Specify the bridge priority. 4. Click OK.

Configuring OSPF (NSM Procedure)

OSPF uses the shortest path first (SPF) algorithm to determine the route to reach each destination. All devices in an area run this algorithm in parallel, storing the results in their individual topological databases. Devices with interfaces to multiple areas run multiple copies of the algorithm.

To configure OSPF in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Protocols** and select **OSPF**.
5. Add/Modify the parameters under the respective tabs as specified in [Table 180 on page 335](#).
6. Click one:
 - **OK**—To save the changes.

- Cancel—To cancel the modifications.
- Apply — To apply the protocol settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See [Updating Devices](#) for more information.

Table 180: OSPF Configuration Fields

Option	Function	Your Action
OSPF		

Table 180: OSPF Configuration Fields (*continued*)

Option	Function	Your Action
Comment	Specifies the comment for OSPF.	1. Enter the comment.
Disable	Specifies whether to disable the OSPF configuration.	1. Specify whether to enable or disable OSPF. <ul style="list-style-type: none"> To enable OSPF, clear the check box. To disable OSPF, select the check box.
Prefix Export Limit	Configure a limit to the number of prefixes to be exported.	1. Enter the prefix export limit or select from the list.
Rib Group	Specifies the routing table group.	1. Select rib group from the list.
Route Type Community	Specifies an extended community value to encode the OSPF route type	1. Select route type community from the list.
Domain VPN Tag	Virtual private network (VPN) tag for OSPFv2 external routes generated by the provider edge (PE) router.	1. Enter the domain VPN tag or select from the list.
Preference	Specifies the route preference for OSPF internal routes.	1. Enter the preference or select from the list.
External Preference	Specifies the external route preference.	1. Enter the external route preference or select from the list.
Reference Bandwidth	Specifies the reference bandwidth used in calculating the default interface cost.	1. Enter the reference bandwidth.
No RFC 1583	Disable compatibility with RFC 1583. Disabling compatibility with RFC 1583 can prevent routing loops.	1. Specify whether to configure RFC 1583. <ul style="list-style-type: none"> To enable compatibility with RFC 1583, clear the check box. To disable compatibility with RFC 1583, select the check box.
No NSSA ABR	Disable compatibility with NSSA ABR.	1. Specify whether NSSA ABR has to be configured. <ul style="list-style-type: none"> To enable NSSA ABR, clear the check box. To disable NSSA ABR, select the check the check box.
Area	Enables you to set up the area details for OSPF.	1. Expand the OSPF tree and select Area . 2. Set up the area range, interface, sham link remote, stub and virtual link.

Table 180: OSPF Configuration Fields (*continued*)

Option	Function	Your Action
Domain ID	Enables you to configure domain ID for the OSPF.	<ol style="list-style-type: none"> 1. Expand the OSPF tree and select Domain ID. 2. Specify the domain ID.
Export	Enables you to specify the export policies to be configured on the peer.	<ol style="list-style-type: none"> 1. Expand the OSPF tree and select Export. 2. Specify the export policies.
Graceful Restart	Enables you to specify the graceful restart parameters for OSPF.	<ol style="list-style-type: none"> 1. Expand the OSPF tree and select Graceful Restart. 2. Set up the graceful restart parameters.
Import	Enables you to specify the import policies to be configured on the peer.	<ol style="list-style-type: none"> 1. Expand the OSPF tree and select Import. 2. Specify the import policies.
Overload	Enables you to configure the local router so that it appears to be overloaded. You might do this when you want the router to participate in OSPF routing, but do not want it to be used for transit traffic.	<ol style="list-style-type: none"> 1. Expand the OSPF tree and select Overload. 2. Specify the comment and timeout.
Sham Link	Enables you to configure the local endpoint of a sham link.	<ol style="list-style-type: none"> 1. Expand the OSPF tree and select Sham Link. 2. Enable the feature and specify the comment and local address.
SPF Options	Enables you to configure options for running the shortest-path-first (SPF) algorithm. You can configure a delay for when to run the SPF algorithm after a network topology change is detected, the maximum number of times the SPF algorithm can run in succession, and a holddown interval after the SPF algorithm runs the maximum number of times.	<ol style="list-style-type: none"> 1. Expand the OSPF tree and select SPF Options. 2. Specify the comment, delay, holddown and rapid runs.
Traceoptions	Enables you to configure OSPF protocol level tracing options.	<ol style="list-style-type: none"> 1. Expand the OSPF tree and select Traceoptions. 2. Expand the Traceoptions tree and set up the file and flag parameters.

Configuring RIP (NSM Procedure)

Routing Information Protocol (RIP) is an interior gateway protocol (IGP) typically used in small, homogeneous networks. RIP uses distance-vector routing to route information through IP networks. Distance-vector routing requires that each device simply informs its neighbors of its routing table. For each network path, the receiving device picks the neighbor advertising the lowest metric, then adds this entry into its routing table for readvertisement. Any host that uses RIP is assumed to have interfaces to one or more networks. These networks are considered to be directly connected networks. RIP relies on access to certain information about each of these networks. The most important information is the network's metric. RIP uses the hop count as the metric (also known as cost) to compare the value of different routes. The hop count is the number of devices that data packets must traverse between RIP networks.

To configure RIP in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Protocols** and select **Rip**.
5. Add/Modify the parameters under the respective tabs as specified in [Table 181 on page 338](#).
6. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply — To apply the protocol settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See [Updating Devices](#) for more information.

Table 181: RIP Configuration Fields

Option	Function	Your Action
RIP		

Table 181: RIP Configuration Fields (*continued*)

Option	Function	Your Action
Comment	Specifies the comment for RIP.	1. Enter the comment.
Metric In	Specifies the metric to add to incoming routes when advertising into RIP routes that were learned from other protocols.	1. Specify the metric to add incoming routes.
Message Size	Specifies the number of route entries to be included in every RIP update message.	1. Enter the message size or select from the list.
Hold Down	Time period the expired route is retained in the routing table before being removed.	1. Enter the hold down value or select from the list.
Route Timeout	Specifies the route timeout interval for RIP.	1. Enter the route timeout or select from the list.
Update Interval	Enables you to configure an update time interval to periodically send out routes learned by RIP to neighbors.	1. Enter the update interval or select from the list.
Authentication Type	The type of authentication for RIP route queries received on an interface.	1. Select authentication type from the list.
Authentication Key	Authentication key for RIP route queries received on an interface.	1. Enter the authentication key.
Graceful Restart	Enables you to specify the graceful restart parameters for RIP.	1. Expand the RIP tree and select Graceful Restart . 2. Enable the feature and set up the graceful restart parameters.
Group	RIP neighbors that share an export policy and metric. The export policy and metric govern what routes to advertise to neighbors in a given group.	1. Expand the RIP tree and select Group . 2. Click the New button or select a group and click Edit button. 3. Set up the Bfd Liveness Detection , Export, Import and Neighbor for RIP.
Import	Enables you to specify the import policies to be configured on the peer.	1. Expand the RIP tree and select Import . 2. Specify the import policies.
Receive	Enables you to configure RIP receive options.	1. Expand the RIP tree and select Receive . 2. Specify the receive options.

Table 181: RIP Configuration Fields (*continued*)

Option	Function	Your Action
RIB Group	The routing table group.	<ol style="list-style-type: none"> 1. Expand the RIP tree and select Rib Group. 2. Specify the comment and ribgroup name.
Send	Enables you to configure RIP send options.	<ol style="list-style-type: none"> 1. Expand the RIP tree and select Send. 2. Specify the send options.
Traceoptions	Enables you to configure RIP protocol level tracing options.	<ol style="list-style-type: none"> 1. Expand the RIP tree and select Traceoptions. 2. Expand the Traceoptions tree and set up the file and flag parameters.

Configuring RIPng Protocol (NSM Procedure)

To have a router exchange routes with other routers, you must configure RIP next generation (RIPng) groups and neighbors. RIPng routes received from routers not configured as RIPng neighbors are ignored. Likewise, RIPng routes are advertised only to routers configured as RIPng neighbors. See the following topics:

- [Configuring RIPng on the Router \(NSM Procedure\) on page 340](#)
- [Configuring Graceful Restart for RIPng \(NSM Procedure\) on page 341](#)
- [Configuring Group on page 342](#)
- [Enable or Disable Receiving of Update Messages \(NSM Procedure\) on page 348](#)
- [Configuring RIPng Send Update Messages \(NSM Procedure\) on page 348](#)
- [Configuring RIPng Traceoptions \(NSM Procedure\) on page 349](#)

Configuring RIPng on the Router (NSM Procedure)

To configure RIPng in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Ripng**.
5. Add or modify settings as specified in [Table 182 on page 341](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 182: RIPng Configuration Details

Task	Your Action
Configure RIPng.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment. 2. From the Metric In list, select the metric value. Range: 1 through 15 Default: 1 3. From the Holddown list, select the estimated time to wait before making updates to the routing table. Range: 10 through 180 seconds Default: 180 seconds 4. From the Route Timeout list, select the estimated time to wait before making updates to the routing table. Range: 30 through 360 seconds Default: 180 seconds 5. From the Update Interval list, select the estimated time to wait before making updates to the routing table. Range: 10 through 60 seconds Default: 30 seconds

Configuring Graceful Restart for RIPng (NSM Procedure)

You can configure graceful restart parameters specifically for RIPng using the Graceful Restart option.

To configure graceful restart for RIPng in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Ripng**.
5. Add or modify settings as specified in [Table 183 on page 342](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 183: Graceful Restart Configuration Details

Task	Your Action
Configure graceful restart.	<ol style="list-style-type: none"> 1. Click Graceful Restart next to Ripng. 2. Select the Enable Feature check box to enable this option. 3. In the Comment box, enter the comment. 4. Select the Disable check box to disable the graceful restart. 5. From the Restart Time list, select the estimated time period for the restart to finish. Range: 1 through 600 seconds Default: 60 seconds

Configuring Group

- [Configuring Group-Specific RIPng Properties \(NSM Procedure\) on page 342](#)
- [Applying Policies to Routes Exported by RIPng \(NSM Procedure\) on page 344](#)
- [Applying Policies to Routes Imported by RIPng \(NSM Procedure\) on page 344](#)
- [Configuring RIPng Neighbor Properties on page 345](#)

Configuring Group-Specific RIPng Properties (NSM Procedure)

You can group together neighbors that share the same export policy and export metric defaults. You configure group-specific RIPng properties by using the Group option.

To configure group specific properties for RIPng in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Ripng**.
5. Add or modify settings as specified in [Table 184 on page 343](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 184: Group Configuration Details

Task	Your Action
Configuring group specific properties.	<ol style="list-style-type: none"> 1. Click Group next to Ripng. 2. Click Add new entry next to Group. 3. In the Name box, enter the name of the group. 4. In the Comment box, enter the comment. 5. From the Route Timeout list, select the estimated time to wait before making updates to the routing table. Range: 30 through 360 seconds Default: 180 seconds 6. From the Update Interval list, select the estimated time to wait before making updates to the routing table. Range: 10 through 60 seconds Default: 30 seconds 7. From the Preference list, select the preference value. A lower value indicates a more preferred route. Range: 0 through 4,294,967,295 ($2^{32} - 1$) Default: 100 8. From the Metric Out list, select the metric value. Range: 1 through 15 Default: 1
Apply a policy or list of policies to routes being exported to the neighbors.	<ol style="list-style-type: none"> 1. Click Export next to Group. 2. Use the following options to select the policies to export: <ul style="list-style-type: none"> • Click Add after selecting a policy member from the Non member list to add it to the Members list. • Click Remove after selecting a policy from the Members list to remove it from the Members list. • Click Add All to add all the Non members to the Members list. • Click Remove All to remove all the members from the Members list.
Apply one or more policies to routes being imported into the local routing device from the neighbors.	<ol style="list-style-type: none"> 1. Click Import next to Group. 2. Use the following options to select the policies to import: <ul style="list-style-type: none"> • Click Add after selecting a policy member from the Non member list to add it to the Members list. • Click Remove after selecting a policy from the Members list to remove it from the Members list. • Click Add All to add all the Non members to the Members list. • Click Remove All to remove all the members from the Members list.

Applying Policies to Routes Exported by RIPng (NSM Procedure)

By default, RIPng does not export routes it has learned to its neighbors. To have RIPng export routes, apply one or more export policies. To apply export policies and to filter routes being exported from the local routing device to its neighbors use the Export option.

To apply for export policies for RIPng in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Ripng**.
5. Add or modify settings as specified in [Table 185 on page 344](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 185: RIPng Export Policy Configuration Details

Task	Your Action
Apply a policy or list of policies to routes being exported to the neighbors.	<ol style="list-style-type: none"> 1. Click Export next to Group. 2. Use the following options to select the policies to export: <ul style="list-style-type: none"> • Click Add after selecting a policy member from the Non member list to add it to the Members list. • Click Remove after selecting a policy from the Members list to remove it from the Members list. • Click Add All to add all the Non members to the Members list. • Click Remove All to remove all the members from the Members list.

Applying Policies to Routes Imported by RIPng (NSM Procedure)

To filter routes being imported by the local routing device from its neighbors, use the Import option and list the names of one or more policies to be evaluated. If you specify more than one policy, they are evaluated in order (first to last) and the first matching policy is applied to the route. If no match is found, the local routing device does not import any routes.

To apply export policies for RIPng in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Ripng**.

5. Add or modify settings as specified in [Table 186 on page 345](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 186: Import Policy Configuration Details

Task	Your Action
Apply one or more policies to routes being imported into the local routing device from the neighbors.	<ol style="list-style-type: none"> 1. Click Import next to Group. 2. Use the following options to select the policies to import: <ul style="list-style-type: none"> • Click Add after selecting a policy member from the Non member list to add it to the Members list. • Click Remove after selecting a policy from the Members list to remove it from the Members list. • Click Add All to add all the Non members to the Members list. • Click Remove All to remove all the members from the Members list.

Configuring RIPng Neighbor Properties

- [Configuring RIPng Neighbor Properties \(NSM Procedure\) on page 345](#)
- [Applying Policies to RIPng Routes Imported from Neighbors \(NSM Procedure\) on page 346](#)
- [Configuring RIPng Update Messages \(NSM Procedure\) on page 347](#)
- [Enable or Disable Sending of Update Messages \(NSM Procedure\) on page 347](#)

Configuring RIPng Neighbor Properties (NSM Procedure)

To define neighbor-specific properties use the Neighbor option.

To configure neighbor specific parameters for RIPng in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Ripng**.
5. Add or modify settings as specified in [Table 187 on page 346](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 187: Neighbor Properties Configuration Details

Task	Your Action
Define neighbor-specific properties.	<ol style="list-style-type: none"> 1. Click Neighbor next to Group. 2. In the Name box, enter the name of an interface over which a routing device communicates to its neighbors. 3. In the Comment box, enter the comment. 4. From the Route Timeout list, select the estimated time to wait before making updates to the routing table. 5. From the Update Interval list, select the estimated time to wait before making updates to the routing table. 6. From the Metric In list, select the metric value.

Applying Policies to RIPng Routes Imported from Neighbors (NSM Procedure)

To filter routes being imported by the local routing device from its neighbors, use the Import option and list the names of one or more policies to be evaluated. If you specify more than one policy, they are evaluated in order (first to last) and the first matching policy is applied to the route. If no match is found, the local routing device does not import any routes.

To configure neighbor specific parameters for RIPng in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Ripng**.
5. Add or modify settings as specified in [Table 188 on page 346](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 188: Import Policy Configuration Details

Task	Your Action
Apply one or more policies to routes being imported into the local routing device from the neighbors.	<ol style="list-style-type: none"> 1. Click Import Policy next to Neighbor. 2. Use the following options to select the policies to import: <ul style="list-style-type: none"> • Click Add after selecting a policy member from the Non member list to add it to the Members list. • Click Remove after selecting a policy from the Members list to remove it from the Members list. • Click Add All to add all the Non members to the Members list. • Click Remove All to remove all the members from the Members list.

Configuring RIPv6 Update Messages (NSM Procedure)

You can enable and disable the receiving of update messages. By default, receiving update messages is enabled.

To enable or disable the receiving update messages in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Ripng**.
5. Add or modify settings as specified in [Table 189 on page 347](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 189: Receive Message Update Configuration Details

Task	Your Action
Enable or disable the receiving update messages.	<ol style="list-style-type: none"> 1. Click Receive next to Neighbor. 2. In the Comment box, enter the comment. 3. Select the None check box to disable receiving update messages.

Enable or Disable Sending of Update Messages (NSM Procedure)

You can enable and disable the sending of update messages. By default, sending update messages is enabled.

To enable or disable the sending update messages in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Ripng**.
5. Add or modify settings as specified in [Table 190 on page 348](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 190: Send Update Message Configuration Details

Task	Your Action
Enable or disable the sending update messages.	<ol style="list-style-type: none"> 1. Click Send next to Neighbor. 2. In the Comment box, enter the comment. 3. Select the None check box to disable sending update messages.

Enable or Disable Receiving of Update Messages (NSM Procedure)

You can enable and disable the receiving of update messages. By default, receiving update messages is enabled.

To enable or disable the receiving update messages in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Ripng**.
5. Add or modify settings as specified in [Table 191 on page 348](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 191: Receive Message Update Configuration Details

Task	Your Action
Enable or disable the receiving update messages.	<ol style="list-style-type: none"> 1. Click Receive next to Ripng. 2. In the Comment box, enter the comment. 3. Select the None check box to disable receiving update messages.

Configuring RIPng Send Update Messages (NSM Procedure)

You can enable and disable the sending of update messages. By default, sending update messages is enabled.

To enable or disable the sending update messages in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Ripng**.
5. Add or modify settings as specified in [Table 192 on page 349](#).
6. Click one:

- OK—Saves the changes.
- Cancel—Cancels the modifications.

Table 192: RIPng Send Configuration Details

Task	Your Action
Enable or disable the sending update messages.	<ol style="list-style-type: none"> 1. Click Send next to Ripng. 2. In the Comment box, enter the comment. 3. Select the None check box to disable sending update messages.

Configuring RIPng Traceoptions (NSM Procedure)

You can configure the RIPng traceoption using the Traceoption option.

To configure traceoptions in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Ripng**.
5. Add or modify settings as specified in [Table 193 on page 350](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 193: RIPng Traceoption Configuration Details

Task	Your Action
Configure traceoptions.	<ol style="list-style-type: none"> 1. Click Traceoptions next to Ripng. 2. In the Comment box, enter the comment for the traceoptions. 3. Click File next to Traceoptions. 4. In the Comment box, enter the comment for the filename. 5. In the Filename box, enter the name of the file to receive the output of the tracing operation. 6. In the Size box, enter the maximum trace file size. 7. From the Files list, select the maximum number of trace files. 8. Select one of the following: <ul style="list-style-type: none"> • none—To skip the option. • no-world-readable—To restrict the file access to owner. • world-readable—To enable unrestricted access. 9. Click Flag next to Traceoptions. 10. Click Add new entry next to Flag. 11. From the Name list, select the flag to perform the trace operation. 12. In the Comment box, enter the comment for the flag. 13. Select the corresponding modifier for the tracing flag.

Configuring Router Advertisement (NSM Procedure)

You can configure neighbor discovery router advertisement using the Router Advertisement option.

To configure router advertisement in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Router Advertisement**.
5. Add or modify settings as specified in [Table 194 on page 351](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 194: Router Advertisement Configuration Details

Task	Your Action
Configure router advertisement properties on an interface.	<ol style="list-style-type: none"> 1. Click Interface next to Router Advertisement. 2. Click Add new entry next to Interface. 3. In the Name box, enter the name of an interface. 4. In the Comment box, enter the comment. 5. From the Max Advertisement Interval list, select the maximum interval between each router advertisement message. Range: 4 through 1800 seconds Default: 600 seconds 6. From the Min Advertisement Interval list, select the minimum interval between each router advertisement message. Range: 3 seconds through three-quarter times the maximum advertisement interval value Default: One-third the maximum advertisement interval value 7. Select one of the following: <ul style="list-style-type: none"> • None—To skip the option. • managed-configuration—Enable host to use stateful autoconfiguration. • no-managed-configuration—Disable host from using stateful autoconfiguration. 8. Select one of the following: <ul style="list-style-type: none"> • None—To skip the option. • other-stateful-configuration—Enable autoconfiguration of other nonaddress-related information. • no-other-stateful-configuration—Disable autoconfiguration of other nonaddress-related information. 9. From the Reachable Time list, select the length of time that a node considers a neighbor reachable until another reachability confirmation is received from that neighbor. Range: 0 through 3,600,000 milliseconds Default: 0 milliseconds 10. From the Retransmit Timer list, select the retransmission frequency of neighbor solicitation messages. Range: 0 through 4,294,967,295 milliseconds Default: 0 milliseconds 11. Select the Virtual Router Only check box to specify a virtual router. 12. From the Current Hop Limit list, select the hop limit. Range: 0 through 255 Default: 6 13. From the Default Lifetime list, select the default lifetime. Range: Maximum advertisement interval value through 9000 seconds Default: Three times the maximum advertisement interval value

Table 194: Router Advertisement Configuration Details (*continued*)

Task	Your Action
Configure prefix properties in router advertisement messages.	<ol style="list-style-type: none"> 1. Click Prefix next to interface. 2. In the Name box, enter the prefix name. 3. In the Comment box, enter the comment. 4. From the Valid Lifetime list, select the valid lifetime. Range: 0 through 4,294,967,295 seconds Default: 2,592,000 seconds 5. Select one of the following: <ul style="list-style-type: none"> • None—To skip the option. • on-link—Enable prefixes to be used for onlink determination. • no-on-link—Disable prefixes from being used for onlink determination. 6. From the Preferred Lifetime list, select how long the prefix generated by stateless autoconfiguration remains preferred. Range: 0 through 4,294,967,295 Default: 604,800 seconds 7. Select one of the following: <ul style="list-style-type: none"> • None—To skip the option. • autonomous—Use prefixes for address autoconfiguration. • no-autonomous—Do not use prefixes for address autoconfiguration.
Specify router advertisement protocol-level tracing options.	<ol style="list-style-type: none"> 1. Click Traceoptions next to Router Advertisement. 2. In the Comment box, enter the comment for the traceoptions. 3. Click File next to Traceoptions. 4. In the Comment box, enter the comment for the filename. 5. In the Filename box, enter the name of the file to receive the output of the tracing operation. 6. In the Size box, enter the maximum trace file size. 7. From the Files list, select the maximum number of trace files. 8. Select one of the following: <ul style="list-style-type: none"> • None—To skip the option. • no-world-readable—To restrict the file access to owner. • world-readable—To enable unrestricted access. 9. Click Flag next to Traceoptions. 10. Click Add new entry next to Flag. 11. From the Name list, select the flag to perform the trace operation. 12. In the Comment box, enter the comment for the flag.

Configuring ICMP Router Discovery (NSM Procedure)

To configure a router as a server for Internet Control Message Protocol (ICMP) router discovery, use the Router Discovery option.

To configure router discovery in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Router Discovery**.
5. Add or modify settings as specified in [Table 195 on page 353](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 195: Router Discovery Configuration Details

Task	Your Action
Configure router discovery.	<ol style="list-style-type: none"> 1. Click Router Discovery next to Protocols. 2. In the Comment box, enter the comment. 3. Select the Disable check box to disable router discovery.
Configure IP addresses to include in router advertisement packets.	<ol style="list-style-type: none"> 1. Click Address next to Router Discovery. 2. In the Name box, enter the IP address. 3. In the Comment box, enter the comment. 4. Select the Advertise check box to advertise the IP address in its router advertisement packets. 5. Select the Ignore check box to not advertise the IP addresses in router advertisement packets. 6. Select the Broadcast check box to include some addresses in broadcast packets. 7. Select the Multicast check box to include some addresses in multicast packets. 8. Select the Ineligible check box to prevent the address from becoming the default router. 9. From the Priority list, select the preference of the addresses for becoming the default router. Range: 0 through 0x80000000 Default: 0 (This address has the least chance of becoming the default router.)

Table 195: Router Discovery Configuration Details (*continued*)

Task	Your Action
Configure physical interfaces.	<ol style="list-style-type: none"> 1. Click Interface next to Router Discovery. 2. In the Name box, enter the name of the interface. 3. In the Comment box, enter the comment. 4. In the Name box, enter the name of an interface. 5. In the Comment box, enter the comment. 6. From the Max Advertisement Interval list, select the maximum interval between each router advertisement message. Range: 4 through 1800 seconds Default: 600 seconds 7. From the Min Advertisement Interval list, select the minimum interval between each router advertisement message. Range: 3 seconds through 1800 seconds Default: 400 seconds 8. From the Lifetime list, select the lifetime value.
Specify tracing options.	<ol style="list-style-type: none"> 1. Click Traceoptions next to Router Discovery. 2. In the Comment box, enter the comment for the traceoptions. 3. Click File next to Traceoptions. 4. In the Comment box, enter the comment for the filename. 5. In the Filename box, enter the name of the file to receive the output of the tracing operation. 6. In the Size box, enter the maximum trace file size. 7. From the Files list, select the maximum number of trace files. 8. Select one of the following: <ul style="list-style-type: none"> • no-world-readable—To restrict the file access to owner. • world-readable—To enable unrestricted access. 9. Click Flag next to Traceoptions. 10. Click Add new entry next to Flag. 11. From the Name list, select the flag to perform the trace operation. 12. In the Comment box, enter the comment for the flag. 13. Select the corresponding modifier for the tracing flag.

Configuring VRRP (NSM Procedure)

Virtual Router Redundancy Protocol (VRRP) prevents loss of network connectivity to end hosts if the static default IP gateway fails. By implementing VRRP, you can designate a number of routers as backup routers in the event that the default master router fails. VRRP fully supports Virtual Local Area Networks (VLANs) and stacked VLANs (S-VLANs). In case of a failure, VRRP dynamically shifts the packet-forwarding responsibility to a backup router. VRRP creates a redundancy scheme which enables hosts to keep a single IP address for the default gateway but maps the IP address to a well-known virtual MAC address. VRRP provides this redundancy without user intervention or additional configuration at the end hosts.

To configure VRRP in NSM:

1. In the navigation tree select **Device Manager > Devices** and select the device from the list.
2. In the configuration tree, expand **Protocols**.
3. Select **VRRP**.
4. Add/Modify the parameters under the respective tabs as specified in [Table 196 on page 355](#).
5. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply — To apply the protocol settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See [Updating Devices](#) for more information.

Table 196: VRRP Configuration Fields

Field	Function	Your Action
VRRP		
Comment	Specifies comment for VRRP.	<ol style="list-style-type: none">1. Expand the Protocol tree and select VRRP.2. Enter the comment.

Table 196: VRRP Configuration Fields (*continued*)

Field	Function	Your Action
Startup Silent Period	Enables the system to ignore the Master Down Event when an interface transitions from the disabled state to the enabled state. It avoids an incorrect error alarm caused by delay or interruption of incoming VRRP advertisement packets during the interface startup phase.	<ol style="list-style-type: none"> 1. Expand the Protocol tree and select VRRP. 2. Enter the startup silent period or select from the list
Traceoptions	Enables you to configure VRRP level tracing options.	<ol style="list-style-type: none"> 1. Expand the Protocol tree. 2. Select VRRP and expand the tree. 3. Select Traceoptions. 4. Set up the file and flag parameters.

Configuring VSTP (NSM Procedure)

VLAN Spanning Tree Protocol (VSTP) is a spanning tree protocol which creates a loop-free topology in VLANs. VSTP maintains a separate spanning tree instance for each VLAN. Different VLANs can use different spanning tree paths and VSTP can support up to 4094 different spanning tree topologies.

To configure VSTP in NSM:

1. In the navigation tree select **Device Manager > Devices** and select the device from the list.
2. In the configuration tree, expand **Protocols**.
3. Select **VSTP**.
4. Add/Modify the parameters under the respective tabs as specified in [Table 197 on page 357](#).
5. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply — To apply the protocol settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See [Updating Devices](#) for more information.

Table 197: VSTP Configuration Fields

Field	Function	Your Action
VSTP		
Comment	Specifies comment for OSPF.	<ol style="list-style-type: none"> 1. Expand the Protocol tree and select VSTP. 2. Enter the comment.
Disable	Specifies whether to disable the VSTP configuration.	<ol style="list-style-type: none"> 1. Expand the Protocol tree and select VSTP. 2. Specify whether to disable VSTP.
Bridge Priority	The bridge priority determines which bridge is elected as the root bridge. If two bridges have the same path cost to the root bridge, the bridge priority determines which bridge becomes the designated bridge for a LAN segment.	<ol style="list-style-type: none"> 1. Expand the Protocol tree and select VSTP. 2. Enter the bridge priority.
Max Age	Specifies the maximum age of received protocol BPDUs.	<ol style="list-style-type: none"> 1. Expand the Protocol tree and select VSTP. 2. Enter the max age or select from the list.
Hello Time	The time interval at which the root bridge transmits configuration BPDUs.	<ol style="list-style-type: none"> 1. Expand the Protocol tree and select VSTP. 2. Enter the hello time or select from the list.
Forward Delay	Specifies how long a bridge interface remains in the listening and learning states before transitioning to the forwarding state.	<ol style="list-style-type: none"> 1. Expand the Protocol tree and select VSTP. 2. Enter the forward delay time or select from the list.
Interface	Specifies the interface to be associated with VSTP.	<ol style="list-style-type: none"> 1. Expand the Protocol tree. 2. Select VSTP and expand the tree. 3. Select Interfaces. 4. Set up the priority, cost, mode, edge and specify whether the interface has to be disabled.
Traceoptions	Enables you to configure VSTP level tracing options.	<ol style="list-style-type: none"> 1. Expand the Protocol tree. 2. Select VSTP and expand the tree. 3. Select Traceoptions. 4. Set up the file and flag parameters.

Configuring RSVP (NSM Procedure)

To configure the Resource Reservation Protocol (RSVP) in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand **Protocols**.
4. Select **RSVP**.
5. Add or modify settings as specified in [Table 198 on page 358](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 198: RSVP Configuration Details

Task	Your Action
Configure RSVP.	<ol style="list-style-type: none"> 1. Expand RSVP. 2. In the Comment box, enter the comment. 3. Select the Disable check box to explicitly disable RSVP or RSVP graceful restart. 4. Select the No-P2mp-Sublsp check box to reject Resv messages which include the S2L_SUB_LSP object. 5. From the Refresh Time list, select the refresh time. Range: 1 through 255 Default: 3 6. From the Keep Multiplier list, select the keep multiplier value. Range: 1 through 65,535 Default: 30 seconds 7. From the Graceful Deletion-Timeout list, select the time before completing graceful deletion of signaling. Range: 1 through 300 seconds Default: 30 seconds
Configure the optimization interval for fast reroute paths.	<ol style="list-style-type: none"> 1. Expand RSVP. 2. Click Fast Reroute next to RSVP. 3. In the Comment box, enter the comment for the fast reroute. 4. From the Optimize Timer list, select the number of seconds between fast reroute detour Label-Switched Paths (LSP). Range: 0 through 65,535 seconds Default: 0 (disabled)

Table 198: RSVP Configuration Details (*continued*)

Task	Your Action
Configure RSVP graceful restart.	<ol style="list-style-type: none"> 1. Expand RSVP. 2. In the Comment box, enter the comment for the filename. 3. Select the Disable check box to explicitly disable RSVP or RSVP graceful restart. 4. Select the Helper Disable check box to Disable RSVP graceful restart helper mode. 5. From the Maximum Helper Restart Time list, select the maximum length of time the router waits between when it discovers that a neighboring router has gone down and when it declares the neighbor down. Range: 1 through 1800 seconds Default: 20 seconds 6. From the Maximum Helper Recovery Time list, select the maximum length of time the router stores the state of neighboring routers when they undergo a graceful restart. Range: 1 through 3600 seconds Default: 0 (disabled)
Enable RSVP on one or more router interfaces.	<ol style="list-style-type: none"> 1. Click Interface next to Rsvp. 2. Click Add new entry next to Interface. 3. In the Name box, enter the name of the interface. 4. In the Comment box, enter the comment. 5. Select Disable check box to explicitly disable RSVP or RSVP graceful restart. 6. In the Authentication Key box, enter the authentication key (password). 7. Select one of the following: <ul style="list-style-type: none"> • aggregate—To use RSVP aggregate messages. • no-aggregate—To not to use RSVP aggregate messages. 8. Select one of the following: <ul style="list-style-type: none"> • reliable—To enable reliable message delivery on the interface. • no-reliable—To disable reliable message delivery on the interface. 9. From the hello Interval list, select the length of time between hello packets. A value of 0 disables the sending of hello packets on the interface. Range: 1 through 60 seconds Default: 9 seconds 10. In the Bandwidth box, enter the bandwidth in bits per second. 11. From the Update Threshold list, select the percentage change in bandwidth to trigger an Interior Gateway Protocol (IGP) update. Range: 1 through 60 seconds Default: 9 seconds

Table 198: RSVP Configuration Details (*continued*)

Task	Your Action
Configuring link protection on interfaces.	<ol style="list-style-type: none"> 1. Click Link Protection next to interface. 2. In the Comment box, enter the comment. 3. Select the Disable check box to explicitly disable link protection on the specified interface. 4. From the Max Bypasses list, select the maximum number of bypass LSPs. If you configure a value of 0, no dynamic bypass LSPs are allowed to be established for the interface. Range: 1 through 99 Default: 1 5. From the Subscription list, select the percent of the class-type or bypass LSP bandwidth that RSVP allows to be used for reservations. If you specify a value greater than 100, you are oversubscribing the class type or bypass LSP. Range: 0 through 65,000 Default: 100 percent 6. Select No Node Protection to disable node protection 7. From the Class of Service list, select the CoS value. Range: 0 through 7 Default: If you do not specify a Class of Service (CoS) value, the IP precedence bits from the packet's IP header are used as the packet's CoS value. 8. From the Hop Limit list, select the maximum number of hops a bypass can traverse. Range: 2 through 255 hops Default: 255 hops 9. Select the No Cspf check box to disable CSPF computation on all bypass LSPs or on a specific bypass LSP. You need to disable Constraint Shortest Path First (CSPF) for link protection to function properly on interarea paths. 10. From the Setup Priority list, select the setup priority. Range: 0 through 7, where 0 is the highest and 7 is the lowest priority Default: 7 (The session cannot preempt any existing sessions.) 11. From the Reservation Priority list, select the reservation priority. Range: 0 through 7, where 0 is the highest and 7 is the lowest priority. Default: 0 (Once the session is set up, no other session can preempt it.)

Table 198: RSVP Configuration Details (*continued*)

Task	Your Action
Configure administrative groups for bypass LSPs.	<ol style="list-style-type: none"> 1. Click Admin Group next to Link Protection. 2. Click Exclude next to Admin Group. 3. Click Add new entry next to Exclude. 4. In the New exclude window, enter the administrative groups to exclude for a bypass LSP. 5. Click Include All next to Admin Group. 6. Click Add new entry next to Include All. 7. In the New include-all window, enter the administrative groups whose links the bypass LSP must traverse. 8. Click Include Any next to Admin Group. 9. Click Add new entry next to Include Any. 10. In the New include-any window, enter the administrative groups whose links the bypass LSP can traverse.
Configuring the bandwidth for bypass LSPs.	<ol style="list-style-type: none"> 1. Click Bandwidth next to Link Protection. 2. In the Per Traffic Class Bandwidth box, enter the bandwidth. 3. In the class-type number box, enter the class-type bandwidth.
Configure a bypass LSP	<ol style="list-style-type: none"> 1. Click Bypass next to Link Protection. 2. Click Add new entry next to Bypass. 3. Click Admin Group next to Bypass. 4. Click Exclude next to Admin Group. 5. Click Add new entry next to Exclude. 6. In the New exclude window, enter the administrative groups to exclude for a bypass LSP. 7. Click Include All next to Admin Group. 8. Click Add new entry next to Include All. 9. In the New include-all window, enter the administrative groups whose links the bypass LSP must traverse. 10. Click Include Any next to Admin Group. 11. Click Add new entry next to Include Any. 12. In the New include-any window, enter the administrative groups whose links the bypass LSP can traverse. 13. Click Bandwidth next to Link Protection. 14. In the Per Traffic Class Bandwidth box, enter the bandwidth. 15. In the class-type number box, enter the class-type bandwidth. 16. Click Path next to Bypass. 17. Click Add new entry next to Path. 18. In the Name box, enter the IP address of each transit router in the LSP. 19. Select one of the following: <ul style="list-style-type: none"> • loose—If the LSP can traverse other routers before reaching this router. • strict—If the LSP must go to the next address specified in the path statement without traversing other nodes.

Table 198: RSVP Configuration Details (*continued*)

Task	Your Action
Configuring an explicit path for bypass LSPs.	<ol style="list-style-type: none"> 1. Click Path next to Link Protection. 2. Click Add new entry next to Path. 3. In the Name box, enter the IP address of each transit router in the LSP. 4. In the Comment box, enter the comment. 5. Select one of the following: <ul style="list-style-type: none"> • loose—If the LSP can traverse other routers before reaching this router. • strict—If the LSP must go to the next address specified in the path statement without traversing other nodes.
Configuring the bandwidth subscription percentage for LSPs.	<ol style="list-style-type: none"> 1. Click Subscription next to interface. 2. In the Link Subscription box, enter the class-type bandwidth that RSVP allows to be used for reservations. 3. In the class-type number percentage box, enter the percent of class-type bandwidth. You can specify bandwidth subscriptions for class types 0 through 3.
Configuring load balancing across RSVP LSPs.	<ol style="list-style-type: none"> 1. Click Load Balance next to Rsvp. 2. In the Comment box, enter the comment. 3. Select the Bandwidth check box to load-balance traffic between RSVP LSPs based on the bandwidth configured for each LSP.
Configuring RSVP for LMP peer interfaces.	<ol style="list-style-type: none"> 1. Click Peer Interface next to Rsvp. 2. Click Add new entry next to Peer Interface. 3. In the Name box, enter the peer interface name. 4. In the Comment box, enter the comment. 5. Select Disable check box Explicitly disable RSVP or RSVP graceful restart. 6. In the Authentication Key box, enter the authentication key (password). 7. Select one of the following: <ul style="list-style-type: none"> • aggregate—To use RSVP aggregate messages. • no-aggregate—To not to use RSVP aggregate messages. 8. Select one of the following: <ul style="list-style-type: none"> • reliable—To enable reliable message delivery on the interface. • no-reliable—To disable reliable message delivery on the interface. 9. From the Hello Interval list, select the length of time between hello packets. A value of 0 disables the sending of hello packets on the interface. Range: 1 through 60 seconds Default: 9 seconds

Table 198: RSVP Configuration Details (*continued*)

Task	Your Action
Preempt RSVP sessions.	<ol style="list-style-type: none"> 1. Click Preemption next to Rsvp. 2. In the Comment box, enter the comment. 3. Select one of the following: <ul style="list-style-type: none"> • disabled—To stop preempt RSVP sessions. • normal—To preempt RSVP sessions to accommodate new higher-priority sessions when bandwidth is insufficient to handle all sessions. • aggressive—To preempt RSVP sessions whenever bandwidth is insufficient to handle all sessions. 4. Click Soft Preemption next to Preemption. 5. From the Cleanup Timer list, select a timer value for soft preemption A value of 0 disables soft preemption. Range: 0 through 180 seconds Default: 30 seconds
Enable RSVP protocol-level trace options.	<ol style="list-style-type: none"> 1. Click Traceoptions next to Rsvp. 2. In the Comment box, enter the comment for the traceoptions. 3. Click File next to Traceoptions. 4. In the Comment box, enter the comment for the filename. 5. In the Filename box, enter the name of the file to receive the output of the tracing operation. 6. In the Size box, enter the maximum trace file size. 7. From the Files list, select the maximum number of trace files. 8. Select one of the following: <ul style="list-style-type: none"> • no-world-readable—To restrict the file access to owner. • world-readable—To enable unrestricted access. 9. Click Flag next to Traceoptions. 10. Click Add new entry next to Flag. 11. From the Name list, select the flag to perform the trace operation. 12. In the Comment box, enter the comment for the flag. 13. Select the corresponding modifier for the tracing flag.
Enable ultimate-hop popping on point-to-multipoint LSPs.	<ol style="list-style-type: none"> 1. Click Tunnel Services next to Rsvp. 2. Click Devices next to Tunnel Services. 3. Click Add new entry next to Devices. 4. In the New devices window, enter the device names that specify which virtual tunnel interfaces are used to handle the RSVP traffic. Range: 0 to 8 devices

Related Documentation

- [Configuring the ILMI Protocol \(NSM Procedure\) on page 257](#)
- [Configuring Link Management Protocol \(NSM Procedure\) on page 278](#)

CHAPTER 21

Configuration of Routing Options

- [Configuring Confederation \(NSM Procedure\) on page 366](#)
- [Configuring Dynamic Tunnels \(NSM Procedure\) on page 367](#)
- [Configuring Fate Sharing \(NSM Procedure\) on page 368](#)
- [Configuring Flow Route \(NSM Procedure\) on page 370](#)
- [Configuring Forwarding Table \(NSM Procedure\) on page 372](#)
- [Configuring Generated Routes \(NSM Procedure\) on page 373](#)
- [Configuring Instance Export \(NSM Procedure\) on page 374](#)
- [Configuring Instance Import \(NSM Procedure\) on page 375](#)
- [Configuring Interface Routes \(NSM Procedure\) on page 376](#)
- [Configuring Martian Addresses \(NSM Procedure\) on page 377](#)
- [Configuring Maximum Paths \(NSM Procedure\) on page 378](#)
- [Configuring Maximum Prefixes \(NSM Procedure\) on page 379](#)
- [Configuring Multicast \(NSM Procedure\) on page 381](#)
- [Configuring Options \(NSM Procedure\) on page 384](#)
- [Configuring Routing Tables \(NSM Procedure\) on page 385](#)
- [Configuring Routing Table Groups \(NSM Procedure\) on page 387](#)
- [Configuring Source Routing \(NSM Procedure\) on page 388](#)
- [Configuring Static Routes \(NSM Procedure\) on page 389](#)
- [Configuring Traceoptions \(NSM Procedure\) on page 390](#)
- [Configuring Topologies \(NSM Procedure\) on page 391](#)

Configuring Confederation (NSM Procedure)

Grouping autonomous systems (ASs) into confederations reduces the number of BGP connections required to interconnect ASs. If you administer multiple ASs that contain many BGP systems, you can group them into one or more confederations. Each confederation is identified by its own AS number, which is called a confederation AS number. To external ASs, a confederation appears to be a single AS. Thus, the internal topology of the ASs (members) making up the confederation is hidden. Because each confederation is treated as if it were a single AS, you can apply the same routing policy to all the ASs that make up the confederation.

To configure a confederation in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Confederation**.
6. Add or modify the parameters as specified in [Table 199 on page 366](#).
7. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply—To apply the routing option settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 199: Confederation Fields

Option	Function	Your Action
Comment	Specifies the comment for the confederation.	Enter a comment.
Confederation As	Specifies the confederation AS number.	Enter a number from 1 through 65535.

Table 199: Confederation Fields (*continued*)

Option	Function	Your Action
Members	Specifies the AS number of the confederation member, allowing you to add members to the confederation.	<ol style="list-style-type: none"> 1. Expand the Confederation tree and select Members. 2. Click the New button or select a member and click the Edit button. 3. Enter the AS number of the member.

Configuring Dynamic Tunnels (NSM Procedure)

A Virtual Private Network (VPN) that travels through a non-MPLS network requires a generic routing encapsulation (GRE) tunnel. This tunnel can be either a static tunnel or a dynamic tunnel. A static tunnel is configured manually between two provider edge (PE) routers. A dynamic tunnel is configured using BGP route resolution. You can specify the type of tunnel to be dynamically created by including the tunnel-type option.

To configure dynamic tunnels in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Routing Options**.
4. Select **Dynamic Tunnels**.
5. Add or modify settings as specified in [Table 200 on page 367](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 200: Dynamic Tunnels Configuration Details

Task	Your Action
Configure a dynamic tunnel between two PE routers	<ol style="list-style-type: none"> 1. Expand Dynamic Tunnels. 2. In the Comment box, enter the comment. 3. Click Dynamic Tunnel next to Dynamic Tunnels. 4. Click Add new entry next to Dynamic Tunnel. 5. In the Name box, enter the name of the dynamic tunnel. 6. In the Source Address box, enter the source address. 7. From the Tunnel Type list, select the type of tunnel to be dynamically created. The only valid value is gre (for GRE tunnels). 8. Click Destination Networks next to dynamic-tunnel. 9. Click Add new entry next to Destination Networks. 10. In the Name box, enter the prefix name. 11. In the Comment box, enter the comment.

Table 200: Dynamic Tunnels Configuration Details (*continued*)

Task	Your Action
Define tracing operations that track all routing protocol functionality in the router	<ol style="list-style-type: none"> 1. Click Traceoptions next to Dynamic Tunnels. 2. Expand Traceoptions. 3. In the Comment box, enter the comment for the traceoptions. 4. Click File next to Traceoptions. 5. In the Comment box, enter the comment for the filename. 6. In the Filename box, enter the name of the file to receive the output of the tracing operation. 7. In the Size box, enter the maximum trace file size. 8. From the Files list, select the maximum number of trace files. 9. Select one of the following: <ul style="list-style-type: none"> • Select no-world-readable—To restrict the file access to owner. • Select world-readable—To enable unrestricted access. 10. Click Flag next to Traceoptions. 11. Click Add new entry next to Flag. 12. From the Name list, select the flag to perform the trace operation. 13. In the Comment box, enter the comment for the flag. 14. Select the Disable check box to disable the tracing operation. 15. Select the modifier for the tracing flag. You can specify one or more of these modifiers: <ul style="list-style-type: none"> • Select the Send check box for packets being transmitted. • Select Receive check box for packets being received. • Select the Detail check box for detailed trace information. • Select the Disable check box to disable the tracing operation.

Configuring Fate Sharing (NSM Procedure)

Fate sharing allows you to create a database of information that the constrained shortest path first (CSPF) algorithm uses to compute one or more backup routing paths to use in case the primary path becomes unstable. The database describes the relationships between elements of the network. Through fate sharing, you can configure backup paths that minimize the number of shared links and fiber optic cables, to ensure that in the event of damage to a fiber optic cable, only the minimum amount of data is lost and that a path still exists to the destination. For a backup path to work optimally, it must not share links or physical fiber optic cables with the primary path. This ensures that a single point of failure will not affect the primary and backup paths at the same time.

This feature enables you to specify groups of objects that share characteristics resulting in backup paths to be used if primary paths fail. All objects are treated as /32 host addresses. You can specify one or more objects within a group. The objects can be LAN interfaces, device IDs, or point-to-point links.

To configure fate sharing in NSM:

1. In the navigation tree, select **Device Manager > Devices** .
2. In the **Devices** list, double click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Fate Sharing**.
6. Add or modify the parameters as specified in [Table 201 on page 369](#).
7. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply—To apply the routing option settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 201: Fate Sharing Fields

Option	Function	Your Action
Comment	Specifies the comment for the fate sharing.	Enter a comment.
Group		
Name	Specifies the name of the fate sharing group.	<ol style="list-style-type: none">1. Expand the Fate Sharing tree and select Group.2. Click the New button or select a group and click the Edit button.3. Enter the group name.
Comment	Specifies the comment for the fate sharing group.	<ol style="list-style-type: none">1. Expand the Fate Sharing tree and select Group.2. Click the New button or select a group and click the Edit button.3. Enter the comment.

Table 201: Fate Sharing Fields (*continued*)

Option	Function	Your Action
Cost	Specifies the configurable cost attributed to each group, which represents the level of impact this group has on CSPF computations. The higher the cost, the less likely a backup path will share any objects in the group with the primary path.	<ol style="list-style-type: none"> 1. Expand the Fate Sharing tree and select Group. 2. Click the New button or select a group and click the Edit button. 3. Enter the cost or select a value from the list.
From	Specifies the from address and to address for point-to-point link objects.	<ol style="list-style-type: none"> 1. Expand the Group tree and select From. 2. Click the New button or select a group and click the Edit button. 3. Specify the From address.

Configuring Flow Route (NSM Procedure)

Flow routes provide traffic filtering and rate-limiting capabilities much like firewall filters. You can propagate flow routes across different autonomous systems. A flow route is an aggregation of match conditions for IP packets. Flow routes are propagated through the network using flow-specific network-layer reachability information (NLRI) messages and are maintained in the flow routing table. Packets can travel through flow routes only if specific match conditions are met. Flow routes and firewall filters are similar in that they filter packets based on packet components and perform an action on the packets that match.

To configure a flow route in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Flow**.
6. Add or modify the parameters as specified in [Table 202 on page 371](#).
7. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply—To apply the routing option settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 202: Flow Route Fields

Option	Function	Your Action
Comment	Specifies the comment for the flow route.	Enter a comment.
Route		
Name	Specifies the name of the flow route.	<ol style="list-style-type: none"> 1. Expand the Flow tree and select Route. 2. Click the New button or select a flow route and click the Edit button. 3. Enter the flow route name.
Comment	Specifies the comment for the flow route.	<ol style="list-style-type: none"> 1. Expand the Flow tree and select Route. 2. Click the New button or select a flow route and click the Edit button. 3. Enter the comment for the flow route.
Match	Specifies the conditions that the packet must match for the packet to be included in flow route. Match conditions are: <ul style="list-style-type: none"> • Destination Port • DSCP • Fragment • Icmp Code • Icmp Type • Packet Length • Port • Protocol • Source Port • Tcp Flag 	<ol style="list-style-type: none"> 1. Expand the Route tree and select Match. 2. Enter a comment for Comment, a destination address for Destination, and a source address for Source. 3. Configure the match conditions.
Then	Enables you to specify the action to take if the packet matches the conditions you have configured in the flow route.	<ol style="list-style-type: none"> 1. Expand the Route tree and select Then. 2. Configure the then conditions for the packet.

Table 202: Flow Route Fields (*continued*)

Option	Function	Your Action
Validation		
Comment	Specifies a comment for the validation procedure. Flow routes are installed into the flow routing table only if they have been validated using the validation procedure.	<ol style="list-style-type: none"> 1. Expand the Flow tree and select Validation. 2. Enter the comment for the validation procedure.
Traceoptions	Enables you to define tracing operations that track all routing protocol functionality in the device and specify that tracing results be saved in a log file. You can configure the tracing flag, filter, and the tracing policy.	<ol style="list-style-type: none"> 1. Expand the Validation tree and select Traceoptions. 2. Expand the Traceoptions tree and configure the file and flag parameters, and the tracing policy.

Configuring Forwarding Table (NSM Procedure)

A forwarding table contains the routes actually used to forward packets through the device to their next-hop destination. This feature enables you to configure forwarding table in NSM.

To configure forwarding table in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Forwarding Table**.
6. Add or modify the parameters as specified in [Table 203 on page 373](#).
7. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply—To apply the routing option settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 203: Forwarding Table Fields

Option	Function	Your Action
Comment	Specifies the comment for the forwarding table.	Enter a comment.
None	Specifies that no next- hop parameter is to be added to the forwarding table.	Select the option button.
indirect-next-hop	Specifies that the forwarding table supports indirectly connected next hops.	Select the option button to enable indirect-next- hop .
no-indirect-next-hop	Specifies that the forwarding table does not support indirectly connected next hops.	Select the option button to enable no-indirect-next- hop .
Unicast Reverse Path	Enables you to check path validity to protect the network from IP spoofing. A unicast reverse-path-forwarding (RPF) check performs a routing table lookup on an IP packet's source address and checks the incoming interface. The device determines whether the packet is arriving from a path that the sender would use to reach the destination. If the packet is from a valid path, the device forwards the packet to the destination address. If it is not from a valid path, the device discards the packet.	Select the path from the drop-down list.
Export	Enables you to apply one or more policies to routes being exported from the routing table into the forwarding table.	<ol style="list-style-type: none"> 1. Expand the Forwarding Table tree and select Export. 2. Enter the export policies.

Configuring Generated Routes (NSM Procedure)

Generated routes are used as routes of last resort. A packet is forwarded to the route of last resort when the routing tables have no information about how to reach that packet's destination. One use of route generation is to create a default route to use if the routing table contains a route from a peer on a neighboring backbone network. A generated route becomes active when it has one or more contributing routes. A contributing route is an active route that is a specific match for the generated destination.

For example, for the destination **128.100.0.0/16**, routes to **128.100.192.0/19** and **128.100.67.0/24** are contributing routes, but routes to **128.0.0.0/8**, **128.0.0.0/16**, and **128.100.0.0/16** are not. A route can contribute only to a single generated route. However, an active generated route can recursively contribute to a less specific matching generated route. For example, a generated route to the destination **128.100.0.0/16** can contribute to a generated route to **128.96.0.0/13**. By default, when generated routes are installed in the routing table, the next hop device selects from the primary contributing route.

To configure generated routes in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Generate**.
6. Add or modify the parameters as specified in [Table 204 on page 374](#).
7. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply—To apply the routing option settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 204: Generated Routes Fields

Option	Function	Your Action
Comment	Specifies the comment for the generated route.	Enter a comment.
Defaults	Enables you to specify globally generated route options. These are treated as global defaults and apply to all the generated routes you configure.	<ol style="list-style-type: none"> 1. Expand the Generate tree and select Defaults. 2. Configure the default route options.
Route	Enables you to configure individually generated routes. You can also configure globally generated route options. These options apply to the individual destination only and override any options you configured in Defaults.	<ol style="list-style-type: none"> 1. Expand the Generate tree and select Route. 2. Configure the individual route options.

Configuring Instance Export (NSM Procedure)

Current configurations that use routing table groups define a policy to select routes in an IGP export policy. However, no policy controls the export process itself. You can configure the instance export policy to control the export process. The policy model supports both interinstance route export and IGP export.

To configure an instance export policy in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Instance Export** and specify the export policies for routes being exported from a routing instance.
6. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply—To apply the routing option settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Configuring Instance Import (NSM Procedure)

You can apply one or more policies to routes being imported into a routing instance.

To configure instance import in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Instance Import** and specify the import policies to be applied to the routes that are imported to a routing instance.
6. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply—To apply the routing option settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Configuring Interface Routes (NSM Procedure)

You can associate a routing table group with the device's interfaces and specify routing tables into which interface routes are imported. To define the routing tables into which interface routes are imported, you create a routing table group and associate it with the device's interfaces.

To configure interface routes in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Interface Routes**.
6. Add or modify the parameters as specified in [Table 205 on page 376](#).
7. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply—To apply the routing option settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 205: Interface Routes Fields

Option	Function	Your Action
Comment	Specifies the comment for the interface route.	Enter a comment.

Table 205: Interface Routes Fields (*continued*)

Option	Function	Your Action
Family	Specifies the address family as IPv4 or IPv6.	<ol style="list-style-type: none"> 1. Expand the Interface Routes tree and select Family. 2. Click the New button or select a family name and click the Edit button. 3. Enter the family name and comment. 4. Set up the export policy and import policy.
Rib Group	Specifies the routing table groups to which interface routes are imported.	<ol style="list-style-type: none"> 1. Expand the Interface Routes tree and select Rib Group. 2. Enter the comment and Inet.

Configuring Martian Addresses (NSM Procedure)

Martian addresses are host or network addresses about which all routing information is ignored. They commonly are sent by improperly configured systems on the network and have destination addresses that are obviously invalid. You can configure a particular martian address or a range of martian addresses as allowed or disallowed. You can use the match criteria to configure a range of martian addresses.

To configure a martian address in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Martians**.
6. Add or modify the parameters as specified in [Table 206 on page 378](#).
7. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply—To apply the routing option settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 206: Configuring Martian Address Fields

Option	Function	Your Action
Address	Specifies the martian address or the destination prefix of a series of martian addresses that are to be allowed or disallowed.	<ol style="list-style-type: none"> 1. Click the New button or select a martian address and click the Edit button. 2. Enter the address.
Comment	Specifies the comment for the martian address.	<ol style="list-style-type: none"> 1. Click the New button or select a martian address and click the Edit button. 2. Enter the comment for the martian address.
Allow	Enables you to explicitly allow a subset of a range of addresses that are to be disallowed.	<ol style="list-style-type: none"> 1. Click the New button or select a martian address and click the Edit button. 2. Select the check box to allow the disallowed address. Selecting the allow option deletes a particular martian address from the range of martian addresses. 3. Clear the check box to disallow the addresses and mark them as a martian address.
Exact	<p>Specifies match criteria for the route's mask length with the martian address. The criteria are:</p> <ul style="list-style-type: none"> • Exact • Longer • Orlonger • Upto • Through • Prefix Length Range 	<ol style="list-style-type: none"> 1. Click the New button or select a martian address and click the Edit button. 2. Expand the Martian tree and select Exact. 3. Enter the match criteria.

Configuring Maximum Paths (NSM Procedure)

You can configure a limit for the number of routes installed in a routing table based upon the number of route paths in the table.

To configure a maximum paths limit in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Maximum Paths**.

6. Enter the parameters as specified in [Table 207 on page 379](#).
7. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply—To apply the routing option settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 207: Configuring Maximum Paths Fields

Option	Function	Your Action
Comment	Specifies the comment for the maximum path limit.	Enter the comment.
Limit	Indicates the maximum number of routes. If this limit is reached, a warning is triggered and additional routes are rejected.	Enter limit value or select a value from the list.
Log Interval	Indicates the minimum time interval (in seconds) between log messages.	Enter the log interval value or select a value from the list.
Threshold	<p>Specifies what is to be done when the routing table reaches the maximum path value. The options are:</p> <ul style="list-style-type: none"> • None • threshold—Percentage of the maximum number of routes when installed, starts triggering the warning. You can configure a percentage of the Limit value that when reached starts triggering the warnings. • log-only—Sets the route limit as an advisory limit. An advisory limit triggers only a warning, and additional routes are not rejected. 	<ol style="list-style-type: none"> 1. Expand the Maximum Paths tree and select Threshold. 2. Select the option button.

Configuring Maximum Prefixes (NSM Procedure)

You can configure a limit for the number of routes installed in a routing table based upon the number of route prefixes in the table. .

To configure maximum prefixes limit in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Maximum Prefixes**.
6. Enter the parameters as specified in [Table 208 on page 380](#).
7. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply—To apply the routing option settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 208: Configuring Maximum Prefixes Fields

Option	Function	Your Action
Comment	Specifies the comment for the maximum prefix limit.	Enter the comment.
Limit	Indicates the maximum number of route prefixes. If this limit is reached, a warning is triggered and additional routes are rejected.	Enter limit value or select from the list.
Log Interval	Indicates the minimum time interval (in seconds) between log messages.	Enter the log interval value or select from the list.
Threshold	<p>Specifies what is to be done when the routing table reaches the maximum prefix value. The options are:</p> <ul style="list-style-type: none"> • None—No action is to be taken. • threshold—You can configure a percentage for the maximum number of prefixes, which when installed, triggers the warning. • log-only—Sets the prefix limit as an advisory limit. An advisory limit triggers only a warning, and additional routes are not rejected. 	<ol style="list-style-type: none"> 1. Expand the Maximum Prefixes tree and select Threshold. 2. Select the option button.

Configuring Multicast (NSM Procedure)

You can configure generic multicast properties for routing instances. A routing instance is a collection of routing tables, interfaces, and routing protocol parameters. The routing protocol parameters control the information in the routing tables.

To configure generic multicast properties for routing instance in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Multicast**.
6. Add or modify the parameters as specified in [Table 209 on page 381](#).
7. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply—To apply the routing option settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 209: Configuring Multicast Fields

Option	Function	Your Action
Comment	Specifies the comment for the multicast configuration.	Enter the comment.
Backup Pe Group	Enables you to configure a backup provider edge (PE) group for ingress PE device redundancy when point-to-multipoint label-switched paths (LSPs) are used for multicast distribution.	<ol style="list-style-type: none">1. Expand the Multicast tree and select Backup Pe Group.2. Click the New button or select a group and click the Edit button.3. Configure the PE group name, local address, and backup address.

Table 209: Configuring Multicast Fields (*continued*)

Option	Function	Your Action
Flow Map	Enables you to set up multicast flow maps to manage a subset of multicast forwarding table entries. For example, you can specify that certain forwarding cache entries be permanent or have a different timeout value than those of other multicast flows that are not associated with this flow map .	<ol style="list-style-type: none"> 1. Expand the Multicast tree and select Flow Map. 2. Click the New button or select a flow map and click the Edit button. 3. Configure the following to create and define a flow map: <ul style="list-style-type: none"> • Enter the flow map name and comment. • Bandwidth—Specify the bandwidth property of the multicast flow map. • Forwarding Cache—Specify the forwarding cache properties of entries defined by a flow map. You can specify a timeout of never to make the forwarding entries permanent, or you can specify a timeout from 1 through 720 minutes. • Policy—Specify the flow map policies. • Redundant Sources—Specify the addresses for use as backup sources for multicast flows defined by a flow map.
Forwarding Cache	<p>Enables you to configure multicast forwarding cache properties. These properties include threshold suppression and reuse limits, and timeout values.</p> <p>You can specify a value for the threshold to suppress new multicast forwarding cache entries and an optional reuse value for the threshold at which the device begins to create new multicast forwarding cache entries. If you configure both reuse and suppression values, configure a reuse value that is less than the suppression value. The suppression value is mandatory. If you do not specify the optional reuse value, then the number of multicast forwarding cache entries is limited to the suppression value. A new entry is created as soon as the number of multicast forwarding cache entries falls below the suppression value. You can also specify a timeout value for all multicast forwarding cache entries.</p>	<ol style="list-style-type: none"> 1. Expand the Multicast tree and select Forwarding Cache. 2. Configure the timeout and threshold values.

Table 209: Configuring Multicast Fields (*continued*)

Option	Function	Your Action
Interface	Enables you to configure the interfaces for multicast properties on which you plan to manage the maximum bandwidth.	<ol style="list-style-type: none"> 1. Expand the Multicast tree and select Interface. 2. Configure the interface and the bandwidth.
Rpf Check Policy	<p>Multicast reverse path forwarding (RPF) checks are used to prevent multicast routing loops. Routing loops are particularly debilitating in multicast applications because packets are replicated with each pass around the routing loop.</p> <p>You can apply policies for disabling reverse-path forwarding (RPF) checks on arriving multicast packets.</p>	<ol style="list-style-type: none"> 1. Expand the Multicast tree and select Rpf Check Policy. 2. Click the New button or select a policy and click the Edit button. 3. Enter the RPF check policy name.
Scope	Enables you to configure multicast scoping to limit multicast traffic by configuring it to an administratively defined topological region. Multicast scoping controls the propagation of multicast messages—both multicast group joins upstream toward a source and data forwarding downstream. Scoping can relieve stress on scarce resources, such as bandwidth, and improve privacy or scaling properties.	<ol style="list-style-type: none"> 1. Expand the Multicast tree and select Scope. 2. Configure the scope and the interface for the multicast.
Scope Policy	Enables you to configure multicast scoping policy. A multicast scope policy contains a set of device interfaces on which you are configuring scoping and the scope's address range configured as a series of device filters.	<ol style="list-style-type: none"> 1. Expand the Multicast tree and select Scope Policy. 2. Specify the scope policy for the multicast group.
Ssm Groups	Enables you to configure source-specific multicast (SSM) groups. SSM is a service model that identifies session traffic by both source and group address. Using SSM, a client can receive multicast traffic directly from the source. To deploy SSM successfully, you need an end-to-end multicast-enabled network and applications that use an Internet Group Management Protocol version 3 (IGMPv3).	<ol style="list-style-type: none"> 1. Expand the Multicast tree and select Ssm Groups. 2. Click the New button or select a group and click the Edit button. 3. Specify the address range of the SSM group.

Table 209: Configuring Multicast Fields (*continued*)

Option	Function	Your Action
Ssm Map	SSM mapping translate IGMPv1 or IGMPv2 membership reports to an IGMPv3 report allowing you to support an SSM network without requiring all hosts to support IGMPv3.	<ol style="list-style-type: none"> 1. Expand the Multicast tree and select Ssm Map. 2. Click the New button or select an SSM map and click the Edit button. 3. Specify the SSM policy for the SSM map and the source address.
Traceoptions	Defines tracing options for the multicast group. You can also set up the file management and access control parameters .	<ol style="list-style-type: none"> 1. Expand the Multicast tree and select the Traceoptions tab. 2. Set up the file and flag parameters.

Configuring Options (NSM Procedure)

You can configure the types of system logging messages sent about the routing protocols process to the system log message file. These messages are also displayed on the system console. You can log messages at a particular level or up to and including a particular level.

To configure options in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Options**.
6. Enter the parameters as specified in [Table 210 on page 385](#).
7. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply—To apply the routing option settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 210: Configuring Options Fields

Option	Function	Your Action
Comment	Specifies the comment for the message option.	Enter the comment.
Mark	Specifies the mark for the option.	Enter the mark value or select from the list.
Syslog	Enables you to configure the generation of system log messages for a particular severity level and all higher levels.	<ol style="list-style-type: none"> 1. Expand the Options tree and select Syslog. 2. Select the severity levels for system log messages.

Configuring Routing Tables (NSM Procedure)

This feature enables you to configure routing tables. You can also configure the static, martians, aggregate, maximum paths, maximum prefixes, multipath, or generated routes to the routing table. If you are not adding any of those routes, then the creation of the routing table is optional. The Junos OS uses its default routing tables, which are **inet.0** for IPv4 unicast routes, **inet6.0** for IPv6 unicast routes, **inet.1** for the IPv4 multicast forwarding cache, and **inet.3** for IPv4 MPLS.

To configure a routing table in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Rib**.
6. Add or modify the parameters as specified in [Table 211 on page 386](#).
7. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply—To apply the routing option settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 211: Rib Fields

Option	Function	Your Action
Name	Specifies the unique name for the routing table.	<ol style="list-style-type: none"> 1. Expand the Routing Options tree and select Rib. 2. Click the New button or select a routing table and click the Edit button. 3. Enter the name for the routing table.
Comment	Specifies the comment for the route resolution.	<ol style="list-style-type: none"> 1. Expand the Routing Options tree and select Rib. 2. Click the New button or select a routing table and click the Edit button. 3. Enter the comment for the routing table.
Aggregate	Enables you to configure the aggregate routes for the routing table. Aggregation allows you to combine groups of routes with common addresses into a single entry in the routing table. This decreases the size of the routing table as well as the number of route advertisements sent by the router.	<ol style="list-style-type: none"> 1. Expand the Rib tree and select Aggregate. 2. Select the global aggregate route options in Defaults and individual aggregate route options in Route.
Generate	Enables you to configure generated routes, which are used as routes of last resort in the routing table.	<ol style="list-style-type: none"> 1. Expand the Rib tree and select Generate. 2. Select the default route to the destination address in Defaults and individually generated route options in Route.
Martians	Enables you to configure martian addresses in the routing table.	<ol style="list-style-type: none"> 1. Expand the Rib tree and select Martian. 2. Enter the martian addresses.
Maximum Paths	Enables you to configure a limit for the number of routes installed in a routing table.	<ol style="list-style-type: none"> 1. Expand the Rib tree and select Maximum Paths. 2. Enter the Maximum Paths and the Threshold.
Maximum Prefixes	Enables you to configure a limit for the number of routes installed in a routing table.	<ol style="list-style-type: none"> 1. Expand the Rib tree and select Maximum Prefixes. 2. Set up the Maximum Prefixes and the Threshold.

Table 211: Rib Fields (*continued*)

Option	Function	Your Action
Multipath	Enables you to configure the multipath option in the routing table for load sharing between external BGP and internal BGP.	<ol style="list-style-type: none"> 1. Expand the Rib tree and select Multipath. 2. Enter the multipath options.
Static	Enables you to configure static routes to be installed in the routing table.	<ol style="list-style-type: none"> 1. Expand the Rib tree and select Static. 2. Enter the global static route in Defaults and destination address of the static route in Route.

Configuring Routing Table Groups (NSM Procedure)

You can group together one or more routing tables to form a routing table (RIB) group. Within a group, a routing protocol can import routes into all the routing tables in the group and can export routes from a single routing table. Each routing table group contains one or more routing tables that the Junos OS uses when importing routes. In the same way, each routing table group optionally contains one routing table that the Junos OS uses when exporting routes to the routing protocols. You can also specify the import and the export route tables and the import policies for the routing table group.

To configure routing table groups in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Rib Groups**.
6. Add or modify the parameters as specified in [Table 212 on page 388](#).
7. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply—To apply the routing option settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 212: Rib Group Fields

Option	Function	Your Action
Name	Specifies the unique name for the routing table group.	<ol style="list-style-type: none"> 1. Expand the Routing Options tree and select Rib Group. 2. Click the New button or select a routing table group and click the Edit button. 3. Enter the name for the routing table group.
Comment	Specifies the comment for the routing table group.	<ol style="list-style-type: none"> 1. Expand the Routing Options tree and select Rib Group. 2. Click the New button or select a routing table group and click the Edit button. 3. Enter the comment for the routing table group.
Export Rib	Specifies the routing table from which the Junos OS exports routing information.	<ol style="list-style-type: none"> 1. Expand the Routing Options tree and select Rib Group. 2. Click the New button or select a routing table group and click the Edit button. 3. Enter the name of the routing table.
Import Policy	Enables you to apply one or more policies to routes imported into the routing table group.	<ol style="list-style-type: none"> 1. Expand the rib-group tree and select Import Policy. 2. Set up the import policies for the routing table group.
Import Rib	Specifies the name of the routing table into which the Junos OS is to import routing information. The first routing table name you enter is the primary routing table. Any additional names you enter identify secondary routing tables. When a protocol imports routes, it imports them into the primary and any secondary routing tables.	<ol style="list-style-type: none"> 1. Expand the rib-group tree and select Import Policy. 2. Enter the name of the routing table.

Configuring Source Routing (NSM Procedure)

You can configure source routing to specify IP addresses of the devices along the path, that you want an IP packet to take on its way to its destination.

To configure source routing in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.

- 3. Click the **Configuration** tab.
- 4. In the configuration tree, expand **Routing Options**.
- 5. Select **Source Routing**.
- 6. Enter the parameters as specified in [Table 213 on page 389](#).
- 7. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply—To apply the routing option settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 213: Source Routing Fields

Option	Function	Your Action
Comment	Specifies the comment for the source routing configuration.	Enter the comment.
IP	Specifies the IPv4/IPv6 addressing family for source routing.	Select the check box.

Configuring Static Routes (NSM Procedure)

- You can configure static routes for a routing table group. A router uses static routes in the following scenarios:
- When it does not have a route to a destination that has a better (lower) preference value.
 - When it cannot determine the route to a destination.
 - When it is forwarding unroutable packets.
- A static route is installed in the routing table only when the route is active; that is, the list of next-hop routers configured for that route contains at least one next hop on an operational interface.
- To configure static routes for a routing table group in NSM:
- 1. In the navigation tree, select **Device Manager > Devices**.
 - 2. In the **Devices** list, double-click the device to select it.

3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Static**.
6. Add or modify the parameters as specified in [Table 214 on page 390](#).
7. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply—To apply the routing option settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 214: Static Fields

Option	Function	Your Action
Comment	Specifies the comment for the static route.	Enter the comment.
Rib Group	Specifies the routing table group name for which the static route is configured.	Enter the name.
Defaults	Enables you to configure the global static route options. These options only set the global defaults and apply to all the configured static routes.	<ol style="list-style-type: none"> 1. Expand the Static tree and select Defaults. 2. Enter the default route to the destination address.
Route	Enables you to configure the individual static routes options. These options apply to the individual destination only and override any options configured in the Defaults section.	<ol style="list-style-type: none"> 1. Expand the Static tree and select Route. 2. Enter the individual route.

Configuring Traceoptions (NSM Procedure)

You can configure tracing operations for routing protocols to track all general routing operations and record them in a log file. Any global tracing operations that you configure are inherited by the individual routing protocols. To modify the global tracing operations for an individual protocol, configure the tracing option when configuring that protocol.

To configure tracing options for routing protocols in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Traceoptions**.
6. Add or modify the parameters as specified in [Table 215 on page 391](#).
7. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.
 - Apply—To apply the routing option settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 215: Traceoption Fields

Option	Function	Your Action
Comment	Specifies the comment for the tracing options.	Enter the comment.
File	Specifies the file to receive the output of the tracing operation.	<ol style="list-style-type: none">1. Expand the Traceoptions tree and select File.2. Enter the file parameters.
Flag	Specifies the global routing protocol tracing options to be performed. You can specify more than one option.	<ol style="list-style-type: none">1. Expand the Traceoptions tree and select File.2. Enter the flag parameters.

Configuring Topologies (NSM Procedure)

For Multitopology Routing to run on the router, you need to configure one or more topologies. For each topology, you specify a string value, such as voice, that defines the type of traffic, as well as an interface family, such as IPv4. In addition, a default topology is automatically created. You can also enable a topology for IPv4 multicast traffic. Each topology that you configure creates a new routing table and populates it with direct routes from the topology.

To configure topologies in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Routing Options**.
4. Select **Topologies**.
5. Add or modify settings as specified in [Table 216 on page 392](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 216: Topology Configuration Details

Task	Your Action
Configure topologies.	<ol style="list-style-type: none"> 1. Expand Topologies. 2. In the Comment box, enter the comment.
Configure the type of family address type.	<ol style="list-style-type: none"> 1. Click Family next to Topologies. 2. Click Add new entry next to Family. 3. Expand key-chain. 4. From the Name list, select the type of family address type. 5. In the Comment box, enter the comment. 6. Click Topology next to family. 7. Click Add new entry next to Topology. 8. In the Name box, enter the name of the topology. 9. In the Comment box, enter the comment.

Configuration of Security

- [Configuring Topologies \(NSM Procedure\) on page 393](#)
- [Configuring Certificates \(NSM Procedure\) on page 394](#)
- [Configuring Firewall Authentication \(NSM Procedure\) on page 396](#)
- [Configuring a Flow \(NSM Procedure\) on page 399](#)
- [Configuring Forwarding Options \(NSM Procedure\) on page 406](#)
- [Configuring IKE \(NSM Procedure\) on page 407](#)
- [Configuring IPsec \(NSM Procedure\) on page 414](#)
- [Configuring a PKI \(NSM Procedure\) on page 420](#)

Configuring Topologies (NSM Procedure)

For Multitopology Routing to run on the router, you need to configure one or more topologies. For each topology, you specify a string value, such as voice, that defines the type of traffic, as well as an interface family, such as IPv4. In addition, a default topology is automatically created. You can also enable a topology for IPv4 multicast traffic. Each topology that you configure creates a new routing table and populates it with direct routes from the topology.

To configure topologies in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Routing Options**.
4. Select **Topologies**.
5. Add or modify settings as specified in [Table 216 on page 392](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 217: Topology Configuration Details

Task	Your Action
Configure topologies.	<ol style="list-style-type: none"> 1. Expand Topologies. 2. In the Comment box, enter the comment.
Configure the type of family address type.	<ol style="list-style-type: none"> 1. Click Family next to Topologies. 2. Click Add new entry next to Family. 3. Expand key-chain. 4. From the Name list, select the type of family address type. 5. In the Comment box, enter the comment. 6. Click Topology next to family. 7. Click Add new entry next to Topology. 8. In the Name box, enter the name of the topology. 9. In the Comment box, enter the comment.

Configuring Certificates (NSM Procedure)

The certificates feature allows you to configure the certification authority and local certificate.

To configure certificates feature:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the certificates feature.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Certificates**.
4. Configure the options as specified in [Table 218 on page 394](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the certificates parameters.

Table 218: Certificates Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the certificates.	(Optional) Enter a comment.
Path Length	Specifies the maximum length of the certificate path.	Set the maximum length of the certificate path. Range: 0 - 15.
Maximum Certificates	Specifies the maximum number of certificates to cache.	Set the maximum number of certificates. Range: 64 - 4,294,967,295.
Cache Size	Specifies the maximum size of certificate cache.	Enter the cache size.

Table 218: Certificates Configuration Details (*continued*)

Option	Function	Your Action
Cache Timeout Negative	Specifies (in seconds) the time to cache negative responses.	Set the time to cache negative responses. Range: 10 - 4,294,967,295.
Enrollment Retry	Specifies the number of retry attempts for an enrollment request.	Set the number of retries. Range: 0 - 1080.

- [Configuring Certification Authority \(NSM Procedure\) on page 395](#)
- [Configuring the Local Certificate \(NSM Procedure\) on page 396](#)

Configuring Certification Authority (NSM Procedure)

To configure the certification authority feature:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the certification authority feature.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Certificates > Certification Authority**.
4. Add or modify settings as specified in [Table 219 on page 395](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the certification authority settings.

Table 219: Certification Authority Configuration Details

Option	Function	Your Action
Name	Specifies the certification authority profile name.	Enter the certification authority profile name.
Comment	Supplies a descriptive comment for the certification authority. This is optional.	Enter a comment.
Ca Name	Specifies the certification authority name.	Enter the certification authority name.
File	Specifies the file from which to read the certificate.	Enter the path and the filename.
Crl	Specifies the file to read the CRL.	Enter the path and the CRL filename.
Enrollment Url	Specifies the enrollment URL.	Enter the enrollment URL.
Ldap Url	Specifies the LDAP URL.	Enter the LDAP URL.
Encoding	Specifies the encoding to be used for the certificate or CRL on disk.	Select the encoding type from the list.

Configuring the Local Certificate (NSM Procedure)

To configure the local certificate feature:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the local certificate feature.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Certificates > Local**.
4. Add or modify settings as specified in [Table 220 on page 396](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the local settings.

Table 220: Local Configuration Details

Option	Function	Your Action
Name	Specifies the name of the certificate.	Enter a name.
Comment	Supplies a descriptive comment for the certificate.	(Optional) Enter a comment.
Certificate	Specifies the certificate and the private key.	Enter a private key for the certificate.

Related Documentation

- [Configuring Firewall Authentication \(NSM Procedure\)](#)
- [Configuring a Flow \(NSM Procedure\) on page 399](#)
- [Configuring Forwarding Options \(NSM Procedure\) on page 406](#)

Configuring Firewall Authentication (NSM Procedure)

You can configure the firewall authentication for pass-through, traceoptions, and Web authentication options.

To configure firewall authentication:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the firewall authentication feature.
3. Click the **Configuration** tab. In the configuration tree, select **Access > Firewall Authentication**.
4. Enter a comment for the firewall authentication in **Comment**.
5. Click one:

- **OK**—Saves the changes.
- **Cancel**—Cancels the modifications.
- **Apply**—Applies the firewall authentication parameters.
- [Configuring Pass-Through on page 397](#)
- [Configuring Traceoptions on page 398](#)
- [Configuring Web Authentication on page 399](#)

Configuring Pass-Through

To configure pass-through:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the pass-through feature.
3. Click the **Configuration** tab. In the configuration tree, select **Access > Firewall Authentication > Pass Through**.
4. Enter a comment for pass-through in **Comment**.
5. Select the name of the profile used if it is not used in the policy in **Default Profile**.
6. Add or modify settings as specified in [Table 221 on page 397](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the pass-through settings.

Table 221: Pass-Through Configuration Details

Option	Function	Your Action
Firewall Authentication > Pass Through > Ftp / Http / Telnet		
Comment	Supplies a descriptive comment for the pass-through firewall user authentication for FTP/HTTP/Telnet.	(Optional) Enter a comment.
Firewall Authentication > Pass Through > Ftp / Http / Telnet > Banner		
Comment	Supplies a descriptive comment for the banner session for FTP/HTTP/Telnet.	(Optional) Enter a comment.
Login	Specifies the message that will be displayed before login.	Enter an appropriate login message.
Success	Specifies the message that will be displayed on successful login.	Enter an appropriate message for a successful login.
Fail	Specifies the message that will be displayed after failed user login.	Enter an appropriate message for a failed user login.

Configuring Traceoptions

To configure traceoptions:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the traceoptions.
3. Click the **Configuration** tab. In the configuration tree, select **Access > Firewall Authentication > Traceoptions**.
4. Enter a comment for the traceoptions in **Comment**.
5. Select the check box to disable remote tracing in **No Remote Trace**.
6. Add or modify settings as specified in [Table 222 on page 398](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the traceoptions settings.

Table 222: Traceoptions Configuration Details

Option	Function	Your Action
Firewall Authentication > Traceoptions > File		
Comment	Supplies a descriptive comment for the file traceoptions.	(Optional) Enter a comment.
Filename	Specifies the name of the file in which to write the trace information.	Enter a filename for the trace information.
Size	Specifies the maximum trace file size.	Enter the maximum trace file size.
Files	Specifies the maximum number of trace files.	Set the number of trace files. Range: 2 through 1000.
world-reachable	Specifies that the executables are readable by any user.	Select the option.
no-world-reachable	Specifies that the executables are not readable by any user.	Select the option.
Match	Specifies the regular expression for the lines to be logged.	Enter the regular expression.
Firewall Authentication > Traceoptions > Flag		
Name	Specifies the flag name.	Select a flag name from the list.

Table 222: Traceoptions Configuration Details (*continued*)

Option	Function	Your Action
Comment	Supplies a descriptive comment for the flag option.	(Optional) Enter a comment.

Configuring Web Authentication

To configure Web authentication:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the Web authentication.
3. Click the **Configuration** tab. In the configuration tree, select **Access > Firewall Authentication > Web Authentication**.
4. Enter a comment for the Web authentication in **Comment**.
5. Select the name of the profile used if it is not used in the policy in **Default Profile**.
6. Add or modify settings as specified in [Table 223 on page 399](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the Web authentication settings.

Table 223: Web Authentication Configuration Details

Option	Function	Your Action
Firewall Authentication > Web Authentication > Banner		
Comment	Supplies a descriptive comment for the banner.	(Optional) Enter a comment.
Success	Specifies the message that will be displayed on a successful login.	Enter an appropriate message for a successful login.

Related Documentation

- [Configuring a RADIUS Server \(NSM Procedure\)](#)
- [Configuring RADIUS Options \(NSM Procedure\)](#)
- [Configuring a SecurID Server \(NSM Procedure\)](#)

Configuring a Flow (NSM Procedure)

The flow feature allows you to configure bridge, TCP MSS, TCP session, and traceoptions.

To configure the flow feature:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the flow options.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Flow**.
4. Configure the options as specified in [Table 224 on page 400](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the flow parameters.

Table 224: Flow Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the flow feature.	(Optional) Enter a comment.
Allow Dns Reply	Allows unmatched incoming DNS reply packets.	Select the Allow Dns reply check box to enable this feature.
Route Change Timeout	Specifies the timeout value for route change to nonexistence route.	Set the timeout value for the route change. Range: 6 - 1800.
Syn Flood Protection Mode	Specifies the TCP synchronized flood-protection mode.	Select the synchronized flood protection mode from the list.

You can configure the following options:

- [Configuring a Bridge \(NSM Procedure\) on page 400](#)
- [Configuring the TCP MSS Option \(NSM Procedure\) on page 401](#)
- [Configuring the TCP Session Option \(NSM Procedure\) on page 402](#)
- [Configuring Traceoptions \(NSM Procedure\) on page 403](#)

Configuring a Bridge (NSM Procedure)

To configure a bridge option:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure a bridge option.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Flow > Bridge**.
4. Configure the options as specified in [Table 225 on page 401](#).
5. Click one:

- **OK**—Saves the changes.
- **Cancel**—Cancels the modifications.
- **Apply**—Applies the bridge settings.

Table 225: Bridge Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the bridge option.	(Optional) Enter a comment.
Block Non IP All	Specifies that all non-IP and non-ARP traffic, including broadcast and multicast traffic are blocked.	Select the Block Non IP All check box to enable this feature.
Bypass Non IP Unicast	Allows all non-IP traffic that includes unicast traffic.	Select the Bypass Non IP Unicast check box to enable this feature.
Bridge > No Packet Flooding		
Enable Feature	Allows to enable the feature of setting the No Packet Flooding.	Select Enable Feature to enable this feature.
Comment	Supplies a descriptive comment for the packet flooding option.	(Optional) Enter a comment.
No Trace Route	Specifies that the ICMP must not be sent to trigger MAC learning.	Select the No Trace Route check box to enable this feature.

Configuring the TCP MSS Option (NSM Procedure)

To configure the TCP MSS option:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the TCP MSS option.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Flow > Tcp Mss**.
4. Configure the options as specified in [Table 226 on page 401](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the TCP MSS settings.

Table 226: TCP MSS Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for TCP MSS.	(Optional) Enter a comment.
Tcp Mss > All Tcp		

Table 226: TCP MSS Configuration Details (*continued*)

Option	Function	Your Action
Comment	Supplies a descriptive comment for the all TCP options.	(Optional) Enter a comment.
Mss	Specifies the maximum segment size for all TCP options.	Set the MSS value. Range: 64 - 65535.
Tcp Mss > Gre In		
Enable Feature	Enables the received Generic Routing Encapsulation (GRE) feature.	Select the Enable Feature check box to enable this feature.
Comment	Supplies a descriptive comment for the received GRE.	(Optional) Enter a comment.
Mss	Specifies the maximum segment size for the received GREs.	Set the MSS value. Range: 64 - 65535.
Tcp Mss > Gre Out		
Enable Feature	Enables the sent Generic Routing Encapsulation (GRE) feature.	Select the Enable Feature check box to enable this feature.
Comment	Supplies a descriptive comment for the sent GREs.	(Optional) Enter a comment.
Mss	Specifies the maximum segment size for the sent GREs.	Set the MSS value. Range: 64 - 65535.
Tcp Mss > IPsec Vpn		
Enable Feature	Enables the IPsec VPN feature.	Select the Enable Feature check box to enable this feature.
Comment	Supplies a descriptive comment for the IPsec VPN.	(Optional) Enter a comment.
Mss	Specifies the maximum segment size for IPsec VPNs.	Set the MSS value. Range: 64 - 65535.

Configuring the TCP Session Option (NSM Procedure)

To configure the TCP session option:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the TCP session option.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Flow > Tcp Session**.
4. Configure the options as specified in [Table 227 on page 403](#).
5. Click one:

- **OK**—Saves the changes.
- **Cancel**—Cancels the modifications.
- **Apply**—Applies the TCP session settings.

Table 227: TCP Session Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the TCP session.	(Optional) Enter a comment.
Rst Invalidate Session	Specifies that the session ends immediately on receipt of the reset segment.	Select the Rst Invalidate Session check box to enable this feature.
Rst Sequence Check	Enables checking of the sequence number in the reset segment.	Select the Rst Sequence Check check box to enable this feature.
No Syn Check	Disables the creation-time synchronized flag check.	Select the No Syn Check check box to enable this feature.
Strict Syn Check	Enables the strict synchronized check.	Select the Strict Syn Check check box to enable this feature.
No Syn Check In Tunnel	Disables creation-time synchronized flag check for tunnel packets.	Select the No Syn Check In Tunnel check box to enable this feature.
No Sequence Check	Disables sequence-number checking.	Select the No Sequence Check check box to enable this feature.
Tcp Initial Timeout	Specifies the timeout period for the TCP session when initialization fails.	Set the timeout period when the initialization fails. Range: 20 through 300.

Configuring Traceoptions (NSM Procedure)

The traceoptions feature allows you to configure file and flag options.

To configure the traceoptions:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the traceoptions.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Flow > Traceoptions**.
4. Configure the options as specified in [Table 228 on page 404](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the traceoptions settings.

Table 228: Traceoptions Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the traceoptions.	(Optional) Enter a comment.
No Remote Trace	Disables remote tracing.	Select the No Remote Trace check box to enable this feature.
Rate Limit	Specifies the limit for the incoming rate of trace messages.	Set the incoming rate for trace messages. Range: 0 - 4,294,967,295.

You can now configure the following options:

- [Configuring File Options \(NSM Procedure\) on page 404](#)
- [Configuring Flag Options \(NSM Procedure\) on page 405](#)
- [Configuring Packet Filter Options \(NSM Procedure\) on page 405](#)

Configuring File Options (NSM Procedure)

To configure file options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the file options.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Flow > Traceoptions > File**.
4. Configure the file options as specified in [Table 229 on page 404](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the file settings.

Table 229: File Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the filename.	(Optional) Enter a comment.
Filename	Specifies the filename to write the traceoptions.	Enter a filename.
Size	Specifies the maximum size of the trace file.	Enter the maximum file size.
Files	Specifies the maximum number of the trace files.	Set the maximum number of the trace files. Range: 2 - 1000.
None	Specifies that neither the world-readable nor the no-world-readable option is enabled.	Select the option.

Table 229: File Configuration Details (*continued*)

Option	Function	Your Action
world-readable	Allows any user to read the log file.	(Optional) Select the option.
no-world-readable	Prevents any user from reading the log file.	(Optional) Select the option.
Match	Specifies the regular expression for the lines to be logged.	Enter the match expression.

Configuring Flag Options (NSM Procedure)

To configure flag options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the flag options.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Flow > Traceoptions > Flag**.
4. Add or modify settings as specified in [Table 230 on page 405](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the flag settings.

Table 230: Flag Configuration Details

Option	Function	Your Action
Name	Specifies the trace flag name.	Select a name from the list.
Comment	Supplies a descriptive comment for the trace flag.	(Optional) Enter a comment.

Configuring Packet Filter Options (NSM Procedure)

To configure packet filter options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the packet filter options.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Flow > Traceoptions > Packet Filter**.
4. Add or modify settings as specified in [Table 231 on page 406](#).
5. Click one:
 - **OK**—Saves the changes.

- **Cancel**—Cancels the modifications.
- **Apply**—Applies the packet filter settings.

Table 231: Packet Filter Configuration Details

Option	Function	Your Action
Name	Specifies the trace packet filter name.	Enter a name.
Comment	Supplies a descriptive comment for the packet filter.	(Optional) Enter a comment.
Protocol	Specifies the match IP protocol type.	Select the protocol type from the list.
Source Prefix	Specifies the source IPv4 address prefix.	Enter the source IPv4 address prefix.
Destination Prefix	Specifies the destination IPv4 address prefix.	Enter the destination IPv4 address prefix.
Source Port	Specifies the match TCP/UDP source port.	Select the source port from the list.
Destination Port	Specifies the match TCP/UDP destination port.	Select the destination port from the list.
Interface	Specifies the logical interface.	Select the interface from the list.

**Related
Documentation**

- [Configuring Certificates \(NSM Procedure\) on page 394](#)
- [Configuring Firewall Authentication \(NSM Procedure\)](#)
- [Configuring Forwarding Options \(NSM Procedure\) on page 406](#)

Configuring Forwarding Options (NSM Procedure)

To configure forwarding options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure forwarding options.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Forwarding Options**.
4. Enter a comment in the Forwarding Options workspace that describes the forwarding options.
5. In the configuration tree, select **Security > Forwarding Options > Family**.
6. Enter a comment in the Family workspace that describes the family.
7. Configure the options as specified in [Table 232 on page 407](#).
8. Click one:
 - **OK**—Saves the changes.

- **Cancel**—Cancels the modifications.
- **Apply**—Applies the forwarding options.

Table 232: Forwarding Options Configuration Details

Option	Function	Your Action
Family > Inet6		
Comment	Supplies a descriptive comment for the IPv6 traffic.	(Optional) Enter a comment.
Mode	Specifies the IPv6 traffic forwarding mode.	Select the forwarding mode from the list.
Family > Iso		
Comment	Supplies a descriptive comment for the Intermediate System-to-Intermediate System (IS-IS) protocol traffic.	(Optional) Enter a comment.
Mode	Specifies the iso forwarding mode.	Select the forwarding mode from the list.
Family > Mpls		
Comment	Supplies a descriptive comment for the MPLS.	(Optional) Enter a comment.
Mode	Specifies the MPLS forwarding mode.	Select the forwarding mode from the list.

Related Documentation

- [Configuring Certificates \(NSM Procedure\) on page 394](#)
- [Configuring Firewall Authentication \(NSM Procedure\)](#)
- [Configuring a Flow \(NSM Procedure\) on page 399](#)

Configuring IKE (NSM Procedure)

The Internet Key Exchange (IKE) feature allows you to configure gateway, policy, proposal, respond to bad SPI, and traceoptions.

To configure the IKE feature:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure IKE options.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Ike**.
4. Enter a comment in the IKE workspace that describes the IKE.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

- **Apply**—Applies the IKE parameters.

You can now configure the following options:

- [Configuring a Gateway \(NSM Procedure\) on page 408](#)
- [Configuring a Policy \(NSM Procedure\) on page 410](#)
- [Configuring a Respond Bad SPI \(NSM Procedure\) on page 412](#)
- [Configuring Traceoptions \(NSM Procedure\) on page 412](#)

Configuring a Gateway (NSM Procedure)

To configure the gateway option:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the gateway option.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Ike > Gateway**.
4. Add or modify settings as specified in [Table 233 on page 408](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the gateway settings.

Table 233: Gateway Configuration Details

Option	Function	Your Action
gateway		
Name	Specifies the gateway name.	Enter the gateway name.
Comment	Supplies a descriptive comment for the gateway.	(Optional) Enter a comment.
Ike Policy	Specifies the name of the IKE policy.	Select the IKE policy from the list.
No Nat Traversal	Disables the IPsec NAT traversal.	Select the No Nat Traversal check box to enable this feature.
Nat Keepalive	Specifies the time interval to send the keepalives.	Set the time interval. Range: 1 - 300.
External Interface	Specifies the external interface for the IKE negotiations.	Enter the external interface for the IKE negotiations.
gateway > Address		
address	Specifies the address of the gateway.	Select the option and add or modify the address.

Table 233: Gateway Configuration Details (*continued*)

Option	Function	Your Action
dynamic	Specifies a dynamic IPsec for gateway.	<ol style="list-style-type: none"> 1. Select the option. 2. Select Dynamic and update the following: <ul style="list-style-type: none"> • Comment—Supplies a descriptive comment. • Connections limit—Specifies the maximum number of users connected to the gateway. Range: 0 - 4,294,967,295. • Ike User Type—Specifies the IKE ID type. 3. Select Dynamic > Distinguished Name and select any of the following: <ul style="list-style-type: none"> • None—Specifies that neither distinguished name nor hostname nor inet nor user-at-hostname is specified. • distinguished-name—Specifies the distinguished name for the gateway. Select the option and enter the following: <ul style="list-style-type: none"> • Comment—Supplies a descriptive comment for the distinguished name. • Container—Specifies the container text. • Wildcard—Specifies the wildcard text. • hostname—Specifies the hostname for the gateway. Select the option and enter the hostname.
gateway > Dead Peer Detection		
Enable Feature	Enables the dead peer detection (DPD) feature.	Select the Enable Feature check box to enable this feature.
Comment	Supplies a descriptive comment for the DPD.	(Optional) Enter a comment.
Always Send	Specifies that the DPD messages are sent periodically, regardless of the traffic.	Select the Always Send check box to enable this feature.
Interval	Specifies the time interval to send the DPD messages.	Set the time interval to send the DPD messages. Range: 10 - 60.
Threshold	Specifies the maximum number of DPD transmissions.	Set the threshold for DPD transmissions. Range: 1 - 5.
gateway > Local Identity		
Comment	Supplies a descriptive comment for the gateway local identity.	(Optional) Enter a comment.
gateway > Local Identity > Inet		
None	Specifies that inet, hostname, user-at-hostname, and distinguished-name are not enabled.	Select the option.

Table 233: Gateway Configuration Details (*continued*)

Option	Function	Your Action
inet	Specifies IPv4 traffic.	Select the option.
hostname	Specifies the hostname	Select the option.
user-at-hostname	Specifies the e-mail address.	Select the option.
distinguished-name	Specifies the distinguished name.	Select the option.
gateway > Xauth		
Comment	Supplies a descriptive comment for the gateway authentication.	(Optional) Enter a comment.
Access Profile	Specifies the access profile that contains the authentication information.	Select the access profile from the list.

Configuring a Policy (NSM Procedure)

To configure the policy option:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the policy option.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Ike > Policy**.
4. Add or modify settings as specified in [Table 234 on page 410](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the policy settings.

Table 234: Policy Configuration Details

Option	Function	Your Action
Policy		
Name	Specifies the name of the policy.	Enter the policy name.
Comment	Supplies a descriptive comment for the policy.	(Optional) Enter a comment.
Mode	Defines the IKE mode for phase 1.	Select the mode from the list.
Description	Specifies a text description for the IKE policy.	Enter a Description.
Proposal Set	Specifies the type of the default IKE proposal set.	Select the proposal set from the list.

Table 234: Policy Configuration Details (*continued*)

Option	Function	Your Action
Policy > Certificate		
Comment	Supplies a descriptive comment for the certificate.	(Optional) Enter a comment.
Local Certificate	Specifies the local certificate identifier.	Enter the local certificate identifier.
Peer Certificate Type	Specifies the preferred type of certificate from peer.	Select the certificate type from the list.
Policy > Certificate > Trusted Ca		
Comment	Supplies a descriptive comment for the trusted certification authority.	(Optional) Enter a comment.
Policy > Certificate > Trusted Ca > Ca index		
None	Specifies that neither the ca-index nor use all option is enabled.	Select the option.
ca-index	Specifies the preferred certificate authority ID for the device to use.	Select the option and set the certificate authority ID. Range: 0 - 4,294,967,295.
use-all	Specifies that the device uses all configured CAs.	Select the option.
Policy > Pre Shared Key		
Comment	Supplies a descriptive comment for the preshared key.	(Optional) Enter a comment.
Policy > Pre Shared Key > Ascii Text		
None	Specifies that neither the ascii-text nor hexadecimal key is enabled.	Select the option.
ascii-text	Enables the ASCII text key.	Select the option and enter the ASCII text key.
hexadecimal	Enables the hexadecimal text key.	Select the option and enter the hexadecimal text key.
Policy > Proposals		
Proposals	Specifies the members added as proposals.	Select the proposals from the nonmembers list. Then click Add to move them to the members list.

Configuring a Respond Bad SPI (NSM Procedure)

To configure the respond bad SPI options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the respond bad SPI option.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Ike > Respond Bad Spi**.
4. Select the **Enable Feature** check box.
5. Configure the options as specified in [Table 235 on page 412](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the respond bad SPI parameters.

Table 235: Respond Bad SPI Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the bad SPI.	(Optional) Enter a comment.
Max Responses	Specifies the maximum number of times to respond.	Set the maximum number of times to respond. Range: 1 - 30.

Configuring Traceoptions (NSM Procedure)

The traceoptions feature allows you to configure file and flag options.

To configure traceoptions:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the traceoptions.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Ike > Traceoptions**.
4. Configure the options as specified in [Table 236 on page 413](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the traceoptions settings.

Table 236: Traceoptions Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the traceoptions.	(Optional) Enter a comment.
No Remote Trace	Disables remote tracing.	Select the No Remote Trace check box.

You can now configure the following options:

- [Configuring the File Options \(NSM Procedure\) on page 413](#)
- [Configuring Flag Options \(NSM Procedure\) on page 414](#)

Configuring the File Options (NSM Procedure)

To configure file options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the file options.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Ike > Traceoptions > File**.
4. Configure the file options as specified in [Table 237 on page 413](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the file settings.

Table 237: File Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the filename.	Enter a comment.
Filename	Specifies the filename to write the traceoptions.	Enter a filename.
Size	Specifies the maximum size of the trace file.	Enter the maximum file size.
Files	Specifies the maximum number of trace files.	Set the maximum number of trace files. Range: 2 - 1000.
None	Specifies that neither the world-readable nor the no-world-readable option is enabled.	Select the option.
world-readable	Allows any user to read the log file.	(Optional) Select the option.
no-world-readable	Prevents any user from reading the log file.	(Optional) Select the option.

Table 237: File Configuration Details (*continued*)

Option	Function	Your Action
Match	Specifies the regular expression for the lines to be logged.	Enter the match expression.

Configuring Flag Options (NSM Procedure)

To configure flag options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the flag options.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Ike > Traceoptions > Flag**.
4. Add or modify setting as specified in [Table 238 on page 414](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the flag settings.

Table 238: Flag Configuration Details

Option	Function	Your Action
Name	Specifies the trace flag name.	Select a name from the list.
Comment	Supplies a descriptive comment for the trace flag.	Enter a comment.

- Related Documentation**
- [Configuring IPsec \(NSM Procedure\) on page 414](#)
 - [Configuring a PKI \(NSM Procedure\) on page 420](#)
 - [Configuring NAT \(NSM Procedure\)](#)

Configuring IPsec (NSM Procedure)

The Internet Protocol Security (IPsec) feature allows you to configure policy, proposal, traceoptions, VPN, and VPN monitor options.

To configure the IPsec feature:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the IPsec feature.
3. Click the **Configuration** tab. In the configuration tree, select **Security > IPsec**.

4. Enter a comment in the IPsec workspace that describes the IPsec.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the IPsec parameters.

You can now configure the following options:

- [Configuring a Policy \(NSM Procedure\) on page 415](#)
- [Configuring Traceoptions \(NSM Procedure\) on page 416](#)
- [Configuring a VPN \(NSM Procedure\) on page 416](#)
- [Configuring VPN Monitor Options \(NSM Procedure\) on page 419](#)

Configuring a Policy (NSM Procedure)

To configure the policy option:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the policy option.
3. Click the **Configuration** tab. In the configuration tree, select **Security > IPsec > Policy**.
4. Add or modify settings as specified in [Table 239 on page 415](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the policy settings.

Table 239: Policy Configuration Details

Option	Function	Your Action
policy		
Name	Specifies the name of the policy.	Enter the policy name.
Comment	Supplies a descriptive comment for the policy.	(Optional) Enter a comment.
Description	Specifies a text description for the IPsec policy.	Enter a description.
Proposal Set	Specifies the type of default IPsec proposal set.	Select the proposal set from the list.
policy > Perfect Forward Secrecy		
Comment	Supplies a descriptive comment for the perfect forward secrecy option. This is optional.	Enter a comment.

Table 239: Policy Configuration Details (*continued*)

Option	Function	Your Action
Keys	Defines the Diffies-Hellman group.	Select the perfect forward Secrecy key from the list.
policy > Proposals		
Proposals	Specifies the members added as proposals.	Select the proposals from the nonmembers list. Then click Add to move them to the members list.

Configuring Traceoptions (NSM Procedure)

To configure traceoptions:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the traceoptions.
3. Click the **Configuration** tab. In the configuration tree, select **Security > IPsec > Traceoptions**.
4. Add or modify settings as specified in [Table 240 on page 416](#).
5. Enter a comment in the Traceoptions workspace that describes the traceoptions.
6. In the **Configuration** tab. In the configuration tree, select **Security > IPsec > Traceoptions > Flag**.
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the traceoptions.

Table 240: Traceoptions Configuration Details

Option	Function	Your Action
Name	Specifies the trace flag name.	Select a name from the list.
Comment	Supplies a descriptive comment for the trace flag.	Enter a comment.

Configuring a VPN (NSM Procedure)

To configure a VPN:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure a VPN.
3. Click the **Configuration** tab. In the configuration tree, select **Security > IPsec > Vpn**.

4. Add or modify settings as specified in [Table 241 on page 417](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the VPN settings.

Table 241: VPN Configuration Details

Option	Function	Your Action
vpn		
Name	Specifies the VPN name.	Enter a name.
Comment	Supplies a descriptive comment for the VPN.	(Optional) Enter a comment.
Bind Interface	Specifies the bind to tunnel interface (route-based VPN).	Enter the interface name.
Df Bit	Specifies how to handle the don't fragment bit.	Select the option from the list.
Establish Tunnels	Defines the criteria to establish tunnels.	Select the option from the list.
vpn > Manual > manual > Authentication		
Comment	Supplies a descriptive comment for the authentication option.	(Optional) Enter a comment.
Algorithm	Defines the authentication algorithm.	Select the Algorithm from the drop-down box.
vpn > Manual > manual > Authentication > Key		
Comment	Specifies a descriptive comment for the authentication key.	(Optional) Enter a comment.
vpn > Manual > manual > Authentication > Key > Ascii Text		
None	Specifies that neither the ascii-text nor the hexadecimal key is enabled.	Select the option.
ascii-text	Enables the ASCII text key.	Select the option and enter the ASCII text key.
hexadecimal	Enables the hexadecimal text key.	Select the option and enter the hexadecimal text key.
vpn > Manual > manual > Encryption		
Comment	Supplies a descriptive comment for the encryption option.	(Optional) Enter a comment.

Table 241: VPN Configuration Details (*continued*)

Option	Function	Your Action
Algorithm	Defines the encryption algorithm.	Select the Algorithm from the list.
vpn > Manual > manual > Encryption > Key		
Comment	Specifies a descriptive comment for the encryption key.	(Optional) Enter a comment.
vpn > Manual > manual > Encryption > Key > Ascii Text		
None	Specifies that neither the ascii-text or hexadecimal key is enabled.	Select the option.
ascii-text	Enables the ASCII text key.	Select the option and enter the ASCII text key.
hexadecimal	Enables the hexadecimal text key.	Select the option and enter the hexadecimal text key.
vpn > Manual > ike		
Comment	Specifies a descriptive comment for the IKE.	Enter a comment.
Gateway	Specifies the remote gateway name.	Select the gateway from the list.
Idle Time	Specifies the idle time to remove Secure Authentication (SA).	Set the idle time. Range: 60 - 999999.
No Anti Replay	Disable the snit-reply check.	Select the No Anti Replay check box.
IPsec Policy	Specifies the name of the IPsec policy.	Select the IPsec policy from the list.
Install Interval	Delays the installation of re-entered outbound SAs on the initiator.	Set the duration of the installation. Range: 1 - 10.
vpn > Manual > ike > Proxy identity		
Enable Feature	Enables the proxy identity feature.	Select the Enable Feature check box to enable this feature.
Comment	Specifies a descriptive comment for the proxy identity option.	(Optional) Enter a comment.
Local	Specifies the local IP address.	Enter the IP address.
Remote	Specifies the remote IP address.	Enter the IP address.
Service	Specifies the name of the service.	Select the service from the list.
vpn > Vpn Monitor		

Table 241: VPN Configuration Details (*continued*)

Option	Function	Your Action
Enable Feature	Allows to configure Vpn monitor.	Select the Enable Feature check box to enable this feature.
Comment	Specifies a descriptive comment for the VPN monitor.	(Optional) Enter a comment.
Optimized	Specifies that the VPN monitor is optimized for scalability.	Select the Optimized check box to enable this feature.
Source Interface	Specifies source interface for monitor messages.	Enter the source interface.
Destination IP	Specifies destination IP address for monitor messages.	Enter the destination IP address.

Configuring VPN Monitor Options (NSM Procedure)

To configure VPN monitor options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the VPN monitor options.
3. Click the **Configuration** tab. In the configuration tree, select **Security > IPsec > Vpn Monitor Options**.
4. Select the **Enable Feature** check box from the Vpn Monitor Options workspace.
5. Add or modify settings as specified in [Table 242 on page 419](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the VPN monitor options.

Table 242: VPN Monitor Options Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the for the VPN monitor options.	Enter a comment.
Interval	Specifies (in seconds) the duration of monitoring interval.	Set the interval duration. Range: 1 - 3600.
Threshold	Specifies the number of consecutive failures to determine connectivity.	Set the threshold to determine connectivity. Range: 1 - 65536.

Related Documentation • [Configuring IKE \(NSM Procedure\) on page 407](#)

- [Configuring Forwarding Options \(NSM Procedure\) on page 406](#)
- [Configuring a Flow \(NSM Procedure\) on page 399](#)

Configuring a PKI (NSM Procedure)

The Public Key Infrastructure (PKI) feature allows you to configure automatic re-enrollment, Certificate Authority (CA) certificate, CA profile, certificate revocation list (CRL), local certificate, and traceoptions.

To configure the PKI feature:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the PKI feature.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Pki**.
4. Select the **Enable Feature** check box to enable this feature.
5. Enter a comment in the Pki workspace that describes the PKI.
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the PKI parameters.

You can now configure the following options:

- [Configuring Auto Re-enrollment \(NSM Procedure\) on page 420](#)
- [Configuring a CA Profile \(NSM Procedure\) on page 421](#)
- [Configuring Traceoptions \(NSM Procedure\) on page 423](#)

Configuring Auto Re-enrollment (NSM Procedure)

To configure the auto re-enrollment feature:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the auto re-enrollment feature.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Pki > Auto Re Enrollment**.
4. Enter a comment in the Auto Re Enrollment workspace that describes the auto re-enrollment feature.
5. In the configuration tree, select **Security > Pki > Auto Re Enrollment > Certificate Id**.
6. Add or modify settings as specified in [Table 243 on page 421](#).
7. Click one:

- **OK**—Saves the changes.
- **Cancel**—Cancels the modifications.
- **Apply**—Applies the auto re-enrollment parameters.

Table 243: Auto Re-enrollment Configuration Details

Option	Function	Your Action
Name	Specifies the name of the certificate ID.	Enter the name of the certificate ID.
Comment	Specifies a descriptive comment for the certificate ID.	Enter a comment.
Ca Profile Name	Specifies the name of the CA profile.	Select the CA profile name from the list.
Challenge Password	Specifies the password used by the CA for enrollment and revocation.	Enter the password.
Re Enroll Trigger Time Percentage	Specifies (in percentage) the re-enrollment trigger time before the expiration.	Set the re-enrollment trigger time. Range: 1 - 99.
Re Generate Keypair	Generates a new key pair for an auto re-enrollment.	Select the Re Generate Keypair check box to enable this feature.

Configuring a CA Profile (NSM Procedure)

The CA Profile feature allows you to configure the administrator, enrollment and revocation list.

To configure the CA profile:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the CA profile.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Pki > Ca Profile**.
4. Add or modify settings as specified in [Table 244 on page 421](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the CA profile parameters.

Table 244: CA Profile Configuration Details

Option	Function	Your Action
ca-profile		
Name	Specifies the name of the CA profile.	Enter the name of the CA profile.

Table 244: CA Profile Configuration Details (*continued*)

Option	Function	Your Action
Comment	Supplies a descriptive comment for the CA profile.	(Optional) Enter a comment.
Ca Identity	Specifies the CA identifier.	Enter the CA identifier.
ca-profile > Administrator		
Comment	Supplies a descriptive comment for the CA profile administrator.	(Optional) Enter a comment.
Email Address	Specifies the administrators email address where the certificate requests are sent.	Enter the e-mail address.
ca-profile > Enrollment		
Comment	Supplies a descriptive comment for the CA profile enrollment.	(Optional) Enter a comment.
Url	Specifies the enrollment URL of the certificate CA.	Enter the enrollment URL of the certificate CA.
Retry	Specifies (in seconds) the number of permissible enrollment retry attempts before terminating.	Set the permissible retry attempts. Range: 0 - 1080.
Retry Interval	Specifies the amount of time between enrollment retries.	Set the enrollment retry interval. Range: 0 - 3600.
ca-profile > Revocation Check		
Comment	Supplies a descriptive comment for the revocation check.	(Optional) Enter a comment.
Disable	Disables a revocation check.	Select the Disable check box to disable this feature.
ca-profile > Revocation Check > Crl		
Comment	Supplies a descriptive comment for the CRL.	(Optional) Enter a comment.
Refresh Interval	Specifies the CRL refresh interval.	Set the CRL refresh interval. Range: 0 through 8784.
ca-profile > Revocation Check > Crl > Disable		
Comment	Supplies a descriptive comment for disabling the CRL.	(Optional) Enter a comment.
On Download Failure	Disables the revocation check for the CRL download failure.	Select the On Download Failure check box to enable this feature.
ca-profile > Revocation Check > Crl > Url		

Table 244: CA Profile Configuration Details (*continued*)

Option	Function	Your Action
Name	Specifies the URL or CRL distribution point for the CA.	Enter the URL or CRL distribution point for the CA.
Comment	Supplies a descriptive comment for the URL or CRL distribution point for CA.	Enter a comment. (Optional)
Password	Specifies the password for authentication with the server.	Enter the password.

Configuring Traceoptions (NSM Procedure)

The traceoptions feature allows you to configure the file and the flag options.

To configure traceoptions:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the traceoptions.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Pki > Traceoptions**.
4. Configure the options as specified in [Table 245 on page 423](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the traceoptions settings.

Table 245: Traceoptions Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the traceoptions.	(Optional) Enter a comment.
No Remote Trace	Disables remote tracing.	Select the No Remote Trace check box to enable this feature.

You can now configure the following options:

- [Configuring the File Options \(NSM Procedure\) on page 424](#)
- [Configuring Flag Options \(NSM Procedure\) on page 424](#)

Configuring the File Options (NSM Procedure)

To configure the file options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the file options.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Pki > Traceoptions > File**.
4. Configure the file options as specified in [Table 246 on page 424](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the file settings.

Table 246: File Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the filename.	Enter a comment.
Filename	Specifies the filename to write the traceoptions.	Enter a filename.
Size	Specifies the maximum size of the trace file.	Enter the maximum file size.
Files	Specifies the maximum number of trace files.	Set the maximum number of trace files. Range: 2 through 1000.
None	Specifies that neither the world-readable nor the no-world-readable option is enabled.	Select the option.
world-readable	Allows any user to read the log file.	(Optional) Select the option.
no-world-readable	Prevents any user from reading the log file.	(Optional) Select the option.
Match	Specifies the regular expression for the lines to be logged.	Enter the match expression.

Configuring Flag Options (NSM Procedure)

To configure flag options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the flag options.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Pki > Traceoptions > Flag**.

4. Add or modify settings as specified in [Table 247 on page 425](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the flag settings.

Table 247: Flag Configuration Details

Option	Function	Your Action
Name	Specifies the trace flag name.	Select a name from the list.
Comment	Supplies a descriptive comment for the trace flag.	Enter a comment.



NOTE: You can also configure CA Certificates, CRLs, and Local Certificates in PKI configuration.

Related Documentation

- [Configuring IPsec \(NSM Procedure\) on page 414](#)
- [Configuring IKE \(NSM Procedure\) on page 407](#)
- [Configuring NAT \(NSM Procedure\)](#)

CHAPTER 23

Configuration of Services

- [Configuring Adaptive Services PICs \(NSM Procedure\) on page 427](#)
- [Configuring Border Signaling Gateways \(NSM Procedure\) on page 428](#)
- [Configuring Class of Service \(NSM Procedure\) on page 447](#)
- [Configuring Intrusion Detection Service \(NSM Procedure\) on page 450](#)
- [Tracing Services PIC Operations \(NSM Procedure\) on page 454](#)
- [Configuring Network Address Translation \(NSM Procedure\) on page 455](#)
- [Configuring PGCP \(NSM Procedure\) on page 460](#)
- [Configuring Service Interface Pools \(NSM Procedure\) on page 490](#)
- [Configuring Stateful Firewall \(NSM Procedure\) on page 491](#)
- [Configuring a Service Set \(NSM Procedure\) on page 493](#)
- [Configuring Captive Portal \(NSM Procedure\) on page 497](#)
- [Configuring Mobile IP \(NSM Procedure\) on page 502](#)
- [Configuring RPM \(NSM Procedure\) on page 513](#)
- [Configuring Unified Access Control \(NSM Procedure\) on page 519](#)

Configuring Adaptive Services PICs (NSM Procedure)

The Adaptive Services (AS) and Multiservices PICs provide adaptive services interfaces, which allow you to coordinate multiple services on a single PIC by configuring a set of services and applications. The AS and Multiservices PICs offer a special range of services you configure in one or more service sets.

To configure adaptive services PICS in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services**.
4. Select **Adaptive Services**.
5. Add or modify the settings as specified in [Table 248 on page 428](#).
6. Click one:

- OK—To save the changes.
- Cancel—To cancel the modifications.

Table 248: Adaptive Services Pics Configuration Details

Task	Your Action
Configure adaptive services or Multiservices PIC tracing operations.	<ol style="list-style-type: none"> 1. Click Traceoptions next to Adaptive Services Pics. 2. Select the No Remote Trace check box to disable remote tracing. 3. Expand Traceoptions. 4. Click File next to Trace Options. 5. In the Comment box, enter the comment. 6. In the Filename box, enter the name of the file to receive the output of the tracing operation. 7. In the Comment box, enter the comment. 8. In the Size box, enter the maximum size of each trace file in kilobytes (KB), megabytes (MB) or gigabytes (GB). Range: 2 through 1000 files Default: 3 files 9. From the Files list, select the maximum number of trace files. 10. Select one of the following: <ul style="list-style-type: none"> • no-world-readable—To allow any user to read the log file. • world-readable—To prevent any user from reading the log file. 11. Click Flag next to Trace Options. 12. Click Add new entry next to flag. 13. From the Name list, select a tracing operation to perform. 14. In the Comment box, enter the comment.

Related Documentation

- [Configuring Service Interface Pools \(NSM Procedure\)](#)
- [Configuring a Service Set \(NSM Procedure\) on page 493](#)
- [Tracing Services PIC Operations \(NSM Procedure\) on page 454](#)

Configuring Border Signaling Gateways (NSM Procedure)

You can configure border signaling gateways using this option. See the following topics:

- [Configuring Gateway Properties \(NSM Procedure\) on page 428](#)

Configuring Gateway Properties (NSM Procedure)

- [Configuring Gateway \(NSM Procedure\) on page 429](#)
- [Configuring an Admission Controller \(NSM Procedure\) on page 429](#)
- [Configuring Session Policy Decision Function \(NSM Procedure\) on page 430](#)

- [Configuring Service Point \(NSM Procedure\) on page 432](#)
- [Configuring SIP Policies and Timers \(NSM Procedure\) on page 433](#)
- [Configuring Traceoptions \(NSM Procedure\) on page 443](#)

Configuring Gateway (NSM Procedure)

To configure a gateway in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Services > Border Signaling Gateway**.
4. Select **Gateway**.
5. Add or modify settings as specified in [Table 249 on page 429](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 249: Gateway Configuration Details

Task	Your Action
Configure a gateway.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. In the Name box, enter the identifier for the BSG. 3. In the Comment box, enter the comment. 4. From the Service Interface list, select the name and logical unit number of the Multiservices PIC or DPC.

Configuring an Admission Controller (NSM Procedure)

To configure an admission controller in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Services > Border Signaling Gateway**.
4. Select **Gateway**.
5. Add or modify settings as specified in [Table 250 on page 430](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.



NOTE: For devices running Junos OS Release 9.5 and later, admission controller settings will be available in the device editor only when the policy-management mode is in the in-device mode. By default, admission controller settings can be created only in the Policy Manager and Object Manager.

Table 250: Admission Controller Configuration Details

Task	Your Action
Configure an admission controller for a border signaling gateway (BSG).	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click Admission Controller next to gateway. 3. In the Name box, enter the identifier for the BSG. 4. In the Comment box, enter the comment. 5. From the Service Interface list, select the name and logical unit number of the Multiservices PIC or DPC. 6. Click Admission Control next to gateway. 7. Click Add new entry next to Admission Control. 8. In the Name box, enter the name of the admission controller. 9. In the Comment box, enter the comment.
Configure admission control settings for dialogs.	<ol style="list-style-type: none"> 1. Click Dialogs next to admission-control. 2. From the Maximum Concurrent list, select the maximum number of concurrent dialogs. 0 causes all calls to be rejected. Range: 0 through 100,000 3. From the Committed Attempts Rate list, select the maximum number of attempts per second to initiate a dialog. Range: 0 through 100 4. From the Committed Burst Rate list, select the maximum number of dialogs allowed to burst above the committed rate and still be accepted.
Configure admission control settings for out-of-dialog transactions.	<ol style="list-style-type: none"> 1. Click Transactions next to admission-control. 2. From the Maximum Concurrent list, select the maximum number of concurrent transactions. 0 causes all calls to be rejected. Range: 0 through 50000 3. From the Committed Attempts Rate list, select the maximum number of attempts per second to initiate an out-of-dialog transaction. Range: 0 through 1500 4. From the Committed Burst Rate list, select the maximum number of transactions allowed to burst above the committed rate and still be accepted. Range: 0 through 3000

Configuring Session Policy Decision Function (NSM Procedure)

To configure session policy decision function in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Services > Border Signaling Gateway**.
4. Select **Gateway**.
5. Add or modify settings as specified in [Table 251 on page 431](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 251: Session Policy Decision Configuration Details

Task	Your Action
Configure the SPDF.	<ol style="list-style-type: none">1. Click Add new entry next to Gateway.2. Click Embedded Spdf next to gateway.3. In the Comment box, enter the comment.
Configure service classes for the embedded SPDF.	<ol style="list-style-type: none">1. Click Service Class next to Embedded Spdf.2. From the Service Interface list, select the name and logical unit number of the Multiservices PIC or DPC.3. Click Add new entry next to Service Class.4. In the Name box, enter the identifier for the service class.5. In the Comment box, enter the comment.

Table 251: Session Policy Decision Configuration Details (*continued*)

Task	Your Action
Specify the service class term properties.	<ol style="list-style-type: none"> 1. Click Term next to service-class. 2. Click Add new entry next to Term. 3. In the Name box, enter the identifier for the term. 4. In the Comment box, enter the comment. 5. Click From next to term. 6. In the Comment box, enter the comment. 7. Click Media Type next to From. 8. Click Add new entry next to Media Type. 9. In the New media-type window, select the type of media that the service class matches. <ul style="list-style-type: none"> • any-media—Match all media types. • audio—Match audio traffic. • video—Match video traffic. 10. Click Then next to term. 11. In the Comment box, enter the comment. 12. Select the Reject check box to not accept the traffic and return a rejection message. 13. From the Committed Information Rate list, select the maximum bandwidth that can be allocated to a packet that is flowing under normal line conditions. Range: 0 through 2147483647 14. From the Committed Burst Size list, select the maximum number of bytes allowed for incoming packets to burst above the committed information rate. Range: 20 through 2147483647 15. From the Dscp list, select the values for DSCP marking that the BSG uses for traffic that matches the service class term. Default: be

Configuring Service Point (NSM Procedure)

To configure session policy decision function in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Services > Border Signaling Gateway**.
4. Select **Gateway**.
5. Add or modify settings as specified in [Table 252 on page 433](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 252: Service Point Configuration Details

Task	Your Action
Configure a service point.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click Service Point next to gateway. 3. Click Add new entry next to Service Point. 4. In the Name box, enter the name. 5. In the Comment box, enter the comment. 6. From the Service Point Type list, select the type of VoIP protocol for this service point. Values: sip 7. From the Service Interface list, select the name of the service interface. 8. From the Default Media Realm list, select the realm number used to match to a virtual interface Range: 0 through 1023
Configure service classes for the embedded SPDF.	<ol style="list-style-type: none"> 1. Click Service Class next to Embedded Spdf. 2. From the Service Interface list, select the name and logical unit number of the Multiservices PIC or DPC. 3. Click Add new entry next to Service Class. 4. In the Name box, enter the identifier for the service class. 5. In the Comment box, enter the comment.
Assign new call usage policies or policy sets to the service point.	<ol style="list-style-type: none"> 1. Click Service Policies next to service-point. 2. In the Comment box, enter the comment. 3. Click New Call Usage Policies next to Service Policies. 4. Click Add new entry next to New Call Usage Policies. 5. In the New new-call-usage-policies window, enter the names of new call usage policies or policy sets. Syntax: If you specify more than one policy or policy set, you must enclose all policy names in brackets. 6. Click New Transaction Policies next to Service Policies. 7. Click Add new entry next to New Transaction Policies. 8. In the New new-transaction-policies window, enter the names of new call usage policies or policy sets. Syntax: If you specify more than one policy or policy set, you must enclose all policy names in brackets. 9. Click Transport Details next to service-point. 10. In the Comment box, enter the comment. 11. From the Port Number list, select the port number. 12. In the IP Address box, enter the IP address. 13. Select the corresponding transport protocol.

Configuring SIP Policies and Timers (NSM Procedure)

See the following topics:

- [Configuring Message Manipulation Rules \(NSM Procedure\) on page 434](#)
- [Configuring New Call Usage Policy \(NSM Procedure\) on page 435](#)

- [Configuring New Call Usage Policy Set \(NSM Procedure\) on page 438](#)
- [Configuring New Transaction Policy \(NSM Procedure\) on page 439](#)
- [Configuring a New Transaction Policy Set \(NSM Procedure\) on page 441](#)
- [Configuring Timers \(NSM Procedure\) on page 442](#)

Configuring Message Manipulation Rules (NSM Procedure)

To configure message manipulation rules in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Services > Border Signaling Gateway**.
4. Select **Gateway**.
5. Add or modify settings as specified in [Table 253 on page 434](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 253: Message Manipulate Rules Configuration Details

Task	Your Action
Configure a message manipulation rule.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click Sip next to gateway. 3. In the Comment box, enter the comment. 4. Click Message Manipulation Rules next to Sip. 5. In the Comment box, enter the comment.
Configure a manipulation rule.	<ol style="list-style-type: none"> 1. Click Manipulation Rule next to Message Manipulation Rules. 2. Click Add new entry next to Manipulation Rule. 3. In the Name box, enter the name of the manipulation rule. 4. In the Comment box, enter the comment. 5. Click Actions next to manipulation-rule. 6. In the Comment box, enter the comment. 7. Click Request Uri next to Actions. 8. In the Comment box, enter the comment. 9. Click Field Value next to Request Uri. 10. In the Comment box, enter the comment. 11. Click Modify Regular Expression next to Field Value. 12. Click Add new entry next to Modify Regular Expression. 13. In the Name box, enter the regular expression that you want to modify. 14. In the Comment box, enter the comment. 15. In the With box, enter the regular expression that you want to modify followed by the value with which you want to replace the regular expression.

Table 253: Message Manipulate Rules Configuration Details (*continued*)

Task	Your Action
Configure Session Initiation Protocol (SIP) header.	<ol style="list-style-type: none"> 1. Click Sip Header next to manipulation-rule. 2. Click Add new entry next to Sip Header. 3. In the Name box, enter the name of the header field in SIP headers for which you want to define field values. 4. In the Comment box, enter the comment. 5. Click Field Value next to sip-header. 6. In the Comment box, enter the comment. 7. Select the Remove All check box to remove all instances of the header field. 8. Click Add next to Field Value. 9. Select from the following field values: <ul style="list-style-type: none"> • Add—Adds an instance of the header field with the field value that you define. If the header field already exists, the software creates a new instance of the header field and inserts it before any existing instance of the header field. Having more than one field value is not allowed for some header fields. • Add Missing—Adds a new header field with the field value that you define if the header field is missing from the SIP header. • Add Overwrite—Adds a new header field with the field value that you define if the header field is missing from the SIP header. If the header field already exists, its field value is overwritten with the new field value. The software overwrites the field value in all instances of the header field. • Modify Regular Expression—Changes the value of a regular expression. • Reject Regular Expression—Rejects SIP messages and terminates the usage that the message is part of if the header field contains the regular expression. • Remove Regular Expression—Removes all of the header fields that have field values that match this regular expression. 10. Enter the Name and Comment.

Configuring New Call Usage Policy (NSM Procedure)

To configure new call usage policy in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Services > Border Signaling Gateway**.
4. Select **Gateway**.
5. Add or modify settings as specified in [Table 254 on page 436](#).
6. Click one:
 - **OK**—Saves the changes.

- **Cancel**—Cancels the modifications.

Table 254: New Call Usage Policy Configuration Details

Task	Your Action
Configure a new call usage policy.	<ol style="list-style-type: none">1. Click Add new entry next to Gateway.2. Click Sip next to gateway.3. In the Comment box, enter the comment.4. Click New Call Usage Policy next to Sip.5. Click Add new entry next to New Call Usage Policy.6. In the Name box, enter the identifier for the new call usage policy.7. In the Comment box, enter the comment.
Define the new call usage policy term properties.	<ol style="list-style-type: none">1. Click Term next to new-call-usage-policy.2. Click Add new entry next to Term.3. In the Name box, enter the identifier for the term.4. In the Comment box, enter the comment.

Table 254: New Call Usage Policy Configuration Details (*continued*)

Task	Your Action
Configure match conditions for a new call usage policy.	<ol style="list-style-type: none"> 1. Click From next to term. 2. In the Comment box, enter the comment. 3. Click Add new entry next to Term. 4. In the Name box, enter the identifier for the term. 5. Click Contact next to From. 6. Click Add new entry next to Contact. 7. In the Comment box, enter the comment. 8. Click Regular Expression next to contact. 9. Click Add new entry next to Regular Expression. 10. In the New regular-expression window, enter the regular expression used to match the contents of the contact field. Syntax: To specify more than one regular expression, enclose the regular expressions in brackets. 11. Click Method next to From. 12. Click Add new entry next to Method. 13. From the Name list, select method-invite to match the policy to SIP INVITE methods. 14. In the Comment box, enter the comment. 15. Click Request Uri next to From. 16. Click Add new entry next to Request Uri. 17. In the Comment box, enter the comment. 18. Click Regular Expression next to request-uri. 19. In the New regular-expression window, enter the regular expression used to match the contents of the request URI field. Syntax: To specify more than one regular expression, enclose the regular expressions in brackets. 20. Click Source Address next to From. 21. Click Add new entry next to Source Address. 22. In the New source-address window, enter the IP addresses that you want to match. Syntax: To specify more than one IP address, enclose the IP addresses in brackets.

Table 254: New Call Usage Policy Configuration Details (*continued*)

Task	Your Action
Define the actions performed on incoming requests that match the new call usage policy.	<ol style="list-style-type: none"> 1. Click Then next to From. 2. In the Comment box, enter the comment. 3. Select one of the following check boxes: <ul style="list-style-type: none"> • accept—To accept the traffic and send it to its destination. • reject—To reject the traffic and return a rejection message. Rejected traffic can be logged or sampled. • trace—To trace messages accepted by this policy. 4. Click Media Policy next to Then. 5. In the Comment box, enter the comment. 6. Select the No Anchoring check box to disable or enable media anchoring for the policy. 7. In the Service Class box, enter the name of the service class to be applied to traffic that matches the new call usage policy. 8. Click Data Inactivity Detection next to Media Policy. 9. In the Comment box, enter the comment. 10. From the Inactivity Duration list, select the time interval that determines inactivity. Range: 30 through 3600

Configuring New Call Usage Policy Set (NSM Procedure)

To configure new call usage policy set in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Services > Border Signaling Gateway**.
4. Select **Gateway**.
5. Add or modify settings as specified in [Table 255 on page 439](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 255: New Call Usage Policy Set Configuration Details

Task	Your Action
Configure a new call usage policy set.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click Sip next to gateway. 3. In the Comment box, enter the comment. 4. Click New Call Usage Policy Set next to Sip. 5. Click Add new entry next to New Call Usage Policy Set. 6. In the Name box, enter the identifier for the new call usage policy set. 7. In the Comment box, enter the comment.
Define the new call usage policies.	<ol style="list-style-type: none"> 1. Click Policy Name next to new-call-usage-policy-set. 2. Click Add new entry next to Policy Name. 3. In the New policy-name window, enter the names of one or more new call usage policies that you want to add to the set. Syntax: To specify a list of policies, enclose the policy names in brackets.

Configuring New Transaction Policy (NSM Procedure)

To configure new transaction policy in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Services > Border Signaling Gateway**.
4. Select **Gateway**.
5. Add or modify settings as specified in [Table 256 on page 440](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.



NOTE: For devices running Junos OS Release 9.5 and later, new transaction policy settings will be available in the device editor only when the policy-management mode is in-device mode. By default, new transaction policy settings can be created only in the Policy Manager and Object Manager.

Table 256: Transaction Policy Configuration Details

Task	Your Action
Configure new transaction policy.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click Sip next to gateway. 3. In the Comment box, enter the comment. 4. Click New Transaction Policy next to Sip. 5. Click Add new entry next to New Call Transaction Policy. 6. In the Name box, enter the identifier for the new transaction policy. 7. In the Comment box, enter the comment.
Define the new transaction policy term properties.	<ol style="list-style-type: none"> 1. Click Term next to new-transaction-policy. 2. Click Add new entry next to Term. 3. In the Name box, enter the identifier for the term. 4. In the Comment box, enter the comment.
Configure match conditions for a new transaction policy.	<ol style="list-style-type: none"> 1. Click From next to term. 2. In the Comment box, enter the comment. 3. Click Add new entry next to Term. 4. In the Name box, enter the identifier for the term. 5. Click Contact next to From. 6. Click Add new entry next to Contact. 7. In the Comment box, enter the comment. 8. Click Regular Expression next to contact. 9. Click Add new entry next to Regular Expression. 10. In the New regular-expression window, enter the regular expression used to match the contents of the contact field. Syntax: To specify more than one regular expression, enclose the regular expressions in brackets. 11. Click Method next to From. 12. Click Add new entry next to Method. 13. From the Name list, select the type of SIP method. 14. In the Comment box, enter the comment. 15. Click Request Uri next to From. 16. Click Add new entry next to Request Uri. 17. In the Comment box, enter the comment. 18. Click Regular Expression next to request-uri. 19. In the New regular-expression window, enter the regular expression used to match the contents of the request URI field. Syntax: To specify more than one regular expression, enclose the regular expressions in brackets. 20. Click Source Address next to From. 21. Click Add new entry next to Source Address. 22. In the New source-address window, enter the IP addresses that you want to match. Syntax: To specify more than one IP address, enclose the IP addresses in brackets.

Table 256: Transaction Policy Configuration Details (*continued*)

Task	Your Action
Define the actions performed on incoming requests that match this policy.	<ol style="list-style-type: none"> 1. Click Then next to From. 2. In the Comment box, enter the comment. 3. Select the following check boxes: <ul style="list-style-type: none"> • accept—To accept the traffic and send it to its destination • reject—To reject the traffic and return a rejection message. Rejected traffic can be logged or sampled. • trace—To trace messages accepted by this policy 4. In the Admission Control box, enter the controller name. 5. Click Message Manipulation next to Then. 6. In the Comment box, enter the comment. 7. Click Forward Manipulation next to Message Manipulation. 8. Click Add new entry next to Forward Manipulation. 9. In the Name box, enter the name of the forward message manipulation rules that you want to add to your new transaction policy. 10. In the Comment box, enter the comment. 11. Click Reverse Manipulation next to Message Manipulation. 12. Click Add new entry next to Reverse Manipulation. 13. In the Name box, enter the name of the reverse message manipulation rules that you want to add to your new transaction policy. 14. In the Comment box, enter the comment.
Configure the next-hop destination and egress service point for a new transaction policy.	<ol style="list-style-type: none"> 1. Click Route next to Then. 2. In the Comment box, enter the comment. 3. In the Egress Service Point box, enter the name of the service point that you want to use as the egress service point. 4. Click Next Hop next to Route. 5. In the Comment box, enter the comment. 6. Click Address next to Next Hop. 7. Select the SIP entity toward which SIP requests are sent. <ul style="list-style-type: none"> • address—To configure the destination IPv4 address of the next hop to contact <ol style="list-style-type: none"> a. In the Comment box, enter the comment. b. In the IPv4 Address box, enter the destination IPv4 address of the next hop to contact. c. From the Port list, select the destination port of the next hop to contact. Default: 5060 d. Click Transport protocol next to Address. e. In the Comment box, enter the comment. f. Select the transport protocol for routing to the next hop. • request-uri—To route all requests and responses on the dialog according to SIP.

Configuring a New Transaction Policy Set (NSM Procedure)

To configure a new transaction policy set in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Services > Border Signaling Gateway**.
4. Select **Gateway**.
5. Add or modify settings as specified in [Table 257 on page 442](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.



NOTE: For devices running Junos OS Release 9.5 and later, new transaction policy set settings will be available in the device editor only when the policy-management mode is in-device mode. By default, new transaction policy set settings can be created only in the Policy Manager and Object Manager.

Table 257: Transaction Policy Set Configuration Details

Task	Your Action
Configure a new transaction policy set.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click Sip next to gateway. 3. In the Comment box, enter the comment. 4. Click New Transaction Policy Set next to Sip. 5. Click Add new entry next to New Transaction Policy Set. 6. In the Name box, enter the identifier for the new transaction policy set. 7. In the Comment box, enter the comment.
Define the new transaction policies.	<ol style="list-style-type: none"> 1. Click Policy Name next to new-transaction-policy-set. 2. Click Add new entry next to Policy Name. 3. In the New policy-name window, enter the names of one or more new transaction policies that you want to add to the set. Syntax: To specify a list of policies, enclose the policy names in brackets.

Configuring Timers (NSM Procedure)

You can configure timers used to issue SIP timeouts using the Sip option:

To configure timers in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.

3. Click the **Configuration** tab. In the configuration tree, expand **Services > Border Signaling Gateway**.
4. Select **Gateway**.
5. Add or modify settings as specified in [Table 258 on page 443](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 258: Timers Configuration Details

Task	Your Action
Configure timers used to issue SIP timeouts.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click Sip next to gateway. 3. In the Comment box, enter the comment. 4. Click Timers next to Sip. 5. In the Comment box, enter the comment. 6. From the Inactive Call list, select the maximum time for signaling inactivity. Range: 300 through 86400 7. From the Timer C list, select the duration of the timeout period. Range: 180 through 300

Configuring Traceoptions (NSM Procedure)

You can configure border signaling gateway tracing operations using the Traceoptions option:

To configure traceoptions in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Services > Border Signaling Gateway**.
4. Select **Gateway**.
5. Add or modify settings as specified in [Table 259 on page 444](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 259: Traceoption BSG Configuration Details

Task	Your Action
Configure border signaling gateway (BSG) tracing operations.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click Traceoptions next to gateway. 3. Click Flag next to Traceoptions. 4. In the Comment box, enter the comment. 5. From the Minimum list, select the severity of the event being traced. <ul style="list-style-type: none"> • debug—Logging of all code flow of control. • trace—Logging of program trace for START, and EXIT macros. • info—Summary logs for normal operations. e.g. the policy decisions made for a call. • warning—Failure-recovery or failure of an external entity. • error—Failure with short-term effect, such as failed processing of a single call. 6. From the Session Trace list, select the minimum trace level for all session-trace messages.
Configure trace level options for the datastore component of the BSG.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click Traceoptions next to gateway. 3. Click Flag next to Traceoptions. 4. Click Datastore next to Flag. 5. In the Comment box, enter the comment. 6. From the Minimum list, select the minimum trace level for all datastore messages. 7. From the Data list, select the trace level for the data subcomponent. 8. From the Handle list, select the trace level for the access API for the database. 9. From the Db list, select the trace level for the wrapper layer around the database.

Table 259: Traceoption BSG Configuration Details (*continued*)

Task	Your Action
Configure trace options for the BSG component that provides an infrastructure that enables incremental functionality implementation.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click Traceoptions next to gateway. 3. Click Flag next to Traceoptions. 4. Click Framework next to Flag. 5. In the Comment box, enter the comment. 6. From the Minimum list, select the minimum trace level for all framework messages. 7. From the Executor list, select the trace level for the framework subcomponent that executes configured actions for an event, handles any error states, delays processing, and so on. 8. From the Action list, select the trace level for the framework subcomponent that creates, initiates, and manipulates event actions. 9. From the Event list, select the trace level for the framework subcomponent that creates, modifies, and terminates event members. 10. From the Freezer list, select the trace level for the framework subcomponent that delays the execution of an event until certain conditions are met. 11. From the Memory Pool list, select the trace level for the framework subcomponent that creates, deletes, and manipulates memory pools and pool managers, and controls the check-in to and check-out from memory pools of memory objects.
Configure trace options for the Signaling Border Controller (SBC) utilities component of the BSG.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click Traceoptions next to gateway. 3. Click Flag next to Traceoptions. 4. Click Sbc Utils next to Flag. 5. In the Comment box, enter the comment. 6. From the Minimum list, select the minimum trace level for all sbc-util messages. 7. From the Configuration list, select the trace level for the configuration component of SBC utilities. 8. From the IPC list, select the trace level for the IPC component of SBC utilities. 9. From the Device Monitor list, select the trace level for the device monitor component of SBC utilities. 10. From the Memory Management list, select the trace level for the memory management component of SBC utilities. 11. From the Message list, select the trace level for the message component of SBC utilities. 12. From the Common list, select the trace level for the common component of SBC utilities. 13. From the User Interface list, select the trace level for the user interface component of SBC utilities. 14. From the Memory Pool list, select the trace level for the message component of SBC utilities. 15. From the Memory Pool list, select the trace level for the memory pool component of SBC utilities.

Table 259: Traceoption BSG Configuration Details (*continued*)

Task	Your Action
Configure trace options for the signaling component of the BSG.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click Traceoptions next to gateway. 3. Click Flag next to Traceoptions. 4. Click Signaling next to Flag. 5. In the Comment box, enter the comment. 6. From the Minimum list, select the minimum trace level for all signaling messages. 7. From the Sip Stack Wrapper list, select the trace options for the glue layer that receives events from the SIP stack and forwards them to the application and, conversely, receives events from the application and forwards them to the SIP stack. 8. From the b2b Wrapper list, select the trace options for entry and exit to the BSG signaling application. 9. From the Ua list, select the trace options for the signaling subcomponent that handles RECEIVE messages. 10. From the B2b list, select the trace options for the signaling component that implements the b2b logic (translating between dialogs, associating dialogs, creating new downstream dialogs, and so on). 11. From the Topology Hiding list, select the trace options for the signaling component that hides the network topology of a network by CONTACT replacement and removal or modification of certain headers. 12. From the Policy list, select the trace options for the signaling component that applies policies for call admission, routing decisions, security settings, and so on.

Table 259: Traceoption BSG Configuration Details (*continued*)

Task	Your Action
Set trace options for the SIP stack component of the BSG.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click Traceoptions next to gateway. 3. Click Flag next to Traceoptions. 4. Click Sip Stack next to Flag. 5. In the Comment box, enter the comment. 6. Select the Event Tracing check box to activate or deactivate the stack's event tracing. 7. Select the Event Tracing check box to activate or deactivate the stack's event tracing. 8. Select the IPs Tracing check box to activate or deactivate the stack's IPS tracing. 9. Select the Per Tracing check box to activate or deactivate the stack's performance tracing. 10. Select the Dev Logging check box to configure development tracing for the stack. 11. Select the Verbose Logging check box to configure verbose tracing for the stack. 12. From the Pd Log Level list, select which types of PD logs are to be printed to the log file. Select one of the following: <ul style="list-style-type: none"> • problem—Problem log messages are sent to the log file. • exception—Exception and problem log messages are sent to the log file. • audit—All log messages are sent to the log file. 13. From the Pd Log Detail list, select the amount of detail to be sent to the log file. Select one of the following: <ul style="list-style-type: none"> • full—All available information is sent to the log file. • summary—The type of logging, the identifier and the first line of the log message are sent to the log file.

Configuring Class of Service (NSM Procedure)

The Class of Service (CoS) configuration available for the AS PIC enables you to configure Differentiated Services (DiffServ) code point (DSCP) marking and forwarding-class assignment for packets transiting the AS PIC.

To configure CoS in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > CoS**.
4. Add or modify the settings as specified in [Table 260 on page 448](#).
5. Click one:
 - **OK**—To save the changes.
 - **Cancel**—To cancel the modifications.

Table 260: CoS Configuration Details

Task	Your Action
Define a CoS application profile.	<ol style="list-style-type: none"> 1. Click Application profile next to CoS. 2. Click Add new entry next to Application Profile. 3. In the Name box, enter the profile name. 4. In the Comment box, enter the comment. 5. Expand application-profile. 6. Click Ftp next to application profile. 7. In the Comment box, enter the comment. 8. Expand Ftp. 9. Click Data next to Ftp. 10. In the Comment box, enter the comment. 11. In the Dscp box, enter the DSCP value or alias. 12. In the Forwarding Class box, enter the forwarding class. 13. Click Sip next to Ftp. 14. In the Comment box, enter the comment. 15. Expand Sip. 16. Click Video next to Sip. 17. In the Comment box, enter the comment. 18. In the Dscp box, enter the name assigned to a set of CoS markers. 19. In the Forwarding Class box, enter the name of the target application. 20. Click Voice next to Sip. 21. In the Comment box, enter the comment. 22. In the Dscp box, enter the DSCP mapping that is applied to the packets. 23. In the Forwarding Class box, enter the name of the target application.

Table 260: CoS Configuration Details (*continued*)

Task	Your Action
Specify the rule the router uses when applying this service.	<ol style="list-style-type: none"> Click Rule next to CoS. Click Add new entry next to rule. In the Name box, enter the rule the router uses when applying this service. In the Comment box, enter the comment. From the Match Direction list, select the direction in which the rule match is applied. <ul style="list-style-type: none"> input—Match on input to interface. output—Match on output from interface. input-output—Match on input to or output from interface. Expand rule. Click Term next to rule. Click Add new entry next to Term. In the Name box, enter the identifier for the term. In the Comment box, enter the comment. Expand term. Click From next to term. In the Comment box, enter the comment. Expand From. From the listed match conditions, select the ones that are applicable for CoS. The match conditions listed are Application Sets, Applications, Destination Address, Destination Address Range, Destination Prefix List, Source Address, Source Address Range, and Source Prefix List. Expand Then. Click Reflexive next to Then. Select one of the following: <ul style="list-style-type: none"> reflexive—To apply the equivalent opposing CoS action to flows in the opposite direction. reverse—To define the CoS behavior for flows in the reverse direction. <ol style="list-style-type: none"> In the Comment box, enter the comment. In the Dscp box, enter the DSCP mapping that is applied to the packets. In the Forwarding Class, enter the forwarding class to which packets are assigned From the Application Profile list, select the identifier for the application profile. Select the Syslog check box to enable system logging.

Table 260: CoS Configuration Details (*continued*)

Task	Your Action
Specify the rule set the router uses when applying this service.	<ol style="list-style-type: none"> 1. Click Rule-Set next to Cos. 2. Click Add new entry next to Rule-Set. 3. In the Name box, enter the identifier for the collection of rules that constitute this rule set. 4. In the Comment box, enter the comment. 5. Expand Rule-Set. 6. Click Rule next to rule-set. 7. Click Add new entry next to Rule. 8. From the Name list, select the identifier for the collection of terms that constitute this rule. 9. In the Comment box, enter the comment.

**Related
Documentation**

- [Configuring Service Interface Pools \(NSM Procedure\)](#)
- [Configuring a Service Set \(NSM Procedure\) on page 493](#)

Configuring Intrusion Detection Service (NSM Procedure)

The Adaptive Services (AS) or Multiservices PIC supports a limited set of intrusion detection services (IDS) to perform attack detection. IDS enables you to focus attack detection and remedial actions on specific hosts or networks that you specify in the IDS terms. Signature detection is not supported.

To configure IDS in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. Click the **Device** tree tab and then double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Ids**.
4. Add or modify the settings as specified in [Table 261 on page 451](#).
5. Click one:
 - **OK**—To save the changes.
 - **Cancel**—To cancel the modifications.

Table 261: IDS Configuration Details

Task	Your Action
Specify the rule the router uses when applying this service.	<ol style="list-style-type: none"> 1. Click Rule next to Ids. 2. Click Add new entry next to Rule. 3. In the Name box, enter the identifier for the collection of terms that constitute this rule. 4. In the Comment box, enter the comment. 5. From the Match Direction list, select the direction in which the rule match is applied. <ul style="list-style-type: none"> • input—To apply the rule match on input. • output—To apply the rule match on output. • input-output—To apply the rule match bidirectionally. 6. Expand rule. 7. Click Term next to rule. 8. Click Add new entry next to Term. 9. In the Name box, enter the Identifier for the term. 10. In the Comment box, enter the comment.
Specify input conditions for the IDS term.	<ol style="list-style-type: none"> 1. Expand term. 2. Click From next to term. 3. In the Comment box, enter the comment. 4. Expand From. 5. From the listed match conditions, select the ones that are applicable for Ids. The match conditions listed are Application Sets, Applications, Destination Address, Destination Address Range, Destination Prefix List, Source Address, Source Address Range, and Source Prefix List.
Define the IDS term actions.	<ol style="list-style-type: none"> 1. Click Then next to term. 2. In the Comment box, enter the comment. 3. Expand Then.

Table 261: IDS Configuration Details (*continued*)

Task	Your Action
Specify the type of data to be aggregated.	<ol style="list-style-type: none"> 1. Click Aggregation next to Then. 2. In the Comment box, enter the comment. 3. From the Source Prefix list, select the prefix value for source IPv4 address aggregation. Range: 1 through 32 4. From the Destination Prefix list, select the prefix value for destination IPv4 address aggregation. Range: 1 through 32 5. From the Source Prefix IPv6 list, select the prefix value for source IPv6 address aggregation. Range: 1 through 128. 6. From the Destination Prefix IPv6 list, select the prefix value for destination IPv6 address aggregation. Range: 1 through 128
Specify handling of entries in the IDS events cache.	<ol style="list-style-type: none"> 1. Click Force Entry next to Then. 2. Select one of the following: <ul style="list-style-type: none"> • force-entry—To ensure that the entry has a permanent place in the IDS cache after one event is registered. • ignore-entry—To ensure that all IDS events are ignored.
Set logging values for this IDS term.	<ol style="list-style-type: none"> 1. Click Logging next to Then. 2. In the Comment box, enter the comment. 3. From the Threshold list, select the logging threshold number of events per second. 4. Select the Syslog check box to enable system logging.

Table 261: IDS Configuration Details (*continued*)

Task	Your Action
Configuring session limit.	<ol style="list-style-type: none"> 1. Click Session Limit next to Then. 2. In the Comment box, enter the comment. 3. Expand Session Limit. 4. Click By Destination, By Source or By Pair next to Session Limit. 5. In the Comment box, enter the comment. 6. In the Maximum box, enter the maximum number of open sessions per IP address or subnet per application. Range: 1 through 32,767 7. In the Rate box, enter the maximum number of sessions per second per IP address or subnet per application. Range: 4 through 32,767 8. In the Packets box, enter the maximum peak packets per second per application or IP address. Range: 4 through 2147483647 9. From the Hold Time list, select the length of time for which to stop all new flows once the rate of events exceeds the threshold set by one or more of the maximum, packets, or rate statements. Range: 0 through 60
Enable SYN-cookie defenses against SYN attacks.	<ol style="list-style-type: none"> 1. Click Syn Cookie next to Then. 2. In the Comment box, enter the comment. 3. From the Threshold list, select the SYN-cookie defense number of SYN attacks per second. 4. From the Mss list, select the maximum segment size value used in TCP delayed binding. Default: 1500 Range: 128 through 8192
Specify the rule set the router uses when applying this service.	<ol style="list-style-type: none"> 1. Click Rule Set next to Ids. 2. Click Add new entry next to Rule Set. 3. In the Name box, enter the rule the router uses when applying this service. 4. In the Comment box, enter the comment. 5. Expand rule-set. 6. Click Rule next to rule-set. 7. Click Add new entry next to Rule. 8. In the Name box, enter the rule the router uses when applying this service. 9. In the Comment box, enter the comment.

- Related Documentation**
- [Configuring a Service Set \(NSM Procedure\) on page 493](#)
 - [Configuring Stateful Firewall \(NSM Procedure\) on page 491](#)

Tracing Services PIC Operations (NSM Procedure)

Tracing operations track all adaptive services operations and record them in a log file. The logged error descriptions provide detailed information to help you solve problems faster.

To configure tracing services PIC operations in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services**.
4. Select **Logging**.
5. Add or modify the settings as specified in [Table 262 on page 455](#).
6. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.

Table 262: Traceoptions Configuration Details

Task	Your Action
Configure Adaptive Services or Multiservices PIC tracing operations.	<ol style="list-style-type: none"> 1. Click Traceoptions next to Logging. 2. In the Comment box, enter the comment. 3. Select the No Remote Trace check box to disable remote tracing globally or for a specific tracing operation.
Specify the name of the file to receive the output of the tracing operation and specifies the maximum number of trace files.	<ol style="list-style-type: none"> 1. Click File next to Traceoptions. 2. In the Comment box, enter the comment for the file. 3. In the Filename box, enter the name of the file to receive the output of the tracing operation. 4. In the Size box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). 5. From the Files list, select the maximum number of trace files. Range: 2 through 1000 Default: 3 files 6. Select one of the following: <ul style="list-style-type: none"> • world-readable—To enable unrestricted file access. • no-world-readable—To restrict file access to owner. This is the default setting. 7. In the Match box, enter the regular expression.
Specify the tracing operation to perform. To specify more than one tracing operation, include multiple flag statements.	<ol style="list-style-type: none"> 1. Click Flag next to Traceoptions. 2. Click Add new entry next to Flag. 3. From the Name list, select the flag. 4. In the Comment box, enter the comment for the flag.

Related Documentation

- [Configuring Adaptive Services PICs \(NSM Procedure\) on page 427](#)
- [Configuring a Service Set \(NSM Procedure\) on page 493](#)
- [Configuring Service Interface Pools \(NSM Procedure\)](#)

Configuring Network Address Translation (NSM Procedure)

Network Address Translation (NAT) is a mechanism for concealing a set of host addresses on a private network behind a pool of public addresses. It can be used as a security measure to protect the host addresses from direct targeting in network attacks.

To configure NAT in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Nat**.
4. Add or modify the settings as specified in [Table 263 on page 457](#).
5. Click one:

- OK—To save the changes.
- Cancel—To cancel the modifications.

Table 263: NAT Configuration Details

Task	Your Action
Enable multicast filters on Ethernet interfaces when IPv6 NAT is used for neighbor discovery.	<ol style="list-style-type: none"> 1. Click IPv6 Multicast Interfaces next to Nat. 2. Click Add new entry next to IPv6 Multicast Interfaces. 3. From the Name list, select All to enable filters on all interfaces. 4. Select Interface name to enable filters on a specific interface only. 5. In the Comment box, enter the comment. 6. Select the Disable check box to disable filters on the specified interfaces.
Specify the NAT name and properties.	<ol style="list-style-type: none"> 1. Click Pool next to Nat. 2. Click Add new entry next to Pool. 3. In the Name box, enter the identifier for the Nat address pool. 4. In the Comment box, enter the comment. 5. Expand pool. 6. Click Address next to pool. 7. Click Add new entry next to Address. 8. In the Name box, enter an IPv4 or IPv6 prefix value. 9. In the Comment box, enter the comment.
Configure the NAT pool address range.	<ol style="list-style-type: none"> 1. Click Address Range next to pool. 2. Click Add new entry next to Address Range. 3. In the Low box, enter the lower boundary for the IPv4 or IPv6 address range. 4. In the High box, enter the upper boundary for the IPv4 or IPv6 address range. 5. In the Comment box, enter the comment.

Table 263: NAT Configuration Details (*continued*)

Task	Your Action
Configure Packet gateway Control Protocol (PGCP).	<ol style="list-style-type: none"> 1. Click Pgcp next to pool. 2. In the Comment box, enter the comment. 3. Click the Remotely Controlled check box to configure the addresses and ports in a NAT pool to be remotely controlled by the gateway controller. 4. From the Ports Per Session list, select the number of ports to be enabled. <p>NOTE: The ports per session should be either 2 or 4.</p> <ol style="list-style-type: none"> 5. Expand Pgcp. 6. Click Hint next to Pgcp. 7. Click Add new entry next to Hint. 8. In the dialog box, enter an alphanumeric string of up to 3 characters that the BGF uses to match with a termination hint located in the Direction field of a nonstandard termination ID.
Configure addresses and ports for use in NAT Rules.	<ol style="list-style-type: none"> 1. Click Port next to pool. 2. In the Comment box, enter the comment. 3. Expand Port. 4. Click Automatic next to Port. 5. Select one of the following: <ul style="list-style-type: none"> • automatic—To configure Router-assigned port. • range—To specify a range with minimum and maximum values. Range: 0 through 65535

Table 263: NAT Configuration Details (*continued*)

Task	Your Action
Specify the rule the router uses when applying this service.	<ol style="list-style-type: none"> 1. Click Rule next to Nat. 2. Click Add new entry next to Rule. 3. In the Name box, enter the Identifier for the collection of terms that comprise this rule. 4. In the Comment box, enter the comment. 5. From the Match Direction list, select the direction in which the rule match is applied. 6. Expand Rule. 7. Click Term next to Rule. 8. Click Add new entry next to Term. 9. In the Name box, enter the identifier for the term. 10. In the Comment box, enter the comment. 11. Expand term. 12. Click From next to term. 13. In the Comment box, enter the comment. 14. Expand From. 15. From the listed match conditions, select the ones that are applicable for Nat. The match conditions listed are Application Sets, Applications, Destination Address, Destination Address Range, Destination Prefix List, Source Address, Source Address Range, and Source Prefix List. 16. Click Then next to From. 17. Expand Then. 18. In the Comment box, enter the comment. 19. Select the Syslog check box to enable system logging. 20. Click No Translation next to Then. 21. Select one of the following: <ul style="list-style-type: none"> • no-translation—To specify that traffic is not to be translated. • translated—To define properties for translated traffic.

Table 263: NAT Configuration Details (*continued*)

Task	Your Action
Specify the rule set the router uses when applying this service.	<ol style="list-style-type: none"> 1. Click Rule Set next to Nat. 2. Click Add new entry next to Rule Set. 3. In the Name box, enter an identifier for the collection of rules that constitute this rule set. 4. In the Comment box, enter the comment. 5. Expand rule-set. 6. Click Rule next to rule-set. 7. Click Add new entry next to Rule. 8. From the Name list, select the identifier for the collection of terms that comprise this rule. 9. In the Comment box, enter the comment.

**Related
Documentation**

- [Configuring Adaptive Services PICs \(NSM Procedure\) on page 427](#)
- [Configuring Service Interface Pools \(NSM Procedure\)](#)
- [Configuring PGCP \(NSM Procedure\) on page 460](#)

Configuring PGCP (NSM Procedure)

You can use the Packet Gateway Control Protocol (PGCP) options to configure the Border Gateway Function. See the following topics:

- [Configuring Gateway \(NSM Procedure\) on page 461](#)
- [Configuring H248 Options Properties \(NSM Procedure\) on page 465](#)
- [Configuring H248 Properties \(NSM Procedure\) on page 471](#)
- [Configuring H248 Timers \(NSM Procedure\) on page 482](#)
- [Configuring the Monitor \(NSM Procedure\) on page 483](#)
- [Configuring Overload Control \(NSM Procedure\) on page 484](#)
- [Configuring Session Mirroring \(NSM Procedure\) on page 485](#)
- [Configuring Media Service \(NSM Procedure\) on page 485](#)
- [Configuring a Rule \(NSM Procedure\) on page 486](#)
- [Configuring Rule Set \(NSM Procedure\) on page 487](#)
- [Configuring Session Mirroring \(NSM Procedure\) on page 487](#)
- [Configuring Traceoptions \(NSM Procedure\) on page 488](#)
- [Configuring Virtual Interface \(NSM Procedure\) on page 489](#)

Configuring Gateway (NSM Procedure)

You can configure a virtual Border gateway Function (BGF) on the router by configuring gateway. See the following topics:

- [Configuring a Virtual Border Gateway Function on the Router \(NSM Procedure\) on page 461](#)
- [Configuring Data Inactivity Detection \(NSM Procedure\) on page 462](#)
- [Configuring Gateway Controller \(NSM Procedure\) on page 463](#)
- [Configuring Graceful Restart \(NSM Procedure\) on page 464](#)

Configuring a Virtual Border Gateway Function on the Router (NSM Procedure)

You can configure a virtual BGF on the router using the Gateway option.

To configure a virtual BGF on the router in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in [Table 264 on page 461](#).
6. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.

Table 264: Virtual BGF Configuration Details

Task	Your Action
Configure a virtual BGF on the router	<ol style="list-style-type: none"> 1. In the Name box, enter the identifier of the virtual BGF. 2. In the Comment box, enter the comment. 3. In the Gateway Address box, enter the IP address of the virtual BGF that you are configuring on the router. 4. From the Gateway Port list, select the port number of the virtual BGF that you are configuring on the router. Range: 0 through 65,535 5. From the Cleanup Timeout list, select the interval before inactivity detection starts. Range: 0 through 65,535 seconds 6. From the Service State list, select the service state of the virtual BGF. 7. From the Max Concurrent Calls list, select the Maximum number of concurrent calls on the virtual BGF. Range: 0 through 10,000

Configuring Data Inactivity Detection (NSM Procedure)

You can configure data inactivity detection to detect latch deadlocks or other media inactivity on a gate.

To configure data inactivity detection on the router in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in [Table 265 on page 463](#).
6. Click one:
 - **OK**—To save the changes.
 - **Cancel**—To cancel the modifications.

Table 265: Data Inactivity Detection Configuration Details

Task	Your Action
Configure data inactivity detection.	<ol style="list-style-type: none"> 1. Expand Gateway. 2. Click Data Inactivity Detection next to Gateway. 3. In the Comment box, enter the comment. 4. From the Inactivity Delay list, select the time interval before checking for media inactivity. Range: 0 through 3600 seconds Default: 5 5. From the Latch Deadlock delay list, select the time interval before checking for data packets. Range: 0 through 3600 seconds 6. Select the Send Notification on Delay check box to send an inactivity notification immediately when no media packets are detected during a delay period that precedes checking for media inactivity. 7. From the Inactivity Duration list, select the time during which no packets are received. Range: 5 through 86400 seconds Default: 30 8. Select the Stop Detection On Drop check box to configure the BGF to stop inactivity detection when a gate action is set to drop.
Change the service state of inactive terminations.	<ol style="list-style-type: none"> 1. Expand Data Inactivity Detection. 2. Click Report Service Change next to Data Inactivity Detection. 3. In the Comment box, enter the comment. 4. From the Service Change Type list, select the method and reason used in changing the service state of the termination to active in order to curtail sending of inactivity messages. <ul style="list-style-type: none"> • forced-906—if the service is to be terminated using a forced termination method with reason code 906 (loss of lower layer connectivity). • forced-910—if the service is to be terminated using a forced termination with reason code 910 (media capability failure).

Configuring Gateway Controller (NSM Procedure)

You can configure a gateway controller either as a remote controller or as a local controller. Configure the gateway controller as a remote controller if you are using an external gateway controller and configure the gateway controller as a local controller if you are using a border signaling gateway (BSG).

To configure gateway controller in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.

5. Add or modify the settings as specified in [Table 266 on page 464](#).
6. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.

Table 266: Gateway Controller Configuration Details

Task	Your Action
Configure a gateway controller.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click Gateway Controller next to gateway. 3. Click Add new entry next to Gateway Controller. 4. In the Name box, enter the name of the gateway controller or BSG. 5. In the Comment box, enter the comment. 6. In the Controller Address box, enter the IP address of the gateway controller. 7. From the Controller Port list, select the port number of the gateway controller. Range: 0 through 65535 8. Expand gateway-controller. 9. Click Interim Ah Scheme. 10. In the Comment box, enter the comment. 11. From the Algorithm list, select the algorithm used for the interim AH scheme. HMAC null is currently the only algorithm supported

Configuring Graceful Restart (NSM Procedure)

You can configure graceful restart properties that are used during synchronization between the pgcpd process and the Multiservices PIC or DPC.

To configure graceful restart in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in [Table 267 on page 465](#).
6. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.

Table 267: Graceful Restart Configuration Details

Task	Your Action
Configure graceful restart properties.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click Graceful Restart next to gateway. 3. In the Comment box, enter the comment. 4. From the Maximum Synchronization Time list, select the maximum time allowed for the synchronization procedure with the PIC or DPC. Range: 0 through 300 5. From the Maximum Synchronization Mismatches list, select the maximum number of mismatches allowed during the synchronization procedure with the PIC or DPC. Range: 0 through 20000 6. Select the No Synchronization check box to disable the synchronization procedure with the PIC.

Configuring H248 Options Properties (NSM Procedure)

You can configure properties for the H.248 options. See the following topics:

- [Configuring H248 Options \(NSM Procedure\) on page 465](#)
- [Changing Encoding Defaults \(NSM Procedure\) on page 466](#)
- [Configuring Service Change \(NSM Procedure\) on page 466](#)

Configuring H248 Options (NSM Procedure)

You can configure options that affect virtual BGF H.248 behavior.

To configure H248 options in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in [Table 268 on page 466](#).
6. Click one:
 - **OK**—To save the changes.
 - **Cancel**—To cancel the modifications.

Table 268: H248 Configuration Details

Task	Your Action
Configure options that affect virtual BGF H.248 behavior.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click H248 Options next to gateway. 3. In the Comment box, enter the comment. 4. Select the Audit Observed Events Returns option to enable a history of media inactivity events to be viewed by the gateway controller.

Changing Encoding Defaults (NSM Procedure)

You can change the encoding defaults using this option.

To configure encoding defaults in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in [Table 269 on page 466](#).
6. Click one:
 - OK—To save the changes
 - Cancel—To cancel the modifications

Table 269: Encoding Defaults Configuration Details

Task	Your Action
Change encoding defaults.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click H248 Options next to gateway. 3. Expand H248 Options. 4. Click Encoding next to H248 Options. 5. In the Comment box, enter the comment. 6. Select the No Dscp Bit Mirroring check box to disable mirroring of DSCP bits. 7. Select the Use Lower Case check box to configure upper-case encoding for H.248 messages.

Configuring Service Change (NSM Procedure)

Service change specifies the method and reason that the virtual BGF includes in ServiceChange commands that it sends to the gateway controller when the state of a control association, virtual interface, or context changes. See the following topics:

- [Configuring Context Indications \(NSM Procedure\) on page 467](#)
- [Configure Control Association Indications \(NSM Procedure\) on page 467](#)
- [Configuring Virtual Interface Indications \(NSM Procedure\) on page 470](#)

Configuring Context Indications (NSM Procedure)

Context indications specify the method and reason that the virtual BGF includes in Service-Interruption ServiceChange commands that it sends to the gateway controller when the gates of a context no longer provide their configured services. When the virtual BGF sends a Service-Interruption message, both terminations in the context become Out-of-Service.

To configure context indications in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in [Table 270 on page 467](#).
6. Click one:
 - **OK**—To save the changes.
 - **Cancel**—To cancel the modifications.

Table 270: Context indication Configuration Details

Task	Your Action
Configure context indications.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click H248 Options next to gateway. 3. Expand H248 Options. 4. Click Service Change next to H248 Options. 5. In the Comment box, enter the comment. 6. Select the Use Wildcard Response check box to enable the virtual BGF to issue service change commands as wildcard-response commands, which trigger a short response from the gateway controller. 7. Expand Service Change. 8. Click Context Indications next to Service Change. 9. In the Comment box, enter the comment. 10. From the State Loss list, select the method and reason that the virtual BGF includes in Service-Interruption ServiceChange commands that it sends to the gateway controller after a state loss on a specific context.

Configure Control Association Indications (NSM Procedure)

Specify the method and reason that the virtual BGF includes in ServiceChange commands that it sends to the gateway controller when the state of the control association changes.

To configure control associations indications in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.

3. In the **Configuration** tab, expand **Services**.
4. Select **Pgcp**.
5. Add or modify the settings as specified in [Table 271 on page 469](#).
6. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.

Table 271: Control Association Configuration Details

Task	Your Action
Specify the method and reason that the virtual BGF includes in Registration Request ServiceChange commands when it attempts to reregister with the gateway controller or register with a new gateway controller after the control association is disconnected.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click H248 Options next to gateway. 3. Expand H248 Options. 4. Click Service Change next to H248 Options. 5. Expand Service Change. 6. Click Control Association Indications next to Service Change. 7. In the Comment box, enter the comment. 8. Expand Control Association Indications. 9. Click Disconnect next to Control Association Indications. 10. In the Comment box, enter the comment. 11. From the Reconnect list, select the method and reason that the virtual BGF includes in Registration Request ServiceChange commands when it attempts to reregister with the gateway controller or register with a new gateway controller after the control association is disconnected. 12. From the Controller Failure list, select the method and reason that the virtual BGF includes in Registration Request ServiceChange commands when it attempts to reregister with the gateway controller or register with a new gateway controller after the control association is disconnected.
Specify the method and reason that the virtual BGF includes in Unregistration Messages in ServiceChange commands that it sends to the gateway controller when a control association transitions to Out-of-Service because of a failure.	<ol style="list-style-type: none"> 1. Click Down next to Control Association. 2. In the Comment box, enter the comment. 3. From the Administrative list, select the method and reason that the virtual BGF includes in Unregistration Messages in ServiceChange commands that it sends to the gateway controller when a control association transitions to Out-of-Service because of an administrative operation. 4. From the Failure list, select the method and reason that the virtual BGF includes in Unregistration or Notification Messages in ServiceChange commands when a control association transitions to Out-of-Service. 5. From the Graceful list, select the method and reason that the virtual BGF includes in Notification ServiceChange commands that it sends to the gateway controller when the control association transitions from In-Service to Out-of-Service-Graceful.

Table 271: Control Association Configuration Details (*continued*)

Task	Your Action
Specify the method and reason that the virtual BGF includes in Notification Messages or Registration commands in ServiceChange commands when a control association transitions to In-Service.	<ol style="list-style-type: none"> 1. Click Up next to Control Association. 2. In the Comment box, enter the comment. 3. From the Failover Cold list, select the method and reason that the virtual BGF includes in Registration ServiceChange commands when it attempts to register with a new gateway controller following a cold failover. 4. From the Failover Warm list, select the method and reason that the virtual BGF includes in Registration ServiceChange commands when it attempts to register with a new gateway controller following a warm failover. 5. From the Cancel Graceful list, select the method and reason that the virtual BGF includes in Notification ServiceChange commands that it sends to the gateway controller when the control association transitions from the Draining state to the Forwarding state.

Configuring Virtual Interface Indications (NSM Procedure)

Virtual interface indications specify the method and reason that the virtual BGF includes in ServiceChange commands that it sends to the gateway controller when the state of the virtual interface changes.

To configure virtual interface indications in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in [Table 272 on page 471](#).
6. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.

Table 272: Virtual Interface Indications Configuration Details

Task	Your Action
Specify the method and reason that the virtual BGF includes in ServiceChange commands that it sends to the gateway controller when the state of the virtual interface changes to Out-of-Service.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click H248 Options next to gateway. 3. Expand H248 Options. 4. Click Service Change next to H248 Options. 5. Expand Service Change. 6. Click Virtual Interface Indications next to Service Change. 7. In the Comment box, enter the comment. 8. Expand Virtual Interface Indications. 9. Click Virtual Interface Down next to Virtual Interface Indications. 10. In the Comment box, enter the comment. 11. From the Graceful list, select the method and reason that the virtual BGF includes in Notification ServiceChange commands that it sends to the gateway controller when the control association transitions from In-Service to Out-of-Service-Graceful. 12. From the Administrative list, select the method and reason that the virtual BGF includes in Unregistration Messages in ServiceChange commands that it sends to the gateway controller when a control association transitions to Out-of-Service because of an administrative operation. 13. From the Failure list, select the method and reason that the virtual BGF includes in Unregistration or Notification Messages in ServiceChange commands when a control association transitions to Out-of-Service. 14. From the Link Loss list, select the method and reason that the virtual BGF includes in Service-Interruption ServiceChange commands that it sends to the gateway controller when the virtual interface transitions to Out-of-Service because of a link loss.
Specifying the ServiceChange command that the virtual BGF sends to the gateway controller when the state of the virtual interface changes to In-Service.	<ol style="list-style-type: none"> 1. Click Virtual Interface Up next to Virtual Interface Indications. 2. In the Comment box, enter the comment. 3. From the Warm list, select the method and reason that the virtual BGF includes in Service-Restoration ServiceChange commands that it sends to the gateway controller when a virtual interface transitions to In-Service. 4. From the Cancel Graceful list, select the method and reason that the virtual BGF includes in Notification ServiceChange commands that it sends to the gateway controller when the control association transitions from the Draining state to the Forwarding state.

Configuring H248 Properties (NSM Procedure)

You can configure default values for H248 properties using the following options. See the following topics:

- [Configuring Application Data Inactivity Detection \(NSM Procedure\) on page 472](#)
- [Configuring Base Root \(NSM Procedure\) on page 472](#)
- [Configuring Differentiated Services \(NSM Procedure\) on page 475](#)

- [Configuring Event Timestamp Notification \(NSM Procedure\) on page 475](#)
- [Hanging Termination Detection \(NSM Procedure\) on page 476](#)
- [Configuring Inactivity Timer \(NSM Procedure\) on page 477](#)
- [Configuring Notification Behavior \(NSM Procedure\) on page 478](#)
- [Configuring Segmentation \(NSM Procedure\) on page 479](#)
- [Configuring Traffic Management \(NSM Procedure\) on page 480](#)

Configuring Application Data Inactivity Detection (NSM Procedure)

You can activate or deactivate regulated notification of media inactivity events.

To configure application data inactivity detection in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in [Table 273 on page 472](#).
6. Click one:
 - **OK**—To save the changes
 - **Cancel**—To cancel the modifications

Table 273: Data Inactivity Detection Configuration Details

Task	Your Action
Activate or deactivate regulated notification of media inactivity events.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click H248 Properties next to gateway. 3. In the Comment box, enter the comment. 4. Expand H248 Properties. 5. Click Application Data Inactivity Detection next to H248 Properties. 6. In the Comment box, enter the comment. 7. From the IP Flow Stop Detection list, select the regulated or non-regulated (immediate) notification of media inactivity events.

Configuring Base Root (NSM Procedure)

You can configure default values for properties in the base root package using the Base Root option:

To configure base root package in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.

3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in [Table 274 on page 474](#).
6. Click one:
 - **OK**—To save the changes.
 - **Cancel**—To cancel the modifications.

Table 274: Base Root Package Configuration Details

Task	Your Action
Set default, maximum, and minimum values for the MG originated pending limit property of the base root package.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click H248 Properties next to gateway. 3. Expand H248 Properties. 4. Click Base Root next to H248 Properties. 5. In the Comment box, enter the comment. 6. Expand Base Root. 7. Click Mg Originated Pending limit next to Base Root. 8. In the Comment box, enter the comment. 9. From the Default list, select the default number of transaction pending messages that the gateway controller can receive from the virtual BGF. <p>Range: 1 through 512</p>
Set default, maximum, and minimum values for the MG provisional response timer property of the base root package.	<ol style="list-style-type: none"> 1. Click Mg Provisional Response Value Timer next to Base Root. 2. In the Comment box, enter the comment. 3. From the Default list, select the default time within which the gateway controller waits for a pending response from the virtual BGF if a transaction cannot be completed. <p>Range: 500 through 3000 milliseconds</p>
Set default, maximum, and minimum values for the MGC originated pending limit property of the base root package.	<ol style="list-style-type: none"> 1. Click Mgc Originated Pending Limit next to Base Root. 2. In the Comment box, enter the comment. 3. From the Default list, select the default number of transaction pending messages that the virtual BGF can receive from the gateway controller. <p>Range: 1 through 512</p>
Set default, maximum, and minimum values for the MGC provisional response timer value property of the base root package.	<ol style="list-style-type: none"> 1. Click Mgc Provisional Response Timer Value next to Base Root. 2. In the Comment box, enter the comment. 3. From the Default list, select the default time within which the virtual BGF waits for a pending response from the gateway controller if a transaction cannot be completed. <p>Range: 500 through 3000 milliseconds</p>
Set default, maximum, and minimum values for the normal MG execution time property of the base root package.	<ol style="list-style-type: none"> 1. Click Normal Mg Execution Time next to Base Root. 2. In the Comment box, enter the comment. 3. From the Default list, select the default interval within which the gateway controller waits for a response to transactions from the virtual BGF. <p>Range: 500 through 29000 milliseconds</p>
Set default, maximum, and minimum values for the normal MGC execution time property of the base root package.	<ol style="list-style-type: none"> 1. Click Normal Mgc Execution Time next to Base Root. 2. In the Comment box, enter the comment. 3. From the Default list, select the default interval within which the virtual BGF waits for a response to transactions from the gateway controller. <p>Range: 500 through 29,000 milliseconds.</p>

Configuring Differentiated Services (NSM Procedure)

You can configure default values for properties in the Differentiated Services (DiffServ) package using the Diffserv option.

To configure DiffServ in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in [Table 275 on page 475](#).
6. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.

Table 275: DiffServ Configuration Details

Task	Your Action
Configure default values for properties in the Differentiated Services (DiffServ) package.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click H248 Properties next to gateway. 3. Expand H248 Properties. 4. Click Diffserv next to H248 Properties. 5. In the Comment box, enter the comment. 6. Click Dscp next to Diffserv. 7. In the Comment box, enter the comment. 8. From the Default list, select the default values for Differentiated Services Code Point (DSCP) marking that the virtual BGF uses for outgoing traffic when the DSCP value is not already defined by the gateway controller.

Configuring Event Timestamp Notification (NSM Procedure)

You can enable or disable the gateway controller to access timestamp information for media inactivity event notifications.

To configure event timestamp notification in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in [Table 276 on page 476](#).
6. Click one:

- OK—To save the changes.
- Cancel—To cancel the modifications.

Table 276: Event Timestamp Notification Configuration Details

Task	Your Action
Configure event timestamp notification.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click H248 Properties next to gateway. 3. Expand H248 Properties. 4. Click Event Timestamp Notification next to H248 Properties. 5. In the Comment box, enter the comment. 6. From the Request Timestamp list, select whether time stamp information is made available to the gateway controller or is suppressed. <ul style="list-style-type: none"> • Select requested to enable gateway controller access to time stamp information for notifications. • Select suppressed to disable gateway controller access to time stamp information for notifications. • Select autonomous which is equivalent to suppressed.

Hanging Termination Detection (NSM Procedure)

You can enable and configure hanging termination detection using this option.

To configure hanging termination detection in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in [Table 277 on page 477](#).
6. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.

Table 277: Hanging Termination Detection Configuration Details

Task	Your Action
Configure hanging termination detection	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click H248 Properties next to gateway. 3. Expand H248 Properties. 4. Click Hanging Termination Detection next to H248 Properties. 5. In the Comment box, enter the comment. 6. From the Timerx list, select the number of seconds between the last message exchanged for this termination and when the BGF sends a notification to the gateway controller. Range: 0 through 2,147,480

Configuring Inactivity Timer (NSM Procedure)

You can configure the inactivity timer package, which allows the BGF to use message inactivity to detect that its active gateway controller has failed using this option.

To configure Inactivity Timer in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in [Table 278 on page 478](#).
6. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.

Table 278: Inactivity Timer Configuration Details

Task	Your Action
Configure the inactivity timeout event.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click H248 Properties next to gateway. 3. Expand H248 Properties. 4. Click Inactivity Timer next to H248 Properties. 5. In the Comment box, enter the comment. 6. Expand Inactivity Timer. 7. Click Inactivity Timeout next to Inactivity Timer. 8. In the Comment box, enter the comment. 9. Select the Detect check box to specify the BGF detects inactivity timeout events received from the BGF by default. 10. Expand Inactivity Timeout.
Configure maximum inactivity time.	<ol style="list-style-type: none"> 1. Click Maximum Inactivity Time next to Inactivity Timeout. 2. In the Comment box, enter the comment. 3. From the Default list, select the default value for the maximum inactivity time. Range: 100 through 65,535 (10-millisecond units)

Configuring Notification Behavior (NSM Procedure)

You can configure the default frequency for regulated media inactivity notifications sent by the BGF using the Notification Behavior option.

To configure notification behavior in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in [Table 279 on page 479](#).
6. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.

Table 279: Notification Behavior Configuration Details

Task	Your Action
Configure the default frequency for sending media inactivity notifications for regulated events.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click H248 Properties next to gateway. 3. Expand H248 Properties. 4. Click Notification Behavior next to H248 properties. 5. In the Comment box, enter the comment. 6. Expand Notification Behavior. 7. Click Notification Regulation next to Notification Behavior. 8. In the Comment box, enter the comment. 9. In the Default box, enter the default frequency for sending media inactivity notifications for regulated events.

Configuring Segmentation (NSM Procedure)

You can configure default values for properties in the segmentation package using this option.

To configure segmentation in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in [Table 280 on page 480](#).
6. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.

Table 280: Segmentation Package Configuration Details

Task	Your Action
Set default, maximum, and minimum values for the MG maximum PDU size property of the segmentation package.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click H248 Properties next to gateway. 3. Expand H248 Properties. 4. Click Segmentation next to H248 properties. 5. In the Comment box, enter the comment. 6. Expand Segmentation. 7. Click Mg Maximum Pdu Size next to Segmentation. 8. In the Comment box, enter the comment. 9. From the Default list, select the default maximum size of messages that the gateway controller sends to the BGF. Range: 512 through 65,507 bytes
Set default, maximum, and minimum values for the MG segmentation timer value property of the segmentation package.	<ol style="list-style-type: none"> 1. Click Mg Segmentation Timer next to Segmentation. 2. In the Comment box, enter the comment. 3. From the Default list, select the default time within which the gateway controller waits to receive outstanding message segments from the virtual BGF after it receives the SegmentationCompleteToken. Range: 500 through 30,000 milliseconds
Set default, minimum, and maximum values for the MGC maximum Protocol Data Unit (PDU) size property of the segmentation package.	<ol style="list-style-type: none"> 1. Click Mgc Maximum Pdu Size next to Segmentation. 2. In the Comment box, enter the comment. 3. From the Default list, select the default maximum size of messages that the virtual BGF sends to the gateway controller. Range: 512 through 65,507 bytes
Set default, maximum, and minimum values for the MGC segmentation timer value property of the segmentation package.	<ol style="list-style-type: none"> 1. Click Mgc Segmentation Timer next to Segmentation. 2. In the Comment box, enter the comment. 3. From the Default list, select the default time within which the virtual BGF waits to receive outstanding message segments from the gateway controller after it receives the SegmentationCompleteToken. Range: 500 through 30,000 milliseconds

Configuring Traffic Management (NSM Procedure)

You can configure traffic management of the gate stream and the RTP Control Protocol (RTCP) stream. The parameters for the RTCP stream take effect only when the gate is an Real-time Transport Protocol (RTP)/RTCP gate.

To configure traffic management in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.

5. Add or modify the settings as specified in [Table 281 on page 481](#).
6. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.

Table 281: Traffic Management Configuration Details

Task	Your Action
Configure the maximum burst size for RTP/RTCP gate streams.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click H248 Properties next to gateway. 3. Expand H248 Properties. 4. Click Traffic Management next to H248 properties. 5. In the Comment box, enter the comment. 6. Click Max Burst Size next to Traffic Management. 7. In the Comment box, enter the comment. 8. From the Default list, select the default maximum burst size. Range: 20 through 2147483647 bytes 9. Expand Maximum Burst Size. 10. Click Rtcp next to Maximum Burst Size. 11. In the Comment box, enter the comment. 12. Expand Rtcp. 13. Click Percentage next to Rtcp. 14. Select one of the following: <ul style="list-style-type: none"> • percentage—if the value entered is a percentage of the RTP gate's rate. • fixed-value—if the value entered is a fixed number of bytes per second. Range: 20 through 2147483647 bytes-per-second
Configure the peak data rate for RTP/RTCP gate streams.	<ol style="list-style-type: none"> 1. Click Peak Data Rate next to Traffic Management. 2. In the Comment box, enter the comment. 3. From the Default list, select the default peak data rate. Range: 125 through 2147483647 bytes per second 4. Expand Peak Data Rate. 5. Click Rtcp next to Peak Data Rate. 6. In the Comment box, enter the comment. 7. Expand Rtcp. 8. Click Percentage next to Rtcp. 9. Select one of the following: <ul style="list-style-type: none"> • percentage—if the value entered is a percentage of the RTP's gate rate. • fixed-value—if the value entered is a fixed number of bits per second. Range: 0 through 2147483647

Table 281: Traffic Management Configuration Details (*continued*)

Task	Your Action
Configure the sustained data rate for streams of any protocol, including RTP.	<ol style="list-style-type: none"> 1. Click Sustained Data Rate next to Traffic Management. 2. In the Comment box, enter the comment. 3. From the Default list, select the default value for sustained data rate. Range: 125 through 4,294,967,295 bytes per second 4. Expand Sustained Data Rate. 5. Click Rtcp next to Sustained Data Rate. 6. In the Comment box, enter the comment. 7. Expand Rtcp. 8. Click Percentage next to Rtcp. 9. Select one of the following: <ul style="list-style-type: none"> • percentage—if the value entered is a percentage of the RTP's gate rate. • fixed-value—if the value entered is a fixed number of bits per second. Range: 0 through 2147483647

Configuring H248 Timers (NSM Procedure)

You can configure H.248 timers for the PGCP connection using the H248 Timers option.

To configure H248 timers in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in [Table 282 on page 483](#).
6. Click one:
 - **OK**—To save the changes.
 - **Cancel**—To cancel the modifications.

Table 282: H248 Timers Configuration Details

Task	Your Action
Configure H248 Timers.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click H248 Timers next to gateway. 3. In the Comment box, enter the comment. 4. From the Maximum Waiting Delay list, select the maximum time the virtual BGF waits before contacting a new gateway controller when the connection to the controlling gateway controller is lost. Range: 100 through 300000 milliseconds Default: 3000 5. From the Tmax Retransmission Delay list, select the duration of the delay before the BGF considers the gateway controller to be down. Range: 1000 through 60000 milliseconds Default: 25000 6. From the Initial Average Ack Delay list, select the assumed initial average delay. Range: 500 through 4000 milliseconds Default: 1000 7. From the Maximum Net Propagation Delay list, select the duration of the maximum network propagation delay time. Range: 500 through 10000 milliseconds Default: 5000

Configuring the Monitor (NSM Procedure)

You can enable Real-Time Control Protocol (RTCP) and Real-Time Transport Protocol (RTP) application-level gateways (ALGs) for media flows and monitor packets using the Monitor option.

To configure the monitor in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in [Table 283 on page 484](#).
6. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.

Table 283: Monitor Configuration Details

Task	Your Action
Configure the monitor.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click Monitor next to gateway. 3. In the Comment box, enter the comment. 4. Expand Monitor. 5. Click Media next to Monitor. 6. In the Comment box, enter the comment. 7. Select the Rtp check box to enable Real-Time Transport Protocol (RTP) application-level gateway (ALG) on media flows created when the gateway controller installs media gates on the virtual BGF. 8. Select the Rtcp check box to enable Real-Time Control Protocol (RTCP) application-level gateway (ALG) on media flows created when the gateway controller installs media gates on the virtual BGF.

Configuring Overload Control (NSM Procedure)

You can configure the BGF to send overload messages to the gateway controller based on the status of its work queue. The overload messages cause the gateway controller to lower the rate at which it admits packets for processing.

To configure overload control in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in [Table 284 on page 484](#).
6. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.

Table 284: Overload Control Configuration Details

Task	Your Action
Configure the BGF to send overload messages.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click Overload Control next to gateway. 3. In the Comment box, enter the comment. 4. From the Queue Limit Percentage list, select the percentage of the overload control work queue in use that triggers creation of an overload notification. Range: 1 through 100

Configuring Session Mirroring (NSM Procedure)

You can configure the session mirroring feature using the Session Mirroring option.

To configure session mirroring in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in [Table 285 on page 485](#).
6. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.

Table 285: Session Mirroring Configuring Details

Task	Your Action
Configure the delivery function that receives the session mirroring information.	<ol style="list-style-type: none"> 1. Click Add new entry next to Gateway. 2. Click Session Mirroring next to gateway. 3. In the Comment box, enter the comment. 4. Select the Disable Session Mirroring check box to disable the session mirroring feature. 5. Expand Session Mirroring. 6. Click Delivery Function next to Session Mirroring. 7. Click Add new entry next to Delivery Function. 8. In the New delivery-function window, enter the name of the delivery function that receives the session mirroring information.

Configuring Media Service (NSM Procedure)

You can configure media services for the Border gateway Function (BGF) configuration. Media services are applied to Packet Gateway Control Protocol (PGCP) packets.

To configure media service in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Media Service**.
5. Add or modify the settings as specified in [Table 286 on page 486](#).
6. Click one:
 - OK—To save the changes.

- **Cancel**—To cancel the modifications.

Table 286: Media Service Configuration Details

Task	Your Action
Configure media service.	<ol style="list-style-type: none"> 1. Click Add new entry next to Media Service. 2. In the Name box, enter the identifier for the media service name. 3. In the Comment box, enter the comment. 4. In the Nat Pool box, enter the identifier for the NAT address pool.

Configuring a Rule (NSM Procedure)

You can specify the rule that the router uses when it applies the media service.

To configure a rule in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Rule**.
5. Add or modify the settings as specified in [Table 287 on page 486](#).
6. Click one:
 - **OK**—To save the changes.
 - **Cancel**—To cancel the modifications.

Table 287: Configuring Rule

Task	Your Action
Configure a rule.	<ol style="list-style-type: none"> 1. Click Add new entry next to Rule. 2. In the Name box, enter the identifier for the rule. 3. In the Comment box, enter the comment. 4. From the Gateway list, select the identifier of the virtual BGF. 5. Expand rule. 6. Click Media Service next to rule. 7. Click Add new entry next to Media Service. 8. In the New media-service window, enter the identifier for the media service name.

Configuring Rule Set (NSM Procedure)

You can specify the rule set the router uses when applying this service.

To configure Rule Set in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Rule Set**.
5. Add or modify the settings as specified in [Table 288 on page 487](#).
6. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.

Table 288: Configuring Rule Set

Task	Your Action
Configure a rule set.	<ol style="list-style-type: none"> 1. Click Add new entry next to Rule Set. 2. In the Name box, enter the identifier for the collection of rules that make up this rule set. 3. In the Comment box, enter the comment. 4. Expand rule-set. 5. Click Rule next to rule-set. 6. Click Add new entry next to Rule. 7. From the Name list, select the identifier for the rule. 8. In the Comment box, enter the comment.

Configuring Session Mirroring (NSM Procedure)

You can configure the session mirroring feature using the session mirroring option.

To configure session mirroring in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Session Mirroring**.
5. Add or modify the settings as specified in [Table 289 on page 488](#).
6. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.

Table 289: Session Mirroring Configuration Details

Task	Your Action
Configure session mirroring.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment. 2. Select the Disable Session Mirroring check box to disable session mirroring on the BGF. 3. Expand Session Mirroring. 4. Click Delivery Function next to Session Mirroring. 5. Click Add new entry next to Delivery Function. 6. In the Name box, enter the name of the delivery function that receives the session mirroring information. 7. In the Comment box, enter the comment. 8. In the Destination Address box, enter the address of the server to which the BGF sends session-mirroring information. 9. From the Destination Port list, select the port on the delivery function server that receives session-mirroring information. Range: 0 through 65535 10. In the Network Operator Id box, enter the network operator ID. The ID can be up to five characters. 11. In the Source Address box, enter the address of the interface on which the BGF sends session-mirroring data to the delivery function. 12. From the Source Port list, select the port on which the BGF sends session-mirroring data to the delivery function. Range: 0 through 65,535 13. Expand delivery-function. 14. Click Memory Management next to delivery-function. 15. In the Comment box, enter the comment. 16. From the Operational Mode list, select the operational mode.

Configuring Traceoptions (NSM Procedure)

You can configure Packet Gateway Control Protocol (PGCP) trace options using the traceoptions option.

To configure traceoptions in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Traceoptions**.
5. Add or modify the settings as specified in [Table 290 on page 489](#).
6. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.

Table 290: Traceoptions Configuration Details

Task	Your Action
Configure PGCP trace options.	<ol style="list-style-type: none"> 1. In the Comment box, enter the comment. 2. Select the No Remote Trace check box to disable remote tracing. 3. Expand Traceoptions. 4. Click File next to Traceoptions. 5. In the Comment box, enter the comment. 6. In the Filename box, enter the name of the file to which the tracing messages are written. 7. In the Size box, enter the size parameter (in bytes) to trigger rotation of files. 8. From the Files list, select the number of trace files. 9. Select one of the following: <ul style="list-style-type: none"> • world-readable—To allow all users to use the log file. • no-world-readable—To disallow all users from using the log file. 10. In the Match box, enter the regular expression. 11. Click Flag next to Traceoptions. 12. Click Add new entry next to Flag. 13. In the Comment box, enter the comment.

Configuring Virtual Interface (NSM Procedure)

You can configure a virtual interface for the BGF using the Virtual Interface option.

To configure virtual interface in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Virtual Interface**.
5. Add or modify the settings as specified in [Table 291 on page 490](#).
6. Click one:
 - **OK**—To save the changes.
 - **Cancel**—To cancel the modifications.

Table 291: Virtual Interface Configuration Details

Task	Your Action
Configure a virtual interface	<ol style="list-style-type: none"> 1. Click Add new entry next to Virtual Interface. 2. In the Name box, enter the identifier number for the interface. Range: 0 through 1023 3. In the Comment box, enter the comment. 4. From the Service State list, select the service state of the virtual interface. 5. In the Interface box, enter the interface name. 6. Expand virtual-interface. 7. Click Media Service next to virtual-interface. 8. Click Add new entry next to Media Service. 9. In the dialog box, enter the identifier for the media service name. 10. Click Routing Instance next to virtual-interface. 11. In the Comment box, enter the comment. 12. From the Routing Instance Name list, select the name of a routing instance. 13. In the Service Interface box, enter the name and logical interface number of the service Interface in <i>interface-name.unit-number</i> form.

Configuring Service Interface Pools (NSM Procedure)

To configure service interface pool options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the service interface pool options.
3. Click the **Configuration** tab. In the configuration tree, expand **Services > Service Interface Pools**.
4. In the Service Interface Pools workspace, enter a comment for the service interface pool.
5. In the configuration tree, select **Services > Service Interface Pools > Pool**.
6. Add or modify settings as specified in [Table 292 on page 490](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the service interface pool options.

Table 292: Service Interface Pools Configuration Details

Option	Function	Your Action
Name	Specifies the service interface pool name.	Enter a name.

Table 292: Service Interface Pools Configuration Details (*continued*)

Option	Function	Your Action
Comment	Specifies the comment for the service interface pool.	Enter a comment.
pool > Interface		
Name	Specifies the services interface name.	Enter a name.
Comment	Specifies the comment for the services interface.	Enter a comment.

**Related
Documentation**

- [Configuring Captive Portal \(NSM Procedure\) on page 497](#)
- [Configuring Mobile IP \(NSM Procedure\) on page 502](#)
- [Configuring RPM \(NSM Procedure\) on page 513](#)
- [Configuring Unified Access Control \(NSM Procedure\) on page 519](#)

Configuring Stateful Firewall (NSM Procedure)

Stateful firewall is a type of firewall filter that considers state information derived from previous communications and other applications when evaluating traffic. Contrasted with a stateless firewall that inspects packets in isolation, a stateful firewall provides an extra layer of security by using state information derived from past communications and other applications to make dynamic control decisions for new communication attempts.

To configure stateful firewall in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Stateful Firewall**.
4. Add or modify the settings as specified in [Table 293 on page 492](#).
5. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.

Table 293: Stateful Firewall Configuration Details

Task	Your Action
Define the rule.	<ol style="list-style-type: none"> 1. Click Rule next to Stateful Firewall. 2. Click Add new entry next to Rule. 3. In the Name box, enter the identifier for the collection of terms that constitute this rule. 4. In the Comment box, enter the comment. 5. From the Match Direction list, select the direction in which the rule match is applied. <ul style="list-style-type: none"> • Select input to apply the rule match on the input side of the interface. • Select output to apply the rule match on the output side of the interface. • Select input-output to apply the rule match bidirectionally.
Define a term.	<ol style="list-style-type: none"> 1. Click Term next to rule. 2. Click Add new entry next to Term. 3. In the Name box, enter the identifier for the term. 4. In the Comment box, enter the comment. 5. Expand term. 6. Click From next to term. 7. In the Comment box, enter the comment. 8. Expand From. 9. From the listed match conditions, select the match condition for stateful firewall. The match conditions listed are Application Sets, Applications, Destination Address, Destination Address Range, Destination Prefix List, Source Address, Source Address Range, and Source Prefix List. 10. Click Then next to term. 11. In the Comment box, enter the comment. 12. Select the Syslog check box to enable system logging. 13. Expand Then. 14. Click Accept next to Then. <ul style="list-style-type: none"> • Select Accept to accept the traffic and send it on to its destination. • Select discard to not accept traffic or process it further. • Select reject to accept the traffic and return a rejection message.
Define IP option.	<ol style="list-style-type: none"> 1. Click Allow IP Options next to Then. 2. Click Add new entry next to Allow IP Options. 3. From the dropdown list, select the IP option name.

Table 293: Stateful Firewall Configuration Details (*continued*)

Task	Your Action
Define the rule set.	<ol style="list-style-type: none"> 1. Click Rule Set next to Stateful Firewall. 2. Click Add new entry next to Rule Set. 3. In the Name box, enter the identifier for the collection of rules that constitute this rule set. 4. In the Comment box, enter the comment. 5. Click Rule next to rule-set. 6. Click Add new entry next to Rule. 7. From the Name list, select the identifier for the collection of terms that constitute this rule. 8. In the Comment box, enter the comment.

**Related
Documentation**

- [Configuring Service Interface Pools \(NSM Procedure\)](#)
- [Configuring a Service Set \(NSM Procedure\) on page 493](#)

Configuring a Service Set (NSM Procedure)

A service set is a collection of services to be performed by an Adaptive Services (AS) or Multiservices PIC.

To configure a service set in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services**.
4. Select **Service Set**.
5. Add or modify the settings as specified in [Table 294 on page 494](#).
6. Click one:
 - OK—Save the changes.
 - Cancel—Cancel the modifications.

Table 294: Service Set Configuration Details

Task	Your Action
Define the service set.	<ol style="list-style-type: none"> 1. Click Add new entry next to Service Set. 2. In the Name box, enter the name that identifies the service set. 3. In the Comment box, enter the comment. 4. In the Max Flows box, enter the maximum number of flows. 5. From the Tcp Mss list, select the TCP Maximum Segment Size (MSS) allowed for the service set. Range: 536 to 65535 6. From the Application Identification Profile list, select the application identification method. 7. From the Idp Profile list, select the Idp profile. <p>NOTE: The IDP profile is a list of IDP policies as defined in the Security > Idp > Idp policy assigned to this device.</p>
Configuring AACL rule and AACL rule set.	<ol style="list-style-type: none"> 1. Click Aacl Rules next to service-set. 2. Select one of the following: <ul style="list-style-type: none"> • aacl-rules—To specify the rule the router uses when applying this service. • aacl-rule-set—To specify the rule set the router uses when applying this service. 3. Click Add new entry. 4. From the Name list, select the identifier for the collection of terms that constitute this rule set. 5. In the Comment box, enter the comment.
Allow multicast traffic to be sent to the Adaptive Services or Multiservices PIC.	<ol style="list-style-type: none"> 1. Click Allow Multicast next to service-set. 2. In the Comment box, enter the comment.
Specify the Class of Service (CoS) service rule or rule set included in this service.	<ol style="list-style-type: none"> 1. Click Cos Rules next to service-set. 2. Select one of the following: <ul style="list-style-type: none"> • cos-rules—To specify cos-rules. • cos-rule-set—To specify cos-rules set. 3. Click Add new entry. 4. From the Name list, select the rule or rule set name. <p>In the Comment box, enter the comment.</p>
Define Junos SDK service set.	<ol style="list-style-type: none"> 1. Click Extension Service next to service-set. 2. Click Add new entry next to Extension Service. 3. In the Name box, enter the identifier for a provider-specific service. 4. In the Comment box, enter the comment.

Table 294: Service Set Configuration Details (*continued*)

Task	Your Action
Specify the intrusion detection service (IDS) rules or rule set included in this service set.	<ol style="list-style-type: none"> 1. Click Ids Rules next to service-set. 2. Select one of the following: <ul style="list-style-type: none"> • ids—rules—To specify the ids rules. • ids-rule-sets—To specify the ids-rule-sets. 3. Click Add new entry. 4. From the Name list, select the rule or rule set name. <p>In the Comment box, enter the comment.</p>
Specify the device name for the interface service PIC.	<ol style="list-style-type: none"> 1. Click Interface Service next to service-set. 2. Select one of the following: <ul style="list-style-type: none"> • interface-service—To specify the device name for the interface service Physical Interface Card. <ol style="list-style-type: none"> a. In the Comment box, enter the comment. b. In the Services Interface box, enter the name of the service device associated with the interface-wide service set. • next-hop-service—To specify interface names or a service interface pool for the forwarding next-hop service set. You cannot specify both a service interface pool and an inside or outside interface. <ol style="list-style-type: none"> a. In the Comment box, enter the comment. b. In the Inside Service Interface box, enter the name and logical unit number of the service interface associated with the service set applied inside the network. c. In the Outside Service Interface box, enter the name and logical unit number of the service interface associated with the service set applied outside the network. d. From the Service Interface Pool list, select the name of the pool of logical interfaces.
Specify the Network Address Translation (NAT) rules or rule set included in this service set.	<ol style="list-style-type: none"> 1. Click Nat Rules next to service-set. 2. Select one of the following: <ul style="list-style-type: none"> • nat-rules—To specify the NAT rules included in this service set. • nat-rule-sets—To specify the NAT rule set included in this service set. 3. Click Add new entry. 4. From the Name list, select the rule or rule set name. 5. In the Comment box, enter the comment.

Table 294: Service Set Configuration Details (*continued*)

Task	Your Action
Specify the Packet Gateway Control Protocol (PGCP) rules or rule set included in this service set.	<ol style="list-style-type: none"> 1. Click Pgcp Rules next to service-set. 2. Select one of the following: <ul style="list-style-type: none"> • pgcp-rules—To specify the pgcp rules included in this service set. • pgcp-rule-set—To specify the pgcp rule set included in this service set. 3. Click Add new entry. 4. From the Name list, select the rule or rule set name. 5. In the Comment box, enter the comment.
Configuring the policy decision statistics profile.	<ol style="list-style-type: none"> 1. Click Policy Decision Statistics Profile next to service-set. 2. In the Comment box, enter the comment. 3. From the Profile Name list, select the policy decision statistics profile.
Define the order in which services are applied for this service set.	<ol style="list-style-type: none"> 1. Click Service Order next to service-set. 2. In the Comment box, enter the comment. 3. Click Forward Flow next to Service Order. 4. Click Add new entry next to Forward Flow. 5. In the New forward-flow window, enter the service order for forward flow. 6. Click Reverse Flow next to Service Order. 7. Click Add new entry next to Reverse Flow. 8. In the New reverse-flow window, enter the service order for reverse flow.
Specify the stateful firewall rules or rule set included in this service set.	<ol style="list-style-type: none"> 1. Click Stateful Firewall Rules next to service-set. 2. Select one of the following: <ul style="list-style-type: none"> • stateful-firewall-rules—To specify the stateful firewall rules. • stateful-firewall-rule-sets—To specify the stateful firewall rule set. 3. Click Add new entry. 4. From the Name list, select the rule or rule set name. 5. In the Comment box, enter the comment.

Table 294: Service Set Configuration Details (*continued*)

Task	Your Action
Configure generation of system log messages for the service set.	<ol style="list-style-type: none"> 1. Click Syslog next to service-set. 2. In the Comment box, enter the comment. 3. Click Host next to Syslog. 4. Click Add new entry next to Host. 5. In the Name box, enter the name of the system logging utility host machine. 6. In the Comment box, enter the comment. 7. From the Facility Override list, select the name of the facility that overrides the default assignment. 8. In the Log Prefix box, enter the system logging prefix value. 9. Click Contents next to host. 10. From the Name list, select the service set. 11. In the Comment box, enter the comment. 12. From the Any list, select the system logging severity level.

Related Documentation

- [Configuring Service Interface Pools \(NSM Procedure\)](#)
- [Configuring Stateful Firewall \(NSM Procedure\) on page 491](#)
- [Configuring Intrusion Detection Service \(NSM Procedure\) on page 450](#)

Configuring Captive Portal (NSM Procedure)

The captive portal feature allows you to configure custom options, interface, and traceoptions.

To configure the captive portal feature:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the captive portal feature.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Captive Portal**.
4. Configure the options as specified in [Table 295 on page 497](#).
5. Click one:
 - **OK** — Saves the changes.
 - **Cancel** — Cancels the modifications.
 - **Apply**—Applies the captive portal parameters.

Table 295: Captive Portal Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the captive portal. This is optional.	Enter a comment.

Table 295: Captive Portal Configuration Details (*continued*)

Option	Function	Your Action
Authentication Profile Name	Specifies the access profile name used for authentication.	Select an authentication profile name from the list.
Secure Authentication	Specifies either secure authentication (using encrypted HTTPS) or nonsecure authentication (using plain-text HTTP).	Select secure authentication from the list.

You can configure the following options with captive portal:

- [Configuring Custom Options \(NSM Procedure\) on page 498](#)
- [Configuring the Interface \(NSM Procedure\) on page 499](#)
- [Configuring Traceoptions \(NSM Procedure\) on page 500](#)

Configuring Custom Options (NSM Procedure)

This section provides information about configuring custom options for captive portal.

To configure custom options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the custom options feature.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Captive Portal > Custom Options**.
4. Select the **Enable Feature** check box.
5. Enter the parameters as specified in [Table 296 on page 498](#).
6. Click one:
 - **OK** — Saves the changes.
 - **Cancel** — Cancels the modifications.
 - **Apply**—Applies the custom option parameters.

Table 296: Custom Options Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the custom option. This is optional.	Enter a comment.
Header Logo	Specifies the path for the header logo.	Enter the path with a file type of JPG, JPEG, GIF, or PNG.
Header Bgcolor	Specifies the header background color.	Enter the header color.
Header Message	Specifies the header message.	Enter a message.

Table 296: Custom Options Configuration Details (*continued*)

Option	Function	Your Action
Banner Message	Specifies the terms and conditions of usage message.	Enter a message.
Form Header Message	Specifies the login form header message.	Enter a message.
Form Header Bgcolor	Specifies the login form header background color.	Enter the form header color.
Form Submit Label	Specifies the label for submitting the form.	Enter a label.
Form Reset Label	Specifies the label for resetting the form.	Enter a label.
Footer Message	Specifies the footer message.	Enter a message.
Footer Bgcolor	Specifies the footer background color.	Enter the footer color.
Post Authentication Url	Specifies the post authentication redirection URL.	Enter a URL.

Configuring the Interface (NSM Procedure)

This section provides information about configuring the interface option for captive portal.

To configure the interface:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the interface feature.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Captive Portal > Interface**.
4. Add or modify the interface settings as specified in [Table 297 on page 499](#).
5. Click one:
 - **OK** — Saves the changes.
 - **Cancel** — Cancels the modifications.

Table 297: Interface Configuration Details

Option	Function	Your Action
Name	Specifies the name of the interface.	Select a name from the list.
Comment	Supplies a descriptive comment for the interface.	Enter a comment.
Supplicant	Specifies the supplicant mode for this interface.	Select a supplicant from the list.
Retries	Specifies the number of retries after which the port enters a wait state.	Set the number of retries. Range: 1 through 10.

Table 297: Interface Configuration Details (*continued*)

Option	Function	Your Action
Quiet Period	Specifies the duration to wait after an authentication failure.	Set the quiet period. Range: 0 through 65535.
Server Timeout	Specifies the timeout interval for the authentication server.	Set the server timeout. Range: 1 through 60.
Session Expiry	Specifies the timeout period before session expiration..	Set the session expiration period. Range: 1 through 65535.

Configuring Traceoptions (NSM Procedure)

The traceoptions feature allows you to configure file and flag options.

To configure traceoptions:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure traceoptions.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Captive Portal > Traceoptions**.
4. Enter a comment in the traceoptions workspace that describes the traceoptions.
5. Click one:
 - **OK** — Saves the changes.
 - **Cancel** — Cancels the modifications.
 - **Apply**—Applies the traceoptions settings.

You can now configure the following options:

- [Configuring File Options \(NSM Procedure\) on page 500](#)
- [Configuring Flag Options \(NSM Procedure\) on page 501](#)

Configuring File Options (NSM Procedure)

To configure file options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure file options.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Captive Portal > Traceoptions > File**.
4. Configure the file options as specified in [Table 298 on page 501](#).
5. Click one:

- **OK** — Saves the changes.
- **Cancel** — Cancels the modifications.
- **Apply**—Applies the file settings.

Table 298: File Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the filename.	Enter a comment.
Filename	Specifies the filename to write the traceoptions.	Enter a filename.
Replace	Specifies whether the trace files must be replaced instead of appended.	Select the Replace check box.
Size	Specifies the maximum size of the trace file.	Enter the maximum file size.
Files	Specifies the maximum number of trace files.	Set the maximum number of trace files. Range: 2 through 1000.
No Stamp	Specifies that you do not want to timestamp the trace file.	Select the No Stamp check box.
None	Specifies that neither the world-readable or no-world-readable option is enabled.	Select the option.
world-readable	Allows any user to read the log file. (Optional)	Select the option.
no-world-readable	Prevents any user from reading the log file. (Optional)	Select the option.

Configuring Flag Options (NSM Procedure)

To configure flag options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure flag options.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Captive Portal > Traceoptions > Flag**.
4. Configure the flag options as specified in [Table 299 on page 502](#).
5. Click one:
 - **OK** — Saves the changes.
 - **Cancel** — Cancels the modifications.
 - **Apply**—Applies the flag settings.

Table 299: Flag Configuration Details

Option	Function	Your Action
Name	Specifies the trace flag name.	Select a name from the list.
Comment	Supplies a descriptive comment for the trace flag.	Enter a comment.
Disable	Disables the trace flag.	Select the Disable check box.

Configuring Mobile IP (NSM Procedure)

The Mobile IP feature allows you to configure the following options: access type, authenticate, dynamic home assignment, home agent, peer, and traceoptions.

To configure the Mobile IP feature:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the Mobile IP feature.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Mobile IP**.
4. Select the **Enable Feature** check box.
5. Enter a comment in the Mobile IP workspace that describes the Mobile IP.
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the Mobile IP settings.

You can now configure the following options:

- [Configuring Access Type \(NSM Procedure\) on page 502](#)
- [Configuring the Authenticate Mechanism \(NSM Procedure\) on page 503](#)
- [Configuring Dynamic Home Assignment \(NSM Procedure\) on page 504](#)
- [Configuring the Home Agent \(NSM Procedure\) on page 505](#)
- [Configuring the Peer \(NSM Procedure\) on page 507](#)
- [Configuring Traceoptions \(NSM Procedure\) on page 510](#)

Configuring Access Type (NSM Procedure)

This section provides information about configuring access type for Mobile IP.

To configure access type:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the access type option.

3. Click the **Configuration** tab. In the configuration tree, select **Services > Mobile IP > Access Type**.
4. Enter a comment in the Access Type workspace that describes the access type.
5. Configure the access type options as specified in [Table 300 on page 503](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the access type options.

Table 300: Access Type Configuration Details

Option	Function	Your Action
Access Type > Wimax		
None	Specifies that neither the wimax or generic environment is specified for the access type..	Select the option.
wimax	Enables Worldwide Interoperability for Microwave Access (WiMAX) environment.	Select the option and enter a Comment in the comment field.
generic	Enables non-WiMAX environment.	Select the option and enter a Comment in the comment field.

Configuring the Authenticate Mechanism (NSM Procedure)

This section provides information about configuring authenticate mechanism for Mobile IP.

To configure the authenticate mechanism :

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the authenticate mechanism.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Mobile IP > Authenticate**.
4. Configure the authenticate options as specified in [Table 301 on page 504](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the authenticate options.

Table 301: Authenticate Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the authenticate option. This is optional.	Enter a comment.
Order	Specifies the order in which to use the authenticate mechanism.	Select an order from the list.

Configuring Dynamic Home Assignment (NSM Procedure)

This section provides information about configuring access dynamic home assignment for Mobile IP.

To configure dynamic home assignment:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure dynamic home assignment.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Mobile IP > Dynamic Home Assignment**.
4. Enter a comment in the Dynamic Home Assignment workspace that describes the dynamic home assignment.
5. In the configuration tree, select **Services > Mobile IP > Dynamic Home Assignment > Home Agent**.
6. Enter a comment in the Home Agent workspace that describes the home agent.
7. In the configuration tree, select **Services > Mobile IP > Dynamic Home Assignment > Home Agent > Nai**.
8. Add or modify settings as specified in [Table 302 on page 504](#).
9. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the Nai options.

Table 302: Dynamic Home Assignment Configuration Details

Option	Function	Your Action
Name	Specifies a name for the network address identifiers (NAI).	Enter a name in the following format: <ul style="list-style-type: none"> • @domain.com • user@domain.com
Comment	Supplies a descriptive comment for the NAI.	Enter a comment.
Home Agent	Specifies the IP address of the home agent.	Enter the IP address.

Configuring the Home Agent (NSM Procedure)

The home agent feature allows you to configure enable service, pool match order, and virtual network.

To configure home agent feature:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the home agent feature.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Mobile IP > Home Agent**.
4. Enter a comment in the Home Agent workspace that describes the home agent.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the home agent options.

You can now configure the following options:

- [Configuring Enable Service \(NSM Procedure\) on page 505](#)
- [Configuring Pool Match Order \(NSM Procedure\) on page 506](#)
- [Configuring the Virtual Network \(NSM Procedure\) on page 506](#)

Configuring Enable Service (NSM Procedure)

This section provides information about configuring the enable service for home agent.

To configure the enable service mechanism:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the enable service mechanism.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Mobile IP > Home Agent > Enable Service**.
4. Add or modify settings as specified in [Table 303 on page 506](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the enable service options.

Table 303: Enable Service Configuration Details

Option	Function	Your Action
Name	Specifies the interface name.	Enter the interface name. Value: gigabit, fast ethernet or a 10-gigabit ethernet interface.
Comment	Specifies the comment for the interface.	Enter a comment.

Configuring Pool Match Order (NSM Procedure)

This section provides information about configuring pool match order for home agent.

To configure the pool match order:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the pool match order.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Mobile IP > Home Agent > Pool Match Order**.
4. Add or modify settings as specified in [Table 304 on page 506](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the pool match order options.

Table 304: Pool Match Order Configuration Details

Option	Function	Your Action
Name	Specifies the name of the pool match order.	Select the name from the list.
Comment	Supplies a descriptive comment for the pool match order.	Enter a comment.

Configuring the Virtual Network (NSM Procedure)

This section provides information about configuring virtual network for home agent.

To configure the virtual network:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the virtual network.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Mobile IP > Home Agent > Virtual Network**.
4. Enter a comment in the Virtual Network workspace that describes the virtual network.

5. Add or modify the settings as specified in [Table 305 on page 507](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the virtual network options.

Table 305: Virtual Network Configuration Details

Option	Function	Your Action
Virtual Network > Home Agent Address		
Name	Specifies the loopback IP address of the home agent.	Enter the IP address.
Comment	Specifies the comment for the home agent.	Enter a comment.
Registration Lifetime	Specifies the maximum registration lifetime.	Set the maximum registration life time. Range: 7 through 65535.
Timestamp Tolerance	Specifies the maximum timestamp tolerance.	Set the maximum timestamp tolerance. Range: 1 through 255.
Starting IP Address	Specifies the starting IP address of the pool.	Enter the IP address.
Ending IP Address	Specifies the ending IP address of the pool.	Enter the IP address.
Revocation Required	Enables registration revocation. <i>NOTE:</i> This is a mandatory field.	Select the check box.

Configuring the Peer (NSM Procedure)

This section provides information about configuring a peer for Mobile IP.

To configure Peer:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the peer feature.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Mobile IP > Peer**.
4. Enter a comment in the Peer workspace that describes the peer.
5. Add or modify the settings as specified in [Table 306 on page 508](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 306: Peer Configuration Details

Option	Function	Your Action
Peer > IP Address		
Name	Specifies the peer IP address.	Enter the IP address.
Comment	Supplies a descriptive comment for the IP address.	Enter a comment.
Peer > IP Address > Spi		
Name	Specifies the Security Parameter Index (SPI) value.	Enter the SPI value in hexadecimal format. For example, 0–9, a–f, A–F.
Comment	Specifies the comment for the SPI value.	Enter a comment.
Peer > IP Address > Spi > Algorithm		
Comment	Specifies the comment for the algorithm.	Enter a comment.
none	Specifies that neither the hmac-md5 or md5 option is specified for the algorithm.	Select the option.
hmac-md5	Specifies hash algorithm that authenticates packet data.	Select the option.
md5	Produces a 128-bit digest.	Select the option.
Peer > IP Address > Spi > Entity Type		
Comment	Specifies the comment for the entity type.	Enter a comment,
none	Specifies that neither the host or the mobility-agent entity type is enabled.	Select the option.
host	Enables the host entity type.	Select the option.
mobility-agent	Enables the mobility-agent entity type.	Select the option.
Peer > IP Address > Spi > Key		
Comment	Specifies the comment for the key.	Enter a comment.
Peer > IP Address > Spi > Key > Hex		
None	Specifies that neither the HEX or ASCII key is enabled.	Select the option.
hex	Enables hexadecimal text key.	<ol style="list-style-type: none"> 1. Select the option. 2. Enter a comment and a hexadecimal value.

Table 306: Peer Configuration Details (*continued*)

Option	Function	Your Action
ascii	Enables ASCII text key.	<ol style="list-style-type: none"> 1. Select the option. 2. Enter a comment and ASCII value.
Peer > IP Address > Spi > Replay Method		
Comment	Specifies the comment for the replay method.	Enter a comment.
Peer > IP Address > Spi > Replay Method > Timestamp		
None	Specifies that the timestamp option is not enabled	Select the option.
timestamp	Enables the timestamp option.	<ol style="list-style-type: none"> 1. Select the option. 2. Enter a comment for the timestamp. 3. Enter the timestamp receive duration. Range: 1 through 255.
none (configuration)	Specifies that the configuration option is not selected.	Select the option.
Peer > Nai		
Name	Specifies the name for the NAI.	Enter a name in the following format: <ul style="list-style-type: none"> • @domain.com • user@domain.com
Comment	Specifies the comment for the NAI.	Enter a comment.
Peer > Nai > Spi		
Name	Specifies the SPI value.	Enter the SPI value in hexadecimal format. (0–9, a–f, A–F).
Comment	Specifies the comment for the SPI value.	Enter a comment.
Peer > Nai > Spi > Algorithm		
Comment	Specifies the comment for the algorithm.	Enter a comment.
none	Specifies that neither the hmac-md5 or md5 option is specified for the algorithm.	Select the option.
hmac-md5	Specifies hash algorithm that authenticates packet data.	Select the option.
md5	Produces a 128-bit digest.	Select the option.
Peer > Nai > Spi > Entity Type		

Table 306: Peer Configuration Details (*continued*)

Option	Function	Your Action
Comment	Specifies the comment for the entity type.	Enter a comment.
none	Specifies that neither the host or the mobility-agent entity type is enabled.	Select the option.
host	Enables the host entity type.	Select the option.
mobility-agent	Enables the mobility-agent entity type.	Select the option.
Peer > Nai > Spi > Key		
Comment	Specifies the comment for the key.	Enter a comment.
Peer > Nai > Spi > Key > Hex		
None	Specifies that neither the HEX or ASCII key is enabled.	Select the option.
hex	Enables hexadecimal text key.	<ol style="list-style-type: none"> 1. Select the option. 2. Enter a comment and a hexadecimal value.
ascii	Enables ASCII text key.	<ol style="list-style-type: none"> 1. Select the option. 2. Enter a comment and an ASCII value.
Peer > Nai > Spi > Replay Method		
Comment	Specifies the comment for the replay method.	Enter a comment.
Peer > Nai > Spi > Replay Method > Timestamp		
None	Specifies that the timestamp option is not enabled	Select the option.
timestamp	Enables the timestamp option.	<ol style="list-style-type: none"> 1. Select the option. 2. Enter a comment for the timestamp. 3. Enter the duration within which the timestamp must be received. Range: 1 through 255.
none (configuration)	Specifies that the configuration option is not selected.	Select the option.

Configuring Traceoptions (NSM Procedure)

The traceoptions feature allows you to configure file and flag options.

To configure traceoptions feature:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure traceoptions.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Mobile IP > Traceoptions**.
4. Configure the options as specified in [Table 307 on page 511](#).
5. Click one:
 - **OK** — Saves the changes.
 - **Cancel** — Cancels the modifications.
 - **Apply**—Applies the traceoptions settings.

Table 307: Traceoptions Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the traceoptions.	Enter a comment.
No Remote Trace	Disables the remote tracing option.	Select the No Remote Trace check box.
Level	Specifies the level of debugging output.	Select the level.

You can configure the following options under traceoptions:

- [Configuring File \(NSM Procedure\) on page 511](#)
- [Configuring Flag \(NSM Procedure\) on page 512](#)

Configuring File (NSM Procedure)

To configure file options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the traceoptions file feature.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Mobile IP > Traceoptions > File**.
4. Configure the file options as specified in [Table 308 on page 512](#).
5. Click one:
 - **OK** — Saves the changes.
 - **Cancel** — Cancels the modifications.
 - **Apply**—Applies the file options.

Table 308: File Configuration Details

Option	Function	Your Action
Comment	Specifies the comment for the filename.	Enter a comment.
Filename	Specifies the filename to write the traceoptions.	Enter a filename.
Size	Specifies the maximum size of the trace file.	Enter the maximum file size.
Files	Specifies the maximum number of trace files.	Set the maximum number of trace files. Range: 2 through 1000.
None	Specifies that neither the world-readable or no-world-readable option is enabled.	Select the option.
no-world-readable	Allows any user to read the log file. (Optional)	Select the option.
world-readable	Prevents any user from reading the log file. (Optional)	Select the option.
Match	Specifies the regular expression for lines to be logged.	Enter the match expression.

Configuring Flag (NSM Procedure)

To configure flag options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure flag options.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Mobile IP > Traceoptions > Flag**.
4. Add or modify the settings as specified in [Table 309 on page 512](#).
5. Click one:
 - **OK** — Saves the changes.
 - **Cancel** — Cancels the modifications.
 - **Apply**—Applies the flag options.

Table 309: Flag Configuration Details

Option	Function	Your Action
Name	Specifies the flag name.	Select a name from the drop-down list.
Comment	Specifies the comment for the flag.	Enter a comment.

Configuring RPM (NSM Procedure)

Real-time Performance Monitoring (RPM) includes the Border Gateway Protocol (BGP), probe, and probe server.

To configure the RPM feature:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the RPM feature.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Rpm**.
4. Select the **Enable Feature** check box.
5. Configure the RPM options as specified in [Table 310 on page 513](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the RPM options.

Table 310: RPM Configuration Options

Option	Function	Your Action
Comment	Supplies a descriptive comment for RPM. This is optional.	Enter a comment.
Probe Limit	Specifies the maximum number of concurrent probes allowed.	Set the probe limit. Range: 1 through 500.

You can configure the following RPM options:

- [Configuring BGP \(NSM Procedure\) on page 513](#)
- [Configuring Probe \(NSM Procedure\) on page 515](#)
- [Configuring Probe Server \(NSM Procedure\) on page 518](#)

Configuring BGP (NSM Procedure)

This section provides information about configuring Border Gateway Protocol (BGP) for RPM.

To configure BGP:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the BGP feature.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Rpm > Bgp**.

4. Configure the options as specified in [Table 311 on page 514](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the BGP parameters.

Table 311: BGP Configuration Options

Option	Function	Your Action
Comment	Supplies a descriptive comment for BGP. This is optional.	Enter a comment.
Probe Type	Specifies the RPM-BGP probe request type.	Select the probe request type.
Probe Count	Specifies the total number of probes per test.	Set the probe count. Range: 1 through 15.
Probe Interval	Specifies the amount of time between probes.	Set the probe interval. Range: 1 through 255.
Test Interval	Specifies the amount of time between tests.	Set the test interval. Range: 0 through 86400.
Destination Port	Specifies the TCP/UDP port number.	Set the destination port number. Range: 7 through 65535.
History Size	Specifies the number of stored history entries.	Set the history size. Range: 0 through 255.
Moving Average Size	Specifies the average number of samples to use for the moving average.	Set the moving average size. Range: 0 through 255.
Data Size	Specifies the size of the data portion of the probe.	Set the data size. Range: 0 through 65507.
Data Fill	Defines content for the data portion of the probes.	Enter the content in hexadecimal format (0-9, a-f, A-F).

BGP allows you to configure routing instance options.

- [Configuring Routing Instances \(NSM Procedure\) on page 514](#)

[Configuring Routing Instances \(NSM Procedure\)](#)

This section provides information about configuring routing instances for BGP.

To configure routing instances:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the BGP routing instances options.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Rpm > Bgp > Routing Instances**.

4. Add or modify the settings as specified in [Table 312 on page 515](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the routing instances options.

Table 312: Routing Instance Configuration Options

Option	Function	Your Action
Name	Specifies the routing instance name.	Enter a name.
Comment	Specifies the comment for the routing instance.	Enter a comment.

Configuring Probe (NSM Procedure)

This section provides information about configuring probe options for RPM.

To configure probe options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the probe mechanism.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Rpm > Probe**.
4. Add or modify settings as specified in [Table 313 on page 515](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the probe options.

Table 313: Probe Configuration Options

Option	Function	Your Action
Name	Specifies the name of the owner.	Enter a name.
Comment	Specifies the comment for the probe.	Enter a comment.
probe > test		
Name	Specifies the name of the test.	Enter a name.
Comment	Specifies a comment for the test.	Enter a comment.
Probe Type	Specifies the probe request type.	Select the probe request type.

Table 313: Probe Configuration Options (*continued*)

Option	Function	Your Action
Probe Count	Specifies the total number of probes per count.	Enter the value or select it from the list. Range: 1 through 15.
Probe Interval	Specifies the amount of time between the probes.	Enter the value or select it from the list. Range: 1 through 255.
Test Interval	Specifies the amount of time between the tests.	Enter the value or select it from the list. Range: 0 through 86400.
Destination Port	Specifies the TCP/UDP port number.	Enter the value or select it from the list. Range: 7 through 65535.
Source Address	Specifies the source address for probes.	Enter the source address.
Routing Instance	Specifies the routing instance used by probes.	Select the routing instance.
History Size	Specifies the number of stored history entries.	Enter the value or select it from the list. Range: 0 through 255.
Moving Average Size	Specifies the average number of samples to use for the moving average.	Enter the value or select it from the list. Range: 0 through 255.
Dscp Code Points	Specifies the Differentiated Services (DiffServ) code point bits or alias.	Select the DSCP code points.
Data Size	Specifies the size of the data portion of the probes.	Enter the value or select it from the list. Range: 0 through 65507
Data Fill	Defines the content of the data portion of the probes.	Enter the content in hexadecimal format (0-9, a-f, A-F).
Destination Interface	Specifies the name of the output interface for probes.	Enter the name of the output interface for probes.
Hardware Timestamp	Specifies that the Packet Forwarding Engine updates the timestamp.	Select the check box.
One Way Hardware Timestamp	Enables hardware timestamps for one-way measurements.	Select the check box.
probe > test > Target		
Comment	Specifies a comment for the target.	Enter a comment.

Table 313: Probe Configuration Options (*continued*)

Option	Function	Your Action
probe > test > Target > Address		
none	Specifies that neither the IP address nor the URL of the remote server that is being probed by the RPM test is specified.	Select the option.
address	Specifies the IP address of the remote server that is being probed by the RPM test.	Select the option and enter the address.
url	Specifies the URL of the remote server that is being probed by the RPM test.	Select the option and enter the URL.
probe > test > Thresholds		
Comment	Specifies a comment for the threshold.	Enter a comment.
Successive Loss	Specifies the number of successive probe losses, which indicates successive failure.	Enter the value or select it from the list. Range: 0 through 15.
Total Loss	Specifies total number of probe losses, which indicates test failure.	Enter the value or select it from the list. Range: 0 through 15.
Rtt	Specifies the maximum round-trip time per probe.	Enter the value or select it from the list. Range: 0 through 60000000.
Jitter Rtt	Specifies the maximum jitter per test.	Enter the value or select it from the list. Range: 0 through 60000000.
Std Dev Rtt	Specifies the maximum standard deviation per test.	Enter the value or select it from the list. Range: 0 through 60000000.
Egress Time	Specifies maximum source-to-destination time per probe.	Enter the value or select it from the list. Range: 0 through 60000000.
Ingress Time	Specifies maximum destination-to-source time per probe.	Enter the value or select it from the list. Range: 0 through 60000000.
Jitter Ingress	Specifies maximum destination-to-source jitter per test.	Enter the value or select it from the list. Range: 0 through 60000000.
Jitter Egress	Specifies maximum source-to-destination jitter per test.	Enter the value or select it from the list. Range: 0 through 60000000.

Table 313: Probe Configuration Options (*continued*)

Option	Function	Your Action
Std Dev Ingress	Specifies maximum destination-to-source standard deviation per test.	Enter the value or select it from the list. Range: 0 through 60000000.
Std Dev Egress	Specifies maximum source-to-destination standard deviation per test.	Enter the value or select it from the list. Range: 0 through 60000000.
probe > test > Traps		
New Traps	Specifies the test traps.	Select a trap.

Configuring Probe Server (NSM Procedure)

This section provides information about configuring probe server options for RPM.

To configure probe server options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure probe server options.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Rpm > Probe Server**.
4. In the Probe Server workspace, enter a comment for the probe server.
5. Configure the options as specified in [Table 314 on page 518](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the probe server settings.

Table 314: Probe Server Configuration Details

Option	Function	Your Action
Probe Server > Icmp		
Comment	Specifies the comment for probe ICMP.	Enter a comment.
Destination Interface	Specifies the name of the output interface for probes.	Enter the name of the destination interface.
Probe Server > Tcp		
Comment	Specifies the comment for TCP.	Enter a comment.

Table 314: Probe Server Configuration Details (*continued*)

Option	Function	Your Action
Port	Specifies the TCP port number.	Set the port number. Range: 0 through 65535.
Destination Interface	Specifies the name of the output interface for probes.	Enter the name of the destination interface.
Probe Server > Udp		
Comment	Specifies the comment for UDP.	Enter a comment.
Port	Specifies the UDP port number.	Set the port number. Range: 0 through 65535.
Destination Interface	Specifies the name of the output interface for probes.	Enter the name of the destination interface.

Configuring Unified Access Control (NSM Procedure)

Unified Access Control (UAC) includes configuring infranet controllers and traceoptions.

To configure the UAC feature:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the UAC feature.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Unified Access Control**.
4. Configure the options as specified in [Table 315 on page 519](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the UAC options.

Table 315: UAC Configuration Details

Option	Function	Your Action
Comment	Specifies the comment for the UAC.	Enter a comment.
Timeout	Specifies (in seconds) the timeout for the idle infranet controller link.	Enter the timeout in seconds. Range: 2 through 4,294,967,295.
Interval	Specifies (in seconds) the heartbeat interval from the infranet controller.	Enter the heartbeat interval in seconds. Range: 1 through 4,294,967,295.
Timeout Action	Specifies the action to be performed when an infranet controller timeout occurs.	Select the timeout action.

Table 315: UAC Configuration Details (*continued*)

Option	Function	Your Action
Test Only Mode	Allows all traffic and log enforcement result.	Select the check box.

UAC includes configuring the following topics:

- [Configuring Infranet Controller \(NSM Procedure\) on page 520](#)
- [Configuring Traceoptions \(NSM Procedure\) on page 521](#)

Configuring Infranet Controller (NSM Procedure)

This section describes how to configure infranet controller for UAC.

To configure infranet controller options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure infranet controller options.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Unified Access Control > Infranet Controller**.
4. Add or modify the settings as specified in [Table 316 on page 520](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the infranet controller options.

Table 316: Infranet Controller Configuration Details

Option	Function	Your Action
Name	Specifies the name of the infranet controller.	Enter a name.
Comment	Specifies the comment for the infranet controller.	Enter a comment.
Address	Specifies the infranet controller IP address.	Enter the IP address.
Port	Specifies the infranet controller port.	Enter the port number. Range: 1 through 65535.
Interface	Specifies the outgoing interface.	Enter an interface.
Password	Specifies the infranet controller server password.	Enter the password.
Server Certificate Subject	Specifies the subject name of the infranet controller certificate to match.	Enter the server certificate subject.
infranet-controller > Ca Profile		

Table 316: Infranet Controller Configuration Details (*continued*)

Option	Function	Your Action
Ca Profile	Specifies the certification authority profile.	Select the required profile from the Non-members list and click Add to move the profiles to the Members list.

Configuring Traceoptions (NSM Procedure)

This section describes how to configure traceoptions for UAC.

To configure traceoptions:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the traceoptions feature.
3. Click the **Configuration** tab. In the configuration tree, select **Services > Unified Access Control > Traceoptions**.
4. In the Traceoptions workspace, enter a comment for the traceoptions.
5. In the configuration tree, select **Services > Unified Access Control > Traceoptions > Flag**.
6. Add or modify settings as specified in [Table 317 on page 521](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 317: Traceoptions Configuration Details

Option	Function	Your Action
Name	Specifies the flag name.	Select a name.
Comment	Specifies the comment for the flag.	Enter a comment.

Configuration of SNMP for Network Management

- [Configuring Basic System Identification for SNMP \(NSM Procedure\) on page 523](#)
- [Configuring SNMP Communities \(NSM Procedure\) on page 524](#)
- [Configuring SNMP Trap Groups \(NSM Procedure\) on page 526](#)
- [Configuring SNMP Views \(NSM Procedure\) on page 528](#)

Configuring Basic System Identification for SNMP (NSM Procedure)

To configure basic system identification information for SNMP:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab and then double-click the device for which you want to configure basic system identification information.
3. Click the **Configuration** tab. In the configuration tree, select **Snmp**.
4. Add or modify basic system identification information as specified in [Table 318 on page 523](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 318: Basic System Identification Details

Option	Function	Your Action
System Name	Specifies a system name for the device.	Enter the system name as a free-form text string.
Description	Provides a description for the system.	Enter a description for the system. For example, type J4350 with 4 PIMs .
Location	Specifies the system location information.	Enter the system location information (such as a lab name and a rack name).

Table 318: Basic System Identification Details (*continued*)

Option	Function	Your Action
Contact	Specifies the contact information for the system.	Enter the system contact information (such as a name and a phone number).
Snmp > Engine Id		
Use Mac Address	Sets the engine ID to use the MAC address.	Select this option.

Related Documentation

- [Configuring SNMP Communities \(NSM Procedure\) on page 524](#)
- [Configuring SNMP Trap Groups \(NSM Procedure\) on page 526](#)
- [Configuring SNMP Views \(NSM Procedure\) on page 528](#)

Configuring SNMP Communities (NSM Procedure)

You can configure an SNMP community to authorize access to the SNMP server by SNMP clients, based on the source IP address of incoming SNMP request packets. A community also defines which MIB objects are available and the operations (read-only or read-write) allowed on those objects. The SNMP client application specifies an SNMP community name in Get, GetNext, GetBulk, and Set SNMP requests. If a community is not configured, all SNMP requests are denied.

To configure SNMP communities in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **SNMP**.
5. Select **Community**.
6. Click the **Add** or **Edit** icon.
7. Enter the parameters as specified in [Table 319 on page 525](#).
8. Click one:
 - **OK**—To save the changes.
 - **Cancel**—To cancel the modifications.
 - **Apply**—To apply the SNMP settings.



NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

Table 319: Configuring Community Fields

Option	Function	Your Action
Name	Specifies the name of the community.	Enter a name for the community.
Comment	Specifies the comment for the community.	Enter a comment.
View	Specifies the view associated with the community.	Enter a name for the view.
Authorization	Specifies the type of access granted to the community. Access is authorized for SNMP Get, GetBulk, GetNext, and Set requests.	Select an access type for the community: <ul style="list-style-type: none"> • None—No requests are enabled. • read-only—Enable Get, GetNext, and GetBulk requests. This option is enabled by default. • read-write—Enable all requests, including Set requests. You must configure a view to enable Set requests.
Client List Name	Specifies a client list or prefix list to be assigned to an SNMP community.	<ol style="list-style-type: none"> 1. Expand the Community tree and select Client List Name. 2. Select a name.

Table 319: Configuring Community Fields (*continued*)

Option	Function	Your Action
Routing Instance	Specifies a routing instance for a community.	<ol style="list-style-type: none"> 1. Expand the Community tree and select Routing Instance. 2. Click the New button or select an entry and click the Edit button. 3. Configure the following to create and define a routing instance: <ul style="list-style-type: none"> • Name—Enter a name for the routing instance. <p>NOTE: On routers, to configure a routing instance within a logical system, specify the logical system name followed by the routing instance name. Use a slash (/) to separate the two names. To configure the default routing instance on a logical system, specify the logical system name followed by "default."</p> <ul style="list-style-type: none"> • Comment—Enter a comment for the routing instance.

Related Documentation

- Configuring Client Lists (NSM Procedure)

Configuring SNMP Trap Groups (NSM Procedure)

You can create and name a group of one or more types of SNMP traps and then define which systems receive the group of SNMP traps. The trap group must be configured for SNMP traps to be sent. The trap group name can be any string and is embedded in the community name field of the trap. To configure your own trap group port, use the **Destination Port** option. The default destination port is port 162. For each trap group that you define, specify:

- At least one system as the recipient of the SNMP traps in the trap group
- The types of traps the trap group can receive
- Routing instance used by the trap group

To configure trap groups in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **SNMP**.
5. Select **Trap Group**.
6. Select the **Enable Feature** check box.

7. Enter the parameters as specified in [Table 320 on page 527](#).
8. Click one:
 - **OK**—To save the changes.
 - **Cancel**—To cancel the modifications.
 - **Apply**—To apply the SNMP settings.

Table 320: Configuring SNMP Trap Group Fields

Option	Function	Your Action
Name	Specifies a name for the trap group.	Enter a name for the trap group.
Version	Specifies the version number of the SNMP trap group.	Select the version number for the SNMP trap group from the list.
Destination Port	Specifies the SNMP trap group port number.	Enter a trap group port number.
Routing Instance	Specifies a routing instance for trap targets.	Enter the name of the routing instance.
Categories	Defines the types of traps that are sent to the targets of the named trap group.	<ol style="list-style-type: none"> 1. Expand the trap-group tree and select Categories. 2. Select the trap type. <p>NOTE: If you do not configure categories, all trap types are included in trap notifications.</p> <ol style="list-style-type: none"> 3. On routers, choose an Otn Alarm and a Sonet Alarm for your trap category.
Targets	Specifies the IPv4 or IPv6 address of the systems to receive traps.	<ol style="list-style-type: none"> 1. Expand the trap-group tree and select Targets. 2. Click the New button or select an OID and click the Edit button. 3. Enter the IPv4 or IPv6 addresses of the system (do not enter hostnames).

- Related Documentation**
- [Configuring Basic System Identification for SNMP \(NSM Procedure\) on page 523](#)
 - [Configuring SNMP Communities \(NSM Procedure\) on page 524](#)
 - [Configuring SNMP Views \(NSM Procedure\) on page 528](#)

Configuring SNMP Views (NSM Procedure)

By default, an SNMP community grants read access and denies write access to all supported MIB objects, including communities configured for read-write authorization. To restrict or grant read or write access to a set of MIB objects, configure a MIB view and associate the view with a community. Each MIB object of a view has a common object identifier (OID) prefix. Each OID represents a subtree of the MIB object hierarchy. The subtree can be represented either by a sequence of integers separated by periods (such as 1.3.6.1.2.1.2) or by its subtree name (such as interfaces). Use a view to specify a group of MIB objects on which to define access. You can also use the wildcard character asterisk (*) to include OIDs that match a particular pattern in the SNMP view. To enable a view, associate it with a community.

To configure SNMP views in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **SNMP**.
5. Select **View**.
6. Select the **Enable Feature** check box.
7. Enter the parameters as specified in [Table 321 on page 528](#).
8. Click one:
 - **OK**—To save the changes.
 - **Cancel**—To cancel the modifications.
 - **Apply**—To apply the SNMP settings.

Table 321: Configuring SNMP View Fields

Option	Function	Your Action
Name	Specifies a name for the view.	Enter a name for the view.
OID	Specifies an OID used to represent a subtree of MIB objects.	<ol style="list-style-type: none"> 1. Expand the View tree and select oid. 2. Click the New button or select an OID and click the Edit button.
Name	Specifies the MIB for the view.	Enter the OID of the MIB in either dotted-integer format or subtree-name format.

Table 321: Configuring SNMP View Fields (*continued*)

Option	Function	Your Action
Include or Exclude	Specifies whether the view includes or excludes the set of MIB objects.	Select exclude to exclude the subtree of MIB objects represented by the specified OID. Select include to include the subtree of MIB objects represented by the specified OID.

**Related
Documentation**

- [Configuring Basic System Identification for SNMP \(NSM Procedure\) on page 523](#)
- [Configuring SNMP Communities \(NSM Procedure\) on page 524](#)
- [Configuring SNMP Trap Groups \(NSM Procedure\) on page 526](#)

CHAPTER 25

Configuration of System

- [Configuring Accounting \(NSM Procedure\) on page 531](#)
- [Configuring Archival \(NSM Procedure\) on page 535](#)
- [Configuring ARP \(NSM Procedure\) on page 536](#)
- [Configuring Auto Configuration \(NSM Procedure\) on page 537](#)
- [Configuring a Backup Router \(NSM Procedure\) on page 539](#)
- [Configuring a Commit \(NSM Procedure\) on page 540](#)
- [Configuring Diag Port Authentication \(NSM Procedure\) on page 540](#)
- [Configuring a Domain Search \(NSM Procedure\) on page 541](#)
- [Configuring Extensions \(NSM Procedure\) on page 541](#)
- [Configuring an Inet6 Backup Router \(NSM Procedure\) on page 544](#)
- [Configuring Internet Options \(NSM Procedure\) on page 545](#)
- [Configuring Location \(NSM Procedure\) on page 548](#)
- [Configuring Login \(NSM Procedure\) on page 549](#)
- [Configuring a Name Server \(NSM Procedure\) on page 554](#)
- [Configuring PIC Console Authentication \(NSM Procedure\) on page 555](#)
- [Configuring Ports \(NSM Procedure\) on page 555](#)
- [Configuring RADIUS Options \(NSM Procedure\) on page 556](#)
- [Configuring RADIUS Server \(NSM Procedure\) on page 557](#)
- [Configuring Root Authentication \(NSM Procedure\) on page 558](#)
- [Configuring Static Host Mapping \(NSM Procedure\) on page 559](#)
- [Configuring TACACS+ Options \(NSM Procedure\) on page 560](#)
- [Configuring TACACS+ Server \(NSM Procedure\) on page 561](#)

Configuring Accounting (NSM Procedure)

The accounting feature directs the voice daemon to generate and collect call records, write them to a file, and store them in an archive.

To configure the accounting feature:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the accounting feature.
3. Click the **Configuration** tab. In the configuration tree, select **System > Accounting**.
4. Enter a comment in the Accounting workspace that describes the accounting.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the accounting parameters.

You can configure the following options with accounting feature:

- [Configuring Destination on page 532](#)
- [Configuring Events on page 534](#)
- [Configuring Traceoptions on page 534](#)

Configuring Destination

To configure destination:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the destination.
3. Click the **Configuration** tab. In the configuration tree, select **System > Accounting > Destination**.
4. Select the **Enable Feature** check box to enable this feature.
5. Enter a comment in the Destination workspace that describes the destination.
6. Add or modify settings as specified in [Table 322 on page 532](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the destination settings.

Table 322: Destination Configuration Details

Option	Function	Your Action
System > Accounting > Destination > Radius		
Enable Feature	Enables to configure the radius feature of the destination option.	Select the Enable Feature check box to enable this feature.

Table 322: Destination Configuration Details (*continued*)

Option	Function	Your Action
Comment	Supplies a descriptive comment for the radius.	(Optional) Enter a comment.
System > Accounting > Destination > Radius > Server		
Name	Specifies the radius server address name.	Enter the radius server address name.
Comment	Supplies a descriptive comment for the radius server.	(Optional) Enter a comment.
Port	Specifies the radius server authentication port number.	Set the radius server authentication port number. Range: 1 - 65535.
Accounting Port	Specifies the radius server accounting port number.	Set the radius server accounting port number. Range: 1 - 65535.
Secret	Specifies the shared secret with the radius server.	Enter the password for the secret with the radius server.
Timeout	Specifies the request timeout period of the radius server.	Set the request timeout period of the radius server. Range: 1 - 90.
Retry	Specifies the number of retry attempts.	Set the retry attempts. Range: 1 - 10.
Source Address	Specifies the source address of the radius.	Enter a source address for the radius.
System > Accounting > Destination > Tacplus		
Enable Feature	Enables to configure the tacplus feature of the destination option.	Select the Enable Feature check box to enable this feature.
Comment	Supplies a descriptive comment for the tacplus.	(Optional) Enter a comment.
System > Accounting > Destination > Tacplus > Server		
Name	Specifies the TACACS+ authentication server address name.	Enter the TACACS+ authentication server address name.
Comment	Supplies a descriptive comment for the TACACS+ authentication server.	(Optional) Enter a comment.
Port	Specifies the TACACS+ authentication server port number.	Set the TACACS+ authentication server port number. Range: 1 - 65535.
Secret	Specifies the shared secret with the authentication server.	Enter the password for the secret with the authentication server.
Timeout	Specifies the request time period of the authentication server.	Set the request timeout period of the authentication server. Range: 1 - 90.

Table 322: Destination Configuration Details (*continued*)

Option	Function	Your Action
Single Connection	Specifies the attempts that the optimize TCP connection tries.	Enable the Single Connection check box to enable this feature.
Source Address	Specifies the source address of the authentication server.	Enter a source address for the authentication server.

Configuring Events

To configure events:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the events.
3. Click the **Configuration** tab. In the configuration tree, select **System > Accounting > Events**.
4. Click + to add a new event.
5. Select the available event from the list.
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the event settings.

Configuring Traceoptions

The traceoptions feature allows you to configure file and flag options.

To configure traceoptions:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the traceoptions.
3. Click the **Configuration** tab. In the configuration tree, select **System > Accounting > Traceoptions**.
4. Enter a comment for the traceoptions.
5. Select the **No Remote Trace** check box to enable remote tracing.
6. Add or modify settings as specified in [Table 323 on page 535](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

- **Apply**—Applies the traceoptions settings.

Table 323: File and Flag Configuration Details

Option	Function	Your Action
System > Accounting > Traceoptions > File		
Comment	Supplies a descriptive comment for the filename.	(Optional) Enter a comment.
Filename	Specifies the filename to write the traceoptions.	Enter a filename.
Size	Specifies the maximum size of the trace files.	Enter the maximum file size.
Files	Specifies the maximum number of trace files.	Set the maximum number of trace files. Range: 2 - 1000.
None	Specifies that neither the world-readable nor the no-world-readable option is enabled.	Select the option.
world-readable	Allows any user to read the log file.	(Optional) Select the option.
no-world-readable	Prevents any user from reading the log file.	(Optional) Select the option.
System > Accounting > Traceoptions > Flag		
Name	Specifies the trace flag name.	Enter a trace flag name.
Comment	Supplies a descriptive comment for the trace flag.	(Optional) Enter a comment.

**Related
Documentation**

- [Configuring Archival \(NSM Procedure\) on page 535](#)
- [Configuring ARP \(NSM Procedure\) on page 536](#)
- [Configuring Auto Configuration \(NSM Procedure\) on page 537](#)

Configuring Archival (NSM Procedure)

To configure the archival feature:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the archival feature.
3. Click the **Configuration** tab. In the configuration tree, select **System > Archival**.
4. Enter a comment in the Archival workspace that describes the archival feature.
5. In the configuration tree, select **System > Archival > Configuration**.
6. Enter a comment in the Configuration workspace that describes the configuration of the archival feature.

7. Add or modify settings as specified in [Table 324 on page 536](#).
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the archival configuration settings.

Table 324: Archival Configuration Details

Option	Function	Your Action
System > Archival > Configuration > Archive Sites		
Name	Specifies the URLs to receive the configuration files.	Enter a flag name.
Comment	Supplies a descriptive comment for the archive site.	(Optional) Enter a comment.
Password	Specifies the password to login into the archive site.	Enter the password.
System > Archival > Configuration > Transfer Interval		
transfer-interval	Specifies (in minutes) the interval between data transfers.	Set the transfer interval time. Range: 0 - 2880.
transfer-on-commit	Configures the router to transfer its currently active configuration to an archive site each time you commit a candidate configuration.	Select the transfer-on-commit check box to enable this feature.

Related Documentation

- [Configuring Accounting \(NSM Procedure\) on page 531](#)
- [Configuring ARP \(NSM Procedure\) on page 536](#)
- [Configuring Auto Configuration \(NSM Procedure\) on page 537](#)

Configuring ARP (NSM Procedure)

The address resolution protocol (ARP) is a protocol that is used to identify the hardware address of a network host. To configure ARP:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the ARP.
3. Click the **Configuration** tab. In the configuration tree, select **System > Arp**.
4. Select **Enable Feature** to enable this feature.
5. Add or modify settings as specified in [Table 325 on page 537](#).
6. Click one:
 - **OK**—Saves the changes.

- **Cancel**—Cancels the modifications.
- **Apply**—Applies the ARP configuration settings.

Table 325: Arp Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the ARP.	(Optional) Enter a comment.
Aging Timer	Specifies the change in the ARP aging time value.	Set the aging timer value. Range: 1 - 240.
Passive Learning	Specifies the ARP passive learning.	Select the Passive Learning check box to enable this feature.
Purging	Specifies that the ARP purges when the link goes down.	Select the Purging check box to enable this feature.
Gratuitous Arp On Ifup	Specifies the gratuitous ARP announcement on the interface up.	Select the Gratuitous Arp On Ifup check box to enable this feature.
Gratuitous Arp Delay	Specifies the delay in the gratuitous Arp request.	Set the gratuitous ARP delay value. Range: -2147483648 - 2147483647.
System > Arp > Interfaces		
Comment	Supplies a descriptive comment for the interface.	(Optional) Enter a comment.
System > Arp > Interfaces > Arp Interface		
Name	Specifies the logical interface name for the ARP interface.	Enter an ARP interface name.
Comment	Supplies a descriptive comment for the ARP interfaces.	(Optional) Enter a comment.
Aging Timer	Specifies the change in the ARP aging time value.	Set the aging timer value. Range: 1 - 240.

Related Documentation

- [Configuring Archival \(NSM Procedure\) on page 535](#)
- [Configuring Accounting \(NSM Procedure\) on page 531](#)
- [Configuring Auto Configuration \(NSM Procedure\) on page 537](#)

Configuring Auto Configuration (NSM Procedure)

To configure the auto configuration feature:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the auto configuration feature.
3. Click the **Configuration** tab. In the configuration tree, select **System > Auto Configuration**.

4. Select **Enable Feature** check box to enable this feature.
5. Enter a comment in the Auto Configuration workspace that describes the auto configuration.
6. Add or modify settings as described in [Table 326 on page 538](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the auto configuration parameters.

Table 326: Auto Configuration Traceoptions Details

Option	Function	Your Action
System > Auto Configuration > Traceoptions		
Comment	Supplies a descriptive comment for the traceoptions.	(Optional) Enter a comment.
No Remote Trace	Specifies that the remote tracing is disabled, upon selecting the check box.	Select the No remote Trace check box to enable this feature.
Level	Specifies the level of debugging output.	Select an option from the list.
System > Auto Configuration > Traceoptions > File		
Comment	Supplies a descriptive comment for the filename.	(Optional) Enter a comment.
Filename	Specifies the filename in which to write the trace information.	Enter the filename.
Size	Specifies the maximum trace file size.	Enter the maximum trace file size.
Files	Specifies the maximum number of trace files.	Set the maximum number of trace files. Range: 2 - 1000.
None	Specifies that neither the world-readable nor the no-world-readable option is enabled.	Select the option.
world-readable	Allows any user to read the log file.	(Optional) Select the option.
no-world-readable	Prevents any user from reading the log file.	(Optional) Select the option.
Match	Specifies the regular expression for the lines to be logged.	Enter the regular expression for the lines to be logged.
System > Auto Configuration > Traceoptions > Flag		
Name	Specifies the trace flag name.	Enter a trace flag name.

Table 326: Auto Configuration Traceoptions Details (*continued*)

Option	Function	Your Action
Comment	Supplies a descriptive comment for the trace flag.	(Optional) Enter a comment.

Related Documentation

- [Configuring ARP \(NSM Procedure\) on page 536](#)
- [Configuring Archival \(NSM Procedure\) on page 535](#)
- [Configuring Accounting \(NSM Procedure\) on page 531](#)

Configuring a Backup Router (NSM Procedure)

During the time that the router is booting, the routing protocol process (RPD) is not running; therefore, the router has no static or default routes. When the routing protocol process fails to start properly, it stops the router from booting. To allow the router to boot and also to ensure that the router is reachable over the network, you configure a backup router. A backup router is a router that is directly connected to the local router (that is, on the same subnet).

To configure a backup router:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the backup router.
3. Click the **Configuration** tab. In the configuration tree, select **System > Backup Router**.
4. Enter a comment in the Backup Router workspace that describes the backup router.
5. Enter an address in the Backup Router workspace for the backup router to use while booting.
6. In the configuration tree, select **System > Backup Router > Destination**.
7. Click + to enter a new destination address for the backup router.
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the backup router configuration settings.

Related Documentation

- [Configuring Authentication Order \(NSM Procedure\) on page 109](#)
- [Configuring Auto Configuration \(NSM Procedure\) on page 537](#)
- [Configuring a Commit \(NSM Procedure\) on page 540](#)

Configuring a Commit (NSM Procedure)

You can configure a commit to automatically result in a commit and synchronize the actions between dual routing engines within the same chassis.

To configure a commit:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the commit.
3. Click the **Configuration** tab. In the configuration tree, select **System > Commit**.
4. Enter a comment in the Commit workspace that describes the commit.
5. Select the **Synchronize** check box in the Commit workspace, to synchronize the commit on both the routing engines.
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the commit settings.

Related Documentation

- [Configuring Diag Port Authentication \(NSM Procedure\) on page 540](#)
- [Configuring a Domain Search \(NSM Procedure\) on page 541](#)
- [Configuring a Backup Router \(NSM Procedure\) on page 539](#)

Configuring Diag Port Authentication (NSM Procedure)

You can configure passwords for performing diagnostics on the router's System Control Board (SCB), System and Switch Board (SSB), Switching and Forwarding Module (SFM), or Forwarding Engine Board (FEB) ports. This password provides an extra level of security.

To configure diag port authentication:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the diag port authentication.
3. Click the **Configuration** tab. In the configuration tree, select **System > Diag Port Authentication**.
4. In the Diag Port Authentication workspace, enter a plain text password value.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

- **Apply**—Applies the diag port authentication settings.

**Related
Documentation**

- [Configuring a Domain Search \(NSM Procedure\) on page 541](#)
- [Configuring a Backup Router \(NSM Procedure\) on page 539](#)
- [Configuring Extensions \(NSM Procedure\) on page 541](#)

Configuring a Domain Search (NSM Procedure)

You can configure the name of the domain in which the clients search for a dynamic host configuration protocol (DHCP) server host. The domain name is appended to hostnames that are not fully qualified. If you do not configure a domain name, the default is the client's current domain. The domain search sets the order in which the clients append domain names when searching for the IP address of a host. You can include one or more domain names in the list.

To configure a domain search:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the domain search.
3. Click the **Configuration** tab. In the configuration tree, select **System > Domain Search**.
4. Click + to enter a new domain search name.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the domain search settings.

**Related
Documentation**

- [Configuring a Backup Router \(NSM Procedure\) on page 539](#)
- [Configuring Extensions \(NSM Procedure\) on page 541](#)
- [Configuring Diag Port Authentication \(NSM Procedure\) on page 540](#)

Configuring Extensions (NSM Procedure)

The extensions feature allows you to configure the providers and the resource limits.

To configure extensions:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the extensions feature.
3. Click the **Configuration** tab. In the configuration tree, select **System > Extensions**.

4. Select **Enable Feature** check box to enable this feature.
5. Enter a comment for the extensions feature.
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the extensions parameters.
- [Configuring Providers on page 542](#)
- [Configuring Resource Limits on page 542](#)

Configuring Providers

To configure providers:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the providers.
3. Click the **Configuration** tab. In the configuration tree, select **System > Extensions > Providers**.
4. Add or modify settings as specified in [Table 327 on page 542](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the provider settings.

Table 327: Provider Configuration Details

Option	Function	Your Action
Name	Specifies the provider name.	Enter a provider name.
Comment	Supplies a descriptive comment for the provider.	(Optional) Enter a comment.
New deployment-scope	Specifies the deployment scope.	Enter a new deployment scope name.

Configuring Resource Limits

To configure resource limits:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the resource limits.
3. Click the **Configuration** tab. In the configuration tree, select **System > Extensions > Resource Limits**.

4. Enter a comment for the resource limits.
5. Add or modify settings as specified in [Table 328 on page 543](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the resource limits settings.



NOTE: You can configure a package or a process resource limit feature from the below table.

Table 328: Resource Limits Configuration Details

Option	Function	Your Action
Name	Specifies the name of the package or the process resource limit.	Enter a name.
Comment	Supplies a descriptive comment for the package or the process resource limit.	(Optional) Enter a comment.
package/process > Resources		
Enable Feature	Specifies that you can enable the package or the process resources configuration feature.	Select the Enable Feature check box to enable this feature.
Comment	Supplies a descriptive comment for the package or the process resources.	(Optional) Enter a comment.
package/process > Resources > Cpu		
Comment	Supplies a descriptive comment for the CPU.	(Optional) Enter a comment
Priority	Specifies the highest priority level that the process can run.	Set the priority value. Range: -2147483648 - 2147483647.
Time	Specifies the maximum amount of CPU time that can be accumulated.	Set the CPU time. Range: 0 - 2147483647.
package/process > Resources > File		
Comment	Supplies a descriptive comment for the file.	(Optional) Enter a comment.
Size	Specifies the maximum size of a file that can be created.	Enter the file size.
Open	Specifies the maximum number of simultaneous open files.	Set the number of open files. Range: 0 - 2147483647.
Core Size	Specifies the maximum size of a core file that can be created.	Enter the core file size.

Table 328: Resource Limits Configuration Details (*continued*)

Option	Function	Your Action
package/process > Resources > Memory		
Comment	Supplies a descriptive comment for the memory.	(Optional) Enter a comment.
Data Size	Specifies the maximum size of the data segment.	Enter the data size.
Locked In	Specifies the maximum bytes that the memory can lock into it.	Enter the locked in size.
Resident Set Size	Specifies the maximum amount of private physical memory at any given moment.	Enter the resident set size.
Socket Buffers	Specifies the maximum amount of physical memory that may be dedicated to the socket buffers.	Enter the memory size for the socket buffers.
Stack Size	Specifies the maximum size of the stack segment.	Enter the stack segment size.

Related Documentation

- [Configuring a Domain Search \(NSM Procedure\) on page 541](#)
- [Configuring Diag Port Authentication \(NSM Procedure\) on page 540](#)
- [Configuring a Commit \(NSM Procedure\) on page 540](#)

Configuring an Inet6 Backup Router (NSM Procedure)

You can configure a backup router running Internet Protocol Version 6 (IPv6). This is to use while the local router or switch (running IPv6) is booting and if the routing protocol processes fail to start. The Junos OS removes the route to this router or switch as soon as the software starts.

To configure an Inet6 backup router:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the Inet6 backup router.
3. Click the **Configuration** tab. In the configuration tree, select **System > Inet6 Backup Router**.
4. Add or modify the settings as described in [Table 329 on page 545](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the Inet6 backup router settings.

Table 329: Inet6 Backup Router Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment of the Inet6 backup router.	(Optional) Enter a comment.
Address	Specifies the address of the router to use while booting.	Enter an address name for the router.
Destination	Specifies the destination network that is reachable through the router.	Enter the destination name for the router.

Related Documentation

- [Configuring Internet Options \(NSM Procedure\) on page 545](#)
- [Configuring Location \(NSM Procedure\) on page 548](#)
- [Configuring Login \(NSM Procedure\) on page 549](#)

Configuring Internet Options (NSM Procedure)

You can configure the system Internet Protocol (IP) options to protect the system against certain types of Denial of Service (DoS) attacks.

To configure Internet options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the internet options.
3. Click the **Configuration** tab. In the configuration tree, select **System > Internet Options**.
4. Add or modify the settings as specified in [Table 330 on page 545](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the internet options configuration settings.

Table 330: Internet Options Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the internet option.	(Optional) Enter a comment.

Table 330: Internet Options Configuration Details (*continued*)

Option	Function	Your Action
None / path-mtu-discovery / no-path-mtu-discovery	Specifies that you can determine the Maximum Transmission Unit (MTU) size on the network path between two IP hosts.	<p>Select an option.</p> <ul style="list-style-type: none"> • path-mtu-discovery-Path MTU discovery is enabled. • no-path-mtu-discovery-Path MTU discovery is disabled. • None-Path MTU discovery is neither enabled nor disabled.
None / gre-path-mtu-discovery / no-gre-path-mtu-discovery	Specifies that you can configure a path MTU discovery for outgoing Generic Routing Encapsulation (GRE) tunnel connections.	<p>Select an option.</p> <ul style="list-style-type: none"> • gre-path-mtu-discovery-GRE path MTU discovery is enabled. • no-gre-path-mtu-discovery-GRE path MTU discovery is disabled. • None-GRE path MTU discovery is neither enabled nor disabled.
None / ipip-path-mtu-discovery / no-ipip-path-mtu-discovery	Specifies that you can configure path MTU discovery for outgoing IP-IP tunnel connections.	<p>Select an option.</p> <ul style="list-style-type: none"> • ipip-path-mtu-discovery-IP-IP path MTU discovery is enabled. • no-ipip-path-mtu-discovery-IP-IP path MTU discovery is disabled. • None-IP-IP path MTU discovery is neither enabled nor disabled.
None / source-quench / no-source-quench	Specifies that you can configure how the Junos OS would handle the Internet Control Message Protocol (ICMP) source quench messages.	<p>Select an option:</p> <ul style="list-style-type: none"> • source-quench-The Junos OS ignores the ICMP source quench messages. • no-source-quench-The Junos OS does not ignore the ICMP source quench messages. • None-ICMP source quench message is neither enabled nor disabled.
Tcp Drop Synfin Set	Specifies that the TCP packets that have both SYN and FIN flags can be dropped.	Select Tcp Drop Synfin Set to enable this feature.
No Tcp Rfc1323	Specifies that you can configure the Junos OS to disable RFC 1323 TCP extensions.	Select No Tcp Rfc1323 to enable this feature.
No Tcp Rfc1323 Paws	Specifies that you can configure the Junos OS to disable the RFC 1323 Protection Against Wrapped Sequence (PAWS) number extension.	Select No Tcp Rfc1323 Paws to enable this feature.

Table 330: Internet Options Configuration Details (*continued*)

Option	Function	Your Action
None / ipv6-reject-zero-hop-limit / no-ipv6-reject-zero-hop-limit	Specifies that you can enable and disable rejection of incoming IPv6 packets that have a zero hop-limit value in their header.	Select an option. <ul style="list-style-type: none"> ipv6-reject-zero-hop-limit-Rejection of incoming IPv6 packets that have a zero hop-limit value is enabled. no-ipv6-reject-zero-hop-limit-Rejection of incoming IPv6 packets that have a zero hop-limit value is disabled. None- Rejection of incoming IPv6 packets that have a zero hop-limit value is neither enabled nor disabled.
IPv6 Duplicate Addr Detection Transmits	Specifies the number of attempts for IPv6 duplicate address detection that can be controlled.	Set the number of attempts. Range: 0 - 4,294,967,295. Default value is 3.
None / ipv6-path-mtu-discovery / no-ipv6-path-mtu-discovery	Specifies that you can configure path MTU discovery for IPv6 packets.	Select an option. <ul style="list-style-type: none"> ipv6-path-mtu-discovery-IPv6 path MTU discovery is enabled. no-ipv6-path-mtu-discovery-IPv6 path MTU discovery is disabled. None-IPv6 path MTU discovery is neither enabled nor disabled.
IPv6 Path Mtu Discovery Timeout	Specifies the IPv6 path MTU discovery timeout.	Set the IPv6 path MTU discovery timeout. Range: 0 - 4,294,967,295. Default value is 10.
No Tcp Reset	Specifies not to send the reset RST TCP packet for packets sent to non-listening ports.	Select an option from the list.
Internet Options > Icmpv4 Rate Limit / Icmpv6 Rate Limit		
Comment	Supplies a descriptive comment for the ICMPv4/ICMPv6 rate limit.	(Optional) Enter a comment.
Packet Rate	Specifies the ICMP rate-limiting packets earned per second.	Set the packet rate value. Range: 0 - 4,294,967,295. Default value is 1,000.
Bucket Size	Specifies the maximum bucket size for the ICMP rate limit.	Set the bucket size value. Range: 0 - 4,294,967,295. Default value is 5.
Internet Options > Source Port		
Comment	Supplies a descriptive comment for the source port.	(Optional) Enter a comment.
Upper Limit	Specifies the upper limit of the source port selection range.	Set the upper limit value. Range: 5,000 - 65,535. Default value is none.

- Related Documentation**
- [Configuring an Inet6 Backup Router \(NSM Procedure\) on page 544](#)
 - [Configuring Extensions \(NSM Procedure\) on page 541](#)
 - [Configuring a Name Server \(NSM Procedure\) on page 554](#)

Configuring Location (NSM Procedure)

To configure location:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure a location.
3. Click the **Configuration** tab. In the configuration tree, select **System > Location**.
4. Add or modify the settings as specified in [Table 331 on page 548](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the location settings.

Table 331: Location Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the location.	(Optional) Enter a comment.
Country Code	Specifies the two letter country code for the location.	Enter the country code for the location.
Postal Code	Specifies the zip code or the postal code for the location.	Enter the zip code or the postal code of the location.
Npa Nxx	Specifies the first six digits of the phone number (area code with the exchange number).	Enter the phone number (area code with the exchange number).
Latitude	Specifies the latitude in degree format.	Enter the latitude of the location.
Longitude	Specifies the longitude in degree format.	Enter the longitude of the location.
Altitude	Specifies (in degrees) the altitude (feet above or below the sea level).	Set the altitude of the location. Range: -2147483648 - 2147483647.
Lata	Specifies the long distance service area.	Enter a long distance service area of the location.
Vcoord	Specifies the Bellcore vertical coordinate information.	Enter a Bellcore vertical coordinate value.
Hcoord	Specifies the Bellcore horizontal coordinate information.	Enter a Bellcore horizontal coordinate value.

Table 331: Location Details (*continued*)

Option	Function	Your Action
Building	Specifies the building name.	Enter the building name.
Floor	Specifies the floor of the building.	Enter the floor of the building.
Rack	Specifies the rack number.	Enter the rack number.
Location > Lcc		
Name	Specifies the name for the LCC number.	Set a name for the LCC number. Range: 0 - 3.
Comment	Supplies a descriptive comment for the LCC.	(Optional) Enter a comment.
Floor	Specifies the floor of the building.	Enter the floor of the building.
Rack	Specifies the rack number	Enter the rack number.

Related Documentation

- [Configuring an Inet6 Backup Router \(NSM Procedure\) on page 544](#)
- [Configuring Internet Options \(NSM Procedure\) on page 545](#)
- [Configuring a Name Server \(NSM Procedure\) on page 554](#)

Configuring Login (NSM Procedure)

By default, no login message is displayed. A system login message appears before the user logs in. A system login announcement appears after the user logs in.

To configure the login message:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the login message.
3. Click the **Configuration** tab. In the configuration tree, select **System > Login**.
4. Enter a comment in the Login workspace that describes the system login.
5. Enter an announcement in the Login workspace that describes the system announcement message.
6. Enter a message in the Login workspace that describes the system login message.
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

- **Apply**—Applies the login parameters.

You can configure the following options while configuring a system login:

- [Configuring Class on page 550](#)
- [Configuring Password on page 551](#)
- [Configuring Retry Options on page 552](#)
- [Configuring User on page 553](#)

Configuring Class

To configure class:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the class.
3. Click the **Configuration** tab. In the configuration tree, select **System > Login > Class**.
4. Add or modify settings as specified in [Table 332 on page 550](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the class settings.

Table 332: Class Configuration Details

Option	Function	Your Action
System > Login > Class > class		
Name	Specifies the login class name.	Enter the login class name.
Comment	Supplies a descriptive comment for the class.	(Optional) Enter a comment.
Access Start	Specifies the start time for the remote access.	Enter the start time in hh:mm format.
Access End	Specifies the end time for the remote access.	Enter the end time in hh:mm format.
Idle Timeout	Specifies the maximum idle time before logging out.	Set the maximum idle time. Range: 0 - 4,294,967,295.
Login Alarms	Specifies the display system alarms when logging in.	Enable the Login Alarms check box to enable this feature.
Login Script	Specifies that you can execute this login script while logging in.	Enter a login script.
Login Tip	Specifies the display login tip when logging in.	Enable the Login Tip check box to enable this feature.

Table 332: Class Configuration Details (*continued*)

Option	Function	Your Action
Allow Commands	Specifies the regular expression for commands to allow explicitly.	Enter the allow commands.
Deny Commands	Specifies the regular expression for commands to deny explicitly.	Enter the deny commands.
Allow Configuration	Specifies the regular expression for configuring the class to allow explicitly.	Enter the allow configure commands.
Deny Configuration	Specifies the regular expression for configuring the class to deny explicitly.	Enter the deny configure commands.
System > Login > Class > class > Allowed Days		
New allowed-days	Specifies the day of the week that is allowed to configure the class.	Select a day of the week from the list.
System > Login > Class > class > Permissions		
New permissions	Specifies the permission required to configure the class.	Enter the permission.

Configuring Password

To configure password:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the password.
3. Click the **Configuration** tab. In the configuration tree, select **System > Login > Password**.
4. Add or modify settings as described in [Table 333 on page 551](#)
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the password settings.

Table 333: Password Configuration Details

Option	Function	Your Action
System > Login > Password		
Comment	Supplies a descriptive comment for the password.	(Optional) Enter a comment.
Minimum Length	Specifies the minimum password length size for all users.	Set the minimum password length size. Range: 6 - 20.

Table 333: Password Configuration Details (*continued*)

Option	Function	Your Action
Maximum Length	Specifies the maximum password length size for all users.	Set the maximum password length size. Range: 20 - 128.
Change Type	Specifies whether the password is checked for either character-sets or set-transitions .	Select an option from the list. <ul style="list-style-type: none"> • character-sets—The total number of character sets used. • set-transitions—The total number of character set changes.
Minimum Changes	Specifies how many character sets or character set changes are required for the password.	Set the minimum changes required for the password.
Format	Specifies the hash algorithm (md5, sha1 or des) for authenticating plain-text passwords.	Select either md5 , or sha1 , or des from the list. The default format is md5 .

Configuring Retry Options

The retry option allows you to calculate the maximum number of times a user can attempt to enter a password while logging in through SSH or Telnet, before being disconnected.

To configure retry options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the retry options.
3. Click the **Configuration** tab. In the configuration tree, select **System > Login > Retry Options**.
4. Add or modify settings as specified in [Table 334 on page 552](#)
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the retry options settings.

Table 334: Retry Options Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the retry options.	(Optional) Enter a comment.
Tries Before Disconnect	Specifies the maximum number of times a user is allowed to attempt to enter a password to log in through SSH or Telnet.	Set the maximum number of times a user is allowed to attempt to enter a password. Range: 1 - 10.

Table 334: Retry Options Configuration Details (*continued*)

Option	Function	Your Action
Backoff Threshold	Specifies the threshold for the number of failed login attempts before the user experiences a delay when attempting to reenter a password.	Set the backoff threshold value. Range: 1 - 3.
Backoff factor	Specifies the length of delay after each failed login attempt.	Set the backoff factor value. Range: 5 - 10.
Minimum Time	Specifies the minimum length of time that the connection remains open while the user is attempting to enter a password to log in.	Set the minimum time. Range: 20 - 60.
Maximum Time	Specifies the maximum length of time that the connection remains open for the user to enter a username and password to log in.	Set the maximum time. Range: 20 - 300.

Configuring User

The user configuration feature allows you to configure access permission for individual users.

To configure a user:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the user.
3. Click the **Configuration** tab. In the configuration tree, select **System > Login > User**.
4. Add or modify settings as specified in [Table 335 on page 553](#)
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the user settings.

Table 335: User Configuration Details

Option	Function	Your Action
System > Login > User > user		
Name	Specifies the user name.	Enter the user name.
Comment	Supplies a descriptive comment for the user.	(Optional) Enter a comment.
Full Name	Specifies the complete name of the user.	Enter the complete name.
Uid	Specifies the user identifier for a login account.	Set the user identifier. Range: 100 - 64000.

Table 335: User Configuration Details (*continued*)

Option	Function	Your Action
Class	Specifies the login class name.	Select a login class name from the list.
System > Login > User > user > Authentication		
Plain Text Password Value	Specifies the plain text password. The user interface (UI) prompts for the password and encrypts it.	Enter a plain text password.
System > Login > User > user > Authentication > Ssh Dsa / Ssh Rsa		
Name	Specifies the ssh Dsa or ssh Rsa name.	Enter a name.
Comment	Supplies a descriptive comment for the ssh..	(Optional) Enter a comment.
From	Specifies the pattern list of allowed hosts.	Enter the pattern-list of allowed hosts.

**Related
Documentation**

- [Configuring Location \(NSM Procedure\) on page 548](#)
- [Configuring Internet Options \(NSM Procedure\) on page 545](#)
- [Configuring a Name Server \(NSM Procedure\) on page 554](#)

Configuring a Name Server (NSM Procedure)

You can configure one or more domain name system (DNS) name servers, to have the router resolve the host names into addresses.

To configure a DNS name server:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure the DNS name server.
3. Click the **Configuration** tab. In the configuration tree, select **System > Name Server**.
4. Click + to add a new name server.
5. Enter a DNS name server address in the name-server workspace.
6. Enter a comment for the DNS name server in the name-server workspace.
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the name server settings.

**Related
Documentation**

- [Configuring Login \(NSM Procedure\) on page 549](#)

- [Configuring Location \(NSM Procedure\) on page 548](#)
- [Configuring Internet Options \(NSM Procedure\) on page 545](#)

Configuring PIC Console Authentication (NSM Procedure)

You can configure console access to Physical Interface Cards (PICs).

To configure a PIC console authentication:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab. Then double-click the device for which you want to configure the PIC console authentication.
3. Click the **Configuration** tab. In the configuration tree, select **System > Pic Console Authentication**.
4. Enter a plain text password in the PIC Console Authentication workspace.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the PIC console authentication settings.

Related Documentation

- [Configuring a Name Server \(NSM Procedure\) on page 554](#)
- [Configuring Login \(NSM Procedure\) on page 549](#)
- [Configuring Location \(NSM Procedure\) on page 548](#)

Configuring Ports (NSM Procedure)

The router's craft interface has two ports for connecting terminals to the router such as auxiliary and console ports.

To configure ports:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab. Then double-click the device for which you want to configure the ports.
3. Click the **Configuration** tab. In the configuration tree, select **System > Ports**.
4. Enter a comment in the Ports workspace that describes the ports.
5. Add or modify the settings as specified in [Table 336 on page 556](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

- **Apply**—Applies the port configuration settings.



NOTE: You can either set auxiliary or console ports from the below table descriptions.

Table 336: Port Configuration Details

Option	Function	Your Action
Ports > Auxiliary/Console		
Comment	Supplies a descriptive comment of the auxiliary/console port.	(Optional) Enter a comment.
Log Out On Disconnect	Specifies that the console session logs out when the cable is unplugged.	Select the Log Out On Disconnect check box to enable this feature.
Disable	Specifies that the auxiliary/console port is disabled.	Select the Disable check box to enable this feature.
Insecure	Specifies that the super user access is not allowed.	Select the Insecure check box to enable this feature.
Type	Specifies the terminal type of the auxiliary/console port.	Select a terminal type from the list.

Related Documentation

- [Configuring PIC Console Authentication \(NSM Procedure\) on page 555](#)
- [Configuring a Name Server \(NSM Procedure\) on page 554](#)
- [Configuring Login \(NSM Procedure\) on page 549](#)

Configuring RADIUS Options (NSM Procedure)

You can configure Remote Authentication Dial In User Service (RADIUS) options for the NAS-IP address for outgoing RADIUS packets and password protocol used in RADIUS packets.

To configure RADIUS options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab. Then double-click the device for which you want to configure radius options.
3. Click the **Configuration** tab. In the configuration tree, select **System > Radius Options**.
4. Enter a comment in the Radius Options workspace that describes the RADIUS options.
5. Select a password protocol in the Radius Options workspace that specifies the password protocol used in the RADIUS packets.

6. Add or modify settings as specified in the [Table 337 on page 557](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the radius option settings.

Table 337: Radius Option Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment of the attributes.	Enter a comment.
Nas IP Address	Specifies the value of NAS-IP address in outgoing RADIUS packets.	Enter the NAS-IP address.

Related Documentation

- [Configuring Ports \(NSM Procedure\) on page 555](#)
- [Configuring PIC Console Authentication \(NSM Procedure\) on page 555](#)
- [Configuring a Name Server \(NSM Procedure\) on page 554](#)

Configuring RADIUS Server (NSM Procedure)

A Remote Authentication Dial-In User Service (RADIUS) server is a type of server that allows you to centralize authentication and accounting for remote users.

To configure a RADIUS server:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab. Then double-click the device for which you want to configure the RADIUS server.
3. Click the **Configuration** tab. In the configuration tree, select **System > Radius Server**.
4. Add or modify settings as specified in the [Table 338 on page 557](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the RADIUS server settings.

Table 338: RADIUS Server Configuration Details

Option	Function	Your Action
Name	Specifies the RADIUS server address name.	Enter the RADIUS server address name.
Comment	Supplies a descriptive comment of the RADIUS server.	(Optional) Enter a comment.

Table 338: RADIUS Server Configuration Details (*continued*)

Option	Function	Your Action
Port	Specifies the RADIUS server authentication port number.	Set the RADIUS server authentication port number. Range: 1 - 65535.
Accounting Port	Specifies the RADIUS server accounting port number.	Set the RADIUS server accounting port number. Range: 1 - 65535.
Secret	Specifies the password to use with the RADIUS server. The secret password used by the local router must match that used by the server.	Enter the shared secret password to use with the RADIUS server.
Timeout	Specifies the amount of time that the local router waits to receive a response from a RADIUS server.	Enter the request time out period. Range: 1 - 90.
Retry	Specifies the number of times that the router is allowed to attempt to contact a RADIUS authentication or accounting server.	Set the retry attempts. Range: 1 - 10.
Source Address	Specifies the source address for each configured RADIUS server.	Enter the source address.

Related Documentation

- [Configuring Ports \(NSM Procedure\) on page 555](#)
- [Configuring RADIUS Options \(NSM Procedure\) on page 556](#)
- [Configuring a Name Server \(NSM Procedure\) on page 554](#)

Configuring Root Authentication (NSM Procedure)

You can configure the authentication methods for the root-level user, whose username is "root."

To configure root authentication:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab. Then double-click the device for which you want to configure root authentication.
3. Click the **Configuration** tab. In the configuration tree, select **System > Root Authentication**.
4. Enter a plaintext password in the Plain text Password Value.



NOTE: You can specify only one plain text password.

5. Add or modify settings as described in [Table 339 on page 559](#)
6. Click one:

- **OK**—Saves the changes.
- **Cancel**—Cancels the modifications.
- **Apply**—Applies the root authentication settings.

Table 339: Root Authentication Configuration Details

Option	Function	Your Action
System > Login > User > user > Authentication > Ssh Dsa / Ssh Rsa		
Name	Specifies the ssh Dsa or ssh Rsa name	Enter a name.
Comment	Supplies a descriptive comment for the ssh.	(Optional) Enter a comment
From	Specifies the pattern list of allowed hosts.	Enter the pattern-list of allowed hosts.

**Related
Documentation**

- [Configuring RADIUS Server \(NSM Procedure\) on page 557](#)
- [Configuring RADIUS Options \(NSM Procedure\) on page 556](#)
- [Configuring a Name Server \(NSM Procedure\) on page 554](#)

Configuring Static Host Mapping (NSM Procedure)

You can map a hostname to one or more IP addresses and aliases, and you can configure an International Organization for Standardization (ISO) system identifier (system ID).

To configure static host mapping:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab. Then double-click the device for which you want to configure static host mapping.
3. Click the **Configuration** tab. In the configuration tree, select **System > Static Host Mapping**.
4. Click the plus sign (+) to add static host mapping.
5. Add or modify settings as specified in the [Table 340 on page 559](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the static host mapping settings.

Table 340: Static Host Mapping Configuration Details

Option	Function	Your Action
Name	Specifies the fully qualified name of the system.	Enter the name of the system.

Table 340: Static Host Mapping Configuration Details (*continued*)

Option	Function	Your Action
Comment	Supplies a descriptive comment of the system.	(Optional) Enter a comment.
Sysid	Specifies the ISO system ID. This is the 6-byte portion of the Intermediate System-to-Intermediate System (IS-IS) network service access point (NSAP).	Enter the system identifier address. NOTE: We recommend to use the host's IP address represented in binary-coded decimal (BCD) format.
static-host-mapping > Alias/Inet/Inet6		
New	Specifies the hostname information.	Click + to enter any one of the following: <ul style="list-style-type: none"> Alias—Specifies the alias for the hostname. Inet—Specifies one or more IP addresses for the host. Inet6—Specifies the 6 byte IP address for the host.

Related Documentation

- [Configuring Root Authentication \(NSM Procedure\) on page 558](#)
- [Configuring RADIUS Server \(NSM Procedure\) on page 557](#)
- [Configuring RADIUS Options \(NSM Procedure\) on page 556](#)

Configuring TACACS+ Options (NSM Procedure)

You can configure the TACACS+ options for authentication and accounting on the system.

To configure TACACS+ options:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab. Then double-click the device for which you want to configure TACACS+ options.
3. Click the **Configuration** tab. In the configuration tree, select **System > Tacplus options**.
4. Add or modify settings as specified in the [Table 341 on page 560](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the TACACS+ options settings.

Table 341: TACACS+ Options Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the TACACS+ option.	(Optional) Enter a comment.
Service Name	Specifies the TACACS+ service name.	Enter the TACACS+ service name.

Table 341: TACACS+ Options Configuration Details (*continued*)

Option	Function	Your Action
None	Specifies hostname information.	Select the None check box to enable this feature.
no-cmd-attribute-value	Specifies the command attribute value to an empty string in the start and stop request for TACACS+ accounting. This option enables logging of accounting records in the correct log file on a TACACS+ server.	Select the no-cmd-attribute-value check box to enable this feature.
exclude-cmd-attribute	Specifies to exclude the command attribute value completely from start and stop accounting records. This option enables logging of accounting records in the correct log file on a TACACS+ server.	Select the exclude-cmd-attribute check box to enable this feature.

Related Documentation

- [Configuring Root Authentication \(NSM Procedure\) on page 558](#)
- [Configuring RADIUS Server \(NSM Procedure\) on page 557](#)
- [Configuring Static Host Mapping \(NSM Procedure\) on page 559](#)

Configuring TACACS+ Server (NSM Procedure)

To configure a TACACS+ server:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab. Then double-click the device for which you want to configure the TACACS+ server.
3. Click the **Configuration** tab. In the configuration tree, select **System > Tacplus Server**.
4. Add or modify settings as specified in the [Table 342 on page 561](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the TACACS+ server settings.

Table 342: TACACS+ Server Configuration Details

Option	Function	Your Action
Name	Specifies the TACACS+ authentication server address.	Enter the TACACS+ authentication server address name.
Comment	Supplies a descriptive comment of the TACACS+ server.	(Optional) Enter a comment.
Port	Specifies the TACACS+ authentication server port number.	Set the TACACS+ authentication server port number. Range: 0 - 65535.

Table 342: TACACS+ Server Configuration Details (*continued*)

Option	Function	Your Action
Secret	Specifies the password to use with the TACACS+ server.	Enter the secret password. NOTE: The secret password used by the local router must match that used by the server.
Timeout	Specifies the amount of time that the local router waits to receive a response from the TACACS+ server.	Set the timeout for the response from the TACACS+ server. Range: 1 - 90.
Single Connection	Specifies the number of attempts needed to connect to a TACACS+ server. NOTE: The software maintains one open TCP connection to the server for multiple requests, rather than opening a connection for each connection attempt.	Select the Single Connection check box to enable this feature.
Source Address	Specifies the source address for the TACACS+ server.	Enter the source address name.

- Related Documentation**
- [Configuring TACACS+ Options \(NSM Procedure\) on page 560](#)
 - [Configuring RADIUS Server \(NSM Procedure\) on page 557](#)
 - [Configuring Static Host Mapping \(NSM Procedure\) on page 559](#)

PART 4

Management

- [Management of M Series and MX Series Devices on page 565](#)
- [Device Inventory in NSM and the CLI on page 567](#)
- [Topology Manager on page 573](#)

Management of M Series and MX Series Devices

- [Managing M Series and MX Series Device Software Versions on page 565](#)

Managing M Series and MX Series Device Software Versions

You can use Network and Security Manager (NSM) to upgrade or adjust the software on managed M Series and MX Series devices running Junos OS Release 9.3 or later.

When a software upgrade is applied to an M Series or MX Series device with dual Routing Engines, the upgraded software is applied to both Routing Engines. The backup is upgraded first. The router then reboots and the backup becomes the master. Then the former master is upgraded, as is the standard procedure for upgrading M Series and MX Series devices with dual Routing Engines.

For more information and steps about updating the device software version, see “Upgrading the Device Software” in the *Network and Security Manager Administration Guide*.

**Related
Documentation**

- [Viewing and Reconciling Device Inventory on page 567](#)
- [Comparing Device Inventory in NSM and the CLI on page 568](#)

Device Inventory in NSM and the CLI

- [Viewing and Reconciling Device Inventory on page 567](#)
- [Comparing Device Inventory in NSM and the CLI on page 568](#)

Viewing and Reconciling Device Inventory

Device inventory management in Network and Security Manager (NSM) allows you to display information about the hardware, software, and license components of each device. It also provides features to update the NSM database with the most current inventory information from the device. In addition, you can use Device Monitor, Device List, and the device tooltip to view the status of inventory synchronization.

These inventory management features are available for all M Series and MX Series devices. You can use these features to make the NSM database match the device inventory, but you cannot write new inventory information to the device.

Initially, the device inventory in the NSM database is generated when the device is first imported into NSM. Immediately after import, the device inventory in the NSM database matches exactly the inventory on the device itself.

If the hardware on the device is changed, the software is upgraded through the WebUI or CLI, new software packages are installed, and then the inventory on the device is no longer synchronized with the NSM database.

The Device Monitor, Device List, and tooltip shows the hardware and software inventory status for each device. Possible states include:

- In Sync—Inventory in the NSM database matches the device.
- Out of Sync—Inventory in the NSM database does not match the device.
- N/A—Either the device is not yet connected and managed by NSM, or the device is a ScreenOS security device or IDP sensor.

Changes to the device inventory are not automatically updated in the NSM database.

For detailed information about comparing and reconciling device inventory, see the *Network and Security Manager Administration Guide*.

- Related Documentation**
- [Managing M Series and MX Series Device Software Versions on page 565](#)
 - [Comparing Device Inventory in NSM and the CLI on page 568](#)

Comparing Device Inventory in NSM and the CLI

NSM and the Junos OS command-line interface (CLI) display similar information about the device inventory, although screens rendered in NSM look different than the Junos OS CLI. This topic provides an introduction to viewing software and hardware inventory using NSM and compares the NSM view with the CLI output for the same device.

- [Viewing Device Inventory in NSM on page 568](#)
- [Viewing Device Inventory from the CLI on page 570](#)

Viewing Device Inventory in NSM

Purpose NSM displays the hardware and software inventory for each device according to the information it has in its database. For a device with dual Routing Engines, NSM collects the inventory data from the master Routing Engine.

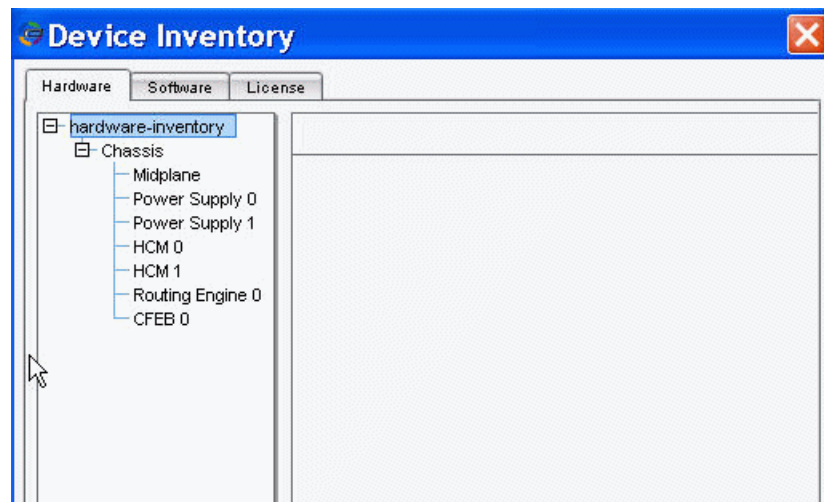
To view the device inventory, the device must be in the Managed state.

Action To view the device inventory, follow these steps:

1. In the navigation tree, select **Device Manager > Devices**.
2. Right-click the device whose inventory you want to view.
3. Select **View/Reconcile Inventory**.

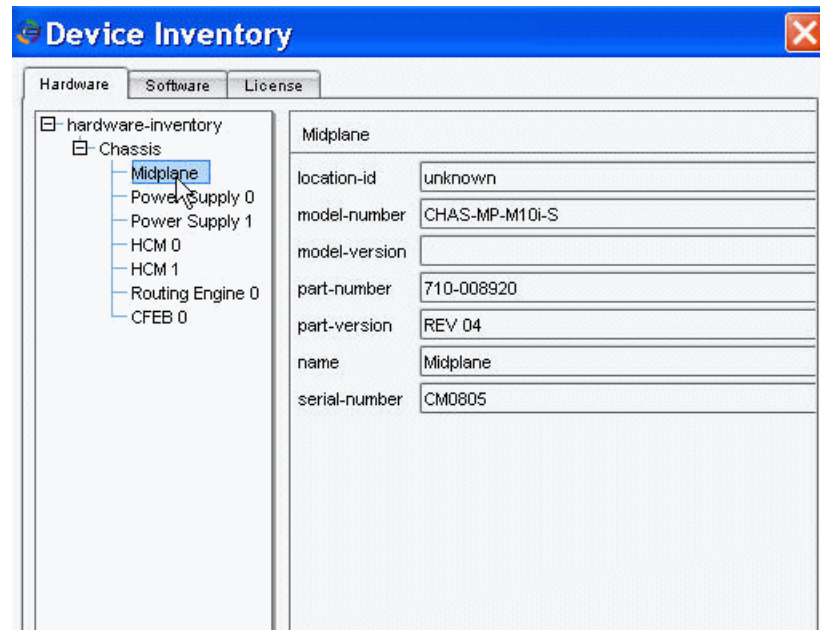
The Device Inventory window opens, similar to the example shown in [Figure 7 on page 568](#).

Figure 7: The Device Inventory Window



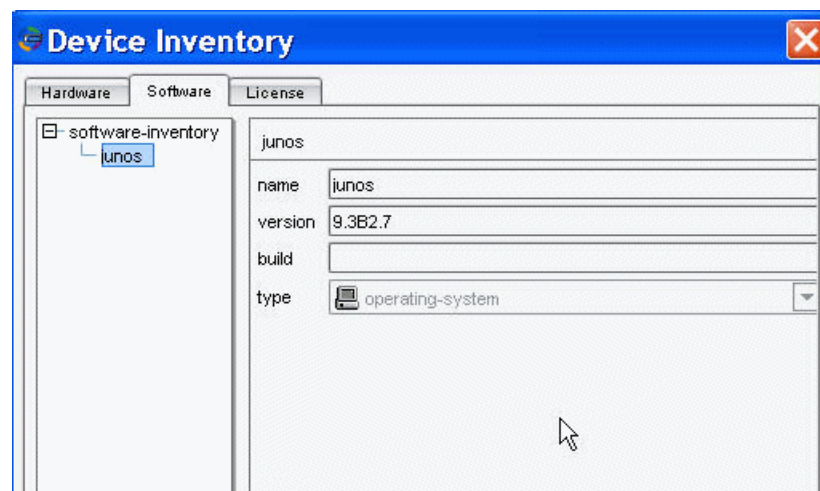
4. Select the **Hardware** tab to display information about hardware modules in the device, including the I/O module, the Routing Engine, and so on. (See [Figure 8 on page 569](#).)

Figure 8: Viewing the Hardware Inventory



5. Select the **Software** tab to display information about the software packages installed in the device, including the installed OS and its version, and any other installed packages. (See [Figure 9 on page 569](#).)

Figure 9: Viewing the Software Inventory



NOTE: The License tab not supported for M Series or MX Series devices.

Viewing Device Inventory from the CLI

Purpose The information displayed in the Device Inventory window, as shown in [“Viewing Device Inventory in NSM” on page 568](#) can also be viewed from the device (router) using the CLI operational mode. Generally, the hardware and software information displayed in the Device Inventory window and the CLI command output is similar.

Action To view device hardware and software inventory, from the device enter the following Junos OS CLI operational mode commands:

```
show chassis hardware
show version
```

Sample Output

The following sample output shows hardware and software inventory for the same router used in [“Viewing Device Inventory in NSM” on page 568](#).

```
user@host> show chassis hardware
Hardware inventory:
Item              Version  Part number  Serial number  Description
Chassis                               39097          M10i
Midplane    REV 04  710-008920  CM0805      M10i Midplane
Power Supply 0    Rev 06    740-008537    5384103        AC Power Supply
Power Supply 1    Rev 06    740-008537    5384265        AC Power Supply
HCM 0             REV 03    710-010580    CM1272         M10i HCM
HCM 1             REV 03    710-010580    CM1187         M10i HCM
Routing Engine 0  REV 09    740-009459    1000602468     RE-5.0
CFEB 0           REV 09    750-010465    DK6820         Internet Processor II
FPC 0
PIC 0             REV 10    750-002971    CL0219         4x OC-3 SONET, MM
PIC 1             REV 11    750-002992    CM4540         4x F/E, 100 BASE-TX
PIC 2             REV 08    750-005724    CL9082         2x OC-3 ATM-II IQ, MM
PIC 3             REV 08    750-005724    CL9078         2x OC-3 ATM-II IQ, MM
FPC 1
PIC 2             REV 12    750-008425    CG1204         Adaptive Services
PIC 3             REV 12    750-012838    DJ0049         4x 1GE(LAN), IQ2
Xcvr 0           REV 01    740-013111    7303532        SFP-T
Xcvr 1           REV 01    740-013111    7314215        SFP-T
Xcvr 2           REV 01    740-013111    7303398        SFP-T
Xcvr 3           REV 01    740-013111    7303376        SFP-T
Fan Tray 1
Rear Right Fan Tray

user@host> show version
Hostname: host
Model: m10i
Junos OS Base OS boot [9.3B2.7]
Junos OS Base OS Software Suite [9.3B2.7]
Junos OS Kernel Software Suite [9.3B2.7]
Junos OS Crypto Software Suite [9.3B2.7]
Junos OS Packet Forwarding Engine Support (M/T Common) [9.3B2.7]
Junos OS Packet Forwarding Engine Support (M7i/M10i) [9.3B2.7]
Junos OS Online Documentation [9.3B2.7]
Junos OS Routing Software Suite [9.3B2.7]
```

Meaning The sample output for the **show chassis hardware** command shows the hardware installed on the M10i device. The row of output showing the midplane is in bold to illustrate that

the midplane information in this example is identical to the midplane information in the NSM UI example.

The sample output for the **show version** command shows the version of Junos OS installed on the M10i device. In this instance, the CLI output provides more information than is provided by the NSM UI.

**Related
Documentation**

- [Managing M Series and MX Series Device Software Versions on page 565](#)
- [Viewing and Reconciling Device Inventory on page 567](#)

CHAPTER 28

Topology Manager

- [Overview of the NSM Topology Manager on page 573](#)
- [Requisites for a Topology Discovery on page 573](#)
- [About the NSM Topology Manager Toolbar on page 574](#)

Overview of the NSM Topology Manager

The Network and Security Manager (NSM) Topology Manager is a tool provided in the NSM user interface (UI) to discover and manage the physical topology of a network of devices connected to a Juniper Networks EX-series switch. These include networking devices such as the J-series, M Series, MX Series, and EX-series, as well as ScreenOS and IDP devices, IP phones, desktops, printers, and servers. The Topology Manager also provides details about connections between a device and the EX-series switch.

For more information about the Topology Manager, see the *Network and Security Manager Administration Guide*.

Related Documentation

- [Requisites for a Topology Discovery on page 573](#)
- [About the NSM Topology Manager Toolbar on page 574](#)

Requisites for a Topology Discovery

To use the Topology Manager, first add one or more EX-series switches to the Device Manager in NSM. You can then use an added device as a *seed* device in initiating a topology discovery.

Alternatively, if there are no devices added or managed in NSM, you can initiate a topology discovery by configuring preferred subnets. All the IP addresses in the included subnets range are discovered. Therefore, you need to have seed devices or preferred subnets, or both to initiate topology discovery. You also need:

1. The management IP address of the EX-series switch that acts as the seed IP address
2. SNMP credentials:
 - For SNMPv1 and SNMPv2c: Community string

- For SNMPv3: Username, security level, authentication type, privacy type, privacy password, and authentication password
3. Enabled Layer 2 protocols like LLDP, STP, RSTP in the switched network, because network discovery depends on these as well as on the Address Forwarding Table information.

For more information about the Topology Manager, see the *Network and Security Manager Administration Guide*.

**Related
Documentation**

- [Overview of the NSM Topology Manager on page 573](#)
- [About the NSM Topology Manager Toolbar on page 574](#)

About the NSM Topology Manager Toolbar

You can use the Topology Manager toolbar to perform the following actions:

- **Zoom in and Zoom out:** Use these tools to view the network topology according to the detail required. These tools are only of use in the map view.
- **Save to file:** Use this tool to save the network topology map as an image file and the devices and links tables as text files from their respective views.
- **Print:** From different views, you can use this tool to print a network topology map as an image file and the devices and links tables as text files.
- **Manage Devices:** Use this tool to select one or more devices from a topology map and manage them in NSM. This tool is applicable only to map views and not the different table views. To add a device:
 - a. Click the **Manage Devices** icon. A dialog box opens.
 - b. Enter the SSH user name and password.
 - c. Click **OK**.
- **Set Preferences:** Use this tool to set preferences according to which the discovery engine can perform a topology discovery. You can set preferences for default SNMP credentials, topology discovery intervals, and subnets to be included or excluded.
- **Start and Stop Topology Discovery:** Use these tools to initiate and stop a topology discovery based on the set of seed devices and credentials specified in the topology preferences.
- **Search:** You can search for a device, end-point device, link, or port in any of the table views by providing a string in the search text box. NSM performs a substring match against all attributes of the particular view and displays the results in the same table. If you navigate to another tab, your search results are lost. You can save the search output in a text file as comma-separated values.

The Topology Manager status bar at the bottom of the screen indicates the timestamp of the last completed topology discovery and whether a discovery is in progress.

For more information about the Topology Manager, see the *Network and Security Manager Administration Guide*.

- Related Documentation**
- [Overview of the NSM Topology Manager on page 573](#)
 - [Requisites for a Topology Discovery on page 573](#)

PART 5

Monitor

- [Real Time Monitor on page 579](#)

CHAPTER 29

Real Time Monitor

- [About the Realtime Monitor on page 579](#)
- [Viewing Device Status on page 579](#)
- [Viewing Device Monitor Alarm Status on page 582](#)
- [Setting the Polling Interval For Device Alarm Status on page 583](#)

About the Realtime Monitor

The Realtime Monitor module in Network and Security Manager (NSM) enables you to monitor real-time status and statistics about all the managed devices in your network at a glance. Features of Realtime Monitor enabled for M Series and MX Series include viewing device status, viewing monitor alarm status, and setting the polling interval for device alarm status. You can use the Realtime Monitor to identify problems and discover trends across multiple geographic regions and functional areas from a central management location.

The Realtime Monitor can also help you quickly identify potential device, network, and system-level problems, such as:

- Configuration status—At the device level, you can monitor the changing status of one or more security devices in real time.
- Connection status—At the network level, you can monitor problems that could lead to failed devices.

The Realtime Monitor does the work of a management expert by first gathering information about specific processes and network activity, then color-coding each event to organize problems.

Related Documentation

- [Viewing Device Status on page 579](#)
- [Viewing Device Monitor Alarm Status on page 582](#)
- [Setting the Polling Interval For Device Alarm Status on page 583](#)

Viewing Device Status

[Table 343 on page 580](#) lists and describes device information that you can view through the Device Monitor.

Table 343: Device Status Information

Column	Description
Name	Unique name assigned to the device in NSM.
Domain	Domain in NSM in which the device is managed.
Platform	Model number of the device.
OS Version	Operating system firmware version running on the device.
Config Status	<p>Current configuration status of the device in NSM:</p> <ul style="list-style-type: none"> • None—No state has been set (does not show in Device Monitor). • Modeled—The device exists in NSM, but a connection to the device has not yet been established. • RMA—Equivalent to bringing the device into the Modeled state. RMA results from an administrator selection in the UI when a device goes down. • Waiting for 1st connect—NSM is waiting for the device to connect. You must enter a command on the device to make it connect to NSM. • Import Needed—You must import the configuration of the device into NSM. When you add a device for the first time, verify that your status indicates "Import Needed" before you attempt to import the device. During migration, this state indicates that import of the security device configuration is still required. • OS Version Adjustment Needed—The firmware version detected running on the device is different than what was previously detected in NSM. This could happen in the event that the automatic adjustment option was cleared during a change device firmware directive or an Update Device directive was issued to an IDP device with a firmware version mismatch. • Platform Mismatch—The device platform selected when adding the DMI device in NSM does not match the device itself. A device in this state cannot connect to NSM. • Device Firmware Mismatch—The OS version selected when adding a DMI device does not match the OS version running on the device itself. • Device Type Mismatch—The type of device specified when adding the device in NSM does not match the device itself. The device type might indicate whether the device is part of a vsys device, part of a cluster, or part of a virtual chassis. A device in this state cannot connect to NSM. • Detected duplicate serial number—The device has the same sequence number as another managed device. A device in this state cannot connect to NSM. • Update Needed—An update to this device is required. • Managed—The device is currently being managed by NSM. • Managed, In Sync—The physical device configuration is synced with the modeled configuration in NSM.

Table 343: Device Status Information (*continued*)

Column	Description
Config Status (continued)	<ul style="list-style-type: none"> Managed, Device Changed—The physical device configuration is out of sync with the modeled configuration in NSM. Changes were made to the physical device configuration (the configuration on the physical device is newer than the modeled configuration). For M Series and MX Series devices with redundant Routing Engines, this status can indicate that a routing engine switchover has occurred. Managed, NSM Changed—The modeled device configuration is out of sync with the physical device configuration. Changes were made to the modeled configuration (the configuration on the NSM is newer than the physical device configuration). Managed, NSM and Device Changed—Both device configurations (physical and modeled) are out of sync with each other. Changes were made to the physical device configuration and to the modeled configuration. Managed, Sync Pending—Completion of the Update Device directive is suspended and waiting for the device to reconnect. This state occurs only for ScreenOS devices that have the Update When Device Connects option selected during the device update.
Connection Status	<p>Connection status of the device in NSM:</p> <ul style="list-style-type: none"> Up—Device is currently connected to NSM. Down—Device is not currently connected to NSM but has connected in the past. Never Connected—Device has never connected to NSM. <p>The Device Server checks the connection status of each device every 120 seconds by default. You can change this behavior by editing the value for the <code>devDaemon.deviceHeartbeatTimeout</code> parameter in the Device Server configuration file. Refer to the <i>Network and Security Manager Installation Guide</i> for more information about editing configuration files.</p> <p>NOTE: If the network connection goes down for a period longer than six to eight minutes, the device connection will permanently time out. If this occurs and the device goes down for any reason, the device still appears as Up in the Device Monitor.</p>
Alarm	<p>Displays the current alarm status for each device in NSM:</p> <ul style="list-style-type: none"> If device has any alarms, the most severe alarm severity is displayed (either Major or Minor). None—The device has no alarms. Unknown—The device status is unknown. For example, the device might not be connected. N/A—The device's alarm is not pollable or discoverable, for example, this column shows "N/A" for ScreenOS and IDP devices. Alarm is colored: <ul style="list-style-type: none"> Red for Major. Orange for Minor. Green for Ignore, None, Unknown, or N/A.

Table 343: Device Status Information (*continued*)

Column	Description
H/W Inventory Status	<p>Displays the inventory status for hardware on the device:</p> <ul style="list-style-type: none"> • In Sync—The inventory information in the NSM database is synchronized with the information about the device. • Out Of Sync—The inventory information in the NSM database is not synchronized with the information about the device. • N/A—The connected device is a ScreenOS or IDP device, or the device is not connected and imported.
S/W Inventory Status	<p>Displays the inventory status for software on the device:</p> <ul style="list-style-type: none"> • In Sync—The inventory information in the NSM database is synchronized with the software on the device. • Out Of Sync—The inventory information in the NSM database is not synchronized with the software on the device. • N/A—The connected device is a ScreenOS or IDP device, or the device is not connected and imported.
License Inventory Status	<p>Displays the inventory status for software on the device:</p> <ul style="list-style-type: none"> • In Sync—The inventory information in the NSM database is synchronized with the licenses on the device. • Out Of Sync—The inventory information in the NSM database is not synchronized with the licenses on the device. • N/A—The connected device is a ScreenOS or IDP device, or the device is not connected and imported.
First Connect	The first time the security device connected to the NSM Device Server.
Latest Connect	The last time the security device connected to the NSM Device Server.
Latest Disconnect	The last time the security device disconnected from the NSM Device Server.

- Related Documentation**
- [About the Realtime Monitor on page 579](#)
 - [Viewing Device Monitor Alarm Status on page 582](#)
 - [Setting the Polling Interval For Device Alarm Status on page 583](#)

Viewing Device Monitor Alarm Status

Purpose Alarms refresh automatically through periodic polling.

Action To view the Alarm status and time:

1. From **Device Monitor**, right-click the device row entry and select the **View Alarm** option.

The device **Alarm Status** dialog box displays the alarm list and polling time for the device.

2. To retrieve the current alarm status in the device, click the **Refresh** button.

The poll time is derived from the device server time.

**Related
Documentation**

- [About the Realtime Monitor on page 579](#)
- [Viewing Device Status on page 579](#)
- [Setting the Polling Interval For Device Alarm Status on page 583](#)

Setting the Polling Interval For Device Alarm Status

The default polling interval is 900 seconds (15 minutes). To configure polling intervals for Alarm Status:

1. From **Device Manager**>**Devices**, double-click the device to open it.

The Info tab dialog box is displayed.

2. Select the **Device Admin** page to set the polling interval for the device.

The minimum polling interval is 60 seconds. The maximum interval is 2,147,483,647 seconds. You cannot disable polling.

**Related
Documentation**

- [About the Realtime Monitor on page 579](#)
- [Viewing Device Status on page 579](#)
- [Viewing Device Monitor Alarm Status on page 582](#)

PART 6

Index

- [Index on page 587](#)

Index

Symbols

#, comments in configuration statements.....	xxix
(), in syntax descriptions.....	xxix
< >, in syntax descriptions.....	xxviii
[], in configuration statements.....	xxix
{ }, in configuration statements.....	xxix
(pipe), in syntax descriptions.....	xxix

A

access address pools, configuring.....	52
access profile, configuring.....	73
access profiles, L2TP	
AAA subscriber management	
RADIUS parameters, configuring.....	65
access profile, configuring.....	57
accounting order, configuring.....	58
accounting parameters, configuring.....	57
authentication order, configuring.....	59
authorization order, configuring.....	59
client filter name, configuring.....	61
configuring.....	56
L2TP client, configuring.....	60
LDAP options, configuring.....	62
LDAP server, configuring.....	63
provisioning order, configuring.....	64
RADIUS parameters, configuring.....	68, 70
session limit, configuring.....	69
subscriber access management	
RADIUS, configuring.....	69
accounting options	
class usage profile, configuring.....	75
filter profile, configuring.....	77
interface profile, configuring.....	78
log file, configuring.....	76
MIB profile, configuring.....	80
policy decision statistics profile,	
configuring.....	79
routing engine profile, configuring.....	81
accounting options, configuring.....	75
adaptive services PICs, configuring.....	427
address assignment pools, configuring.....	49

address family, specifying.....	191
aggregated devices, configuring.....	91
alarm status	
setting polling intervals.....	583
viewing.....	582
API.....	12
application, application set	
configuring.....	83

B

BGP	
configuring.....	254
border signaling gateways, configuring.....	428
braces, in configuration statements.....	xxix
brackets	
angle, in syntax descriptions.....	xxviii
square, in configuration statements.....	xxix
bridge domain	
logical interfaces, configuring.....	85
multicast monitoring options, configuring.....	86
VLAN ID, configuring.....	89
bridge domains properties	
configuring.....	85

C

chassis alarms, configuring.....	92
chassis FPC, configuring.....	94
classifiers	
CoS.....	118
CLI	
about.....	7
code point aliases.....	120
comments, in configuration statements.....	xxix
communities	
configuring.....	524
confederation	
configuring.....	366
configuring, access group profile.....	53
container interfaces, configuring.....	93
conventions	
text and syntax.....	xxviii
CoS classifiers.....	118
CoS code point aliases.....	120
CoS drop profiles.....	121
CoS forwarding classes.....	123
CoS forwarding policy, configuring.....	125
CoS fragmentation maps, configuring.....	126
CoS host outbound traffic, configuring.....	127
CoS interfaces.....	128

CoS restricted queue, configuring.....	141	drop profiles.....	121
CoS rewrite rules.....	134	dynamic tunnels, configuring.....	367
CoS routing instances, configuring.....	137		
CoS scheduler maps.....	140	E	
CoS schedulers.....	138	edit routing-options command.....	18
CoS tracing operations, configuring.....	142	event policy tracing, configuring.....	155
CoS traffic control profiles, configuring.....	143	event policy, configuring.....	152
CoS translation table, configuring.....	144	event script, configuring.....	150
curly braces, in configuration statements.....	xxix		
customer support.....	xxix	F	
contacting JTAC.....	xxix	fate sharing	
D		configuring.....	368
data model, defined.....	11	firewall filter	
device		any family type, configuring.....	157
status.....	16	bridge family type, configuring.....	159
device configuration		Ccc family type, configuring.....	161
about.....	43	inet family type, configuring.....	163
modeling.....	28	inet6 family type, configuring.....	168
device groups		mpls family type, configuring.....	172
planning for.....	29	policer.....	178
using.....	29	VPLS family type, configuring.....	175
device inventory		flow	
reconciling.....	567	configuring.....	370
viewing.....	567	font conventions.....	xxviii
Device Monitor		forwarding	
alarm status.....	582	accounting options, configuring.....	181
device status information.....	579	forwarding classes.....	123
device schemas		forwarding table	
about.....	12	configuring.....	372
devices		G	
adding multiple with discovery rules.....	29	gateway	
importing with dynamic IP address.....	16	admission controller, configuring.....	429
managed.....	25	message manipulation rules, configuring.....	434
modeling.....	28	new call usage policy set, configuring.....	438
DHCP agent		new call usage policy, configuring.....	435
authentication support, configuring.....	183	new transaction policy set, configuring.....	441
default configuration settings, overriding.....	185	new transaction policy, configuring.....	439
group, configuring.....	184	service point, configuring.....	432
name of a group, configuring.....	189	session policy decision function,	
operations, configuring.....	190	configuring.....	430
relay option 60, configuring.....	187	SIP policies and timers, configuring.....	433
relay option 82, configuring.....	188	timers, configuring.....	442
DHCP agent, configuring.....	183	traceoptions, configuring.....	443
discovery rules.....	29	gateway properties, configuring.....	428
distributed data collection.....	13	gateway, configuring.....	429
DMI See distributed data collection		generated routes	
documentation		configuring.....	373
comments on.....	xxix	group specific properties RIPvng, configuring.....	342

group, device.....29

H

H248 options

encoding defaults, changing.....466
service change, configuring.....466

H248 options, configuring.....465

H248 properties

application data inactivity detection,
configuring.....472
base root, configuring.....472
differentiated services, configuring.....475
event timestamp notification,
configuring.....475
hanging termination detection,
configuring.....476
inactivity timer, configuring.....477
notification behavior, configuring.....478
segmentation, configuring.....479
traffic management, configuring.....480

helpers

DNS packet forwarding, enabling.....197
port, configuring.....199
router/interface, configuring.....194
tracing operations, configuring.....201

helpers, configuring.....193

I

ILMI protocol, configuring.....257

inet family type

firewall filter, configuring.....163
prefix-specific actions, configuring.....165
service filters, configuring.....166
simple filters, configuring.....167

inet6 family type

firewall filter, configuring.....169
service filters, configuring.....171

instance export

configuring.....374

instance import

configuring.....375

interface routes

configuring.....376

interface set, configuring.....235

interface trace options, configuring.....236

interfaces

logical interface properties, configuring.....212
properties, configuring.....207
receive bucket properties, configuring.....210

tracing operations, configuring.....210

traffic shaping profile, configuring.....233

transitions, damping.....209

transmit leaky bucket, configuring.....211

Interfaces

MPLS, configuring.....288

interfaces, configuring.....207

intrusion detection service, configuring.....450

inventory *See* device inventory

IP addresses

configuring.....17

J

Job Manager

about.....33
displaying updating errors37
reviewing.....35

Junos OS devices

adding multiple with discovery rules.....29
configuring.....44

Junos OS, upgrading.....565

L

label distribution protocol, configuring.....267

label switched path

administrative group, configuring.....293
automatic bandwidth, configuring.....294
BFD, configuring.....299
fast reroute, configuring.....296
LSP related routes, adding.....297
MPLS LSPs, configuring.....298

label switched path, configuring.....290

layer 2 address learning, configuring.....258

layer 2 circuit

local interface switching, configuring.....259
neighbor interface, configuring.....260
tracing.....264

layer 2 circuit, configuring.....259

LDAP options, configuring.....54

LDAP server, configuring.....55

link management protocol, configuring.....278

load balancing

per-flow/per-prefix, configuring.....202

load balancing, configuring.....192

logical interface

demux source family type, configuring.....214
epd threshold, configuring.....214
IP demux, configuring.....213
unit properties, configuring.....212

logical interfaces	
Ccc family information, configuring.....	216
inet family information, configuring.....	217
inet6 family information, configuring.....	223
ISO family information, configuring.....	230
MPLS family information, configuring.....	231
protocol family information, configuring.....	215
TCC family information, configuring.....	233
LSP	
administrative group, configuring.....	304
BFD, configuring.....	306, 312, 317
class-type bandwidth, configuring.....	305
egress router, configuring.....	314
packets, tracing.....	315
primary paths, configuring.....	303
secondary paths, configuring.....	308
system log messages, configuring.....	316
M	
M Series devices	
adding multiple with discovery rules.....	29
configuring.....	44
managed devices.....	25
manuals	
comments on.....	xxix
martian addresses	
configuring.....	377
maximum paths	
configuring.....	378
maximum prefixes	
configuring.....	379
MPLS	
administrative group, configuring.....	285
administrative groups, configuring.....	285
bandwidth, configuring.....	286
DiffServ-aware, configuring.....	287
packets, tracing.....	323
MPLS statistics, configuring.....	322
MPLS, enabling.....	282
MSDP	
active source limit, configuring.....	325
export policy, configuring.....	326
MSDP peers, configuring.....	328
per-source active source limit, configuring.....	331
routing table group, configuring.....	330
traceoptions, configuring.....	332
MSDP peer group, configuring.....	327
MSDP, configuring.....	324
MSTP.....	332
MTU signaling, configuring.....	320
multicast	
configuring.....	381
multiclass LSP	
class-type bandwidth constraints,	
configuring.....	311
MX Series devices	
adding multiple with discovery rules.....	29
configuring.....	44
N	
named paths, configuring.....	319
navigation tree.....	7
NetConf.....	13
network	
connectivity, checking	18
ping command.....	18
network address translation, configuring.....	455
no-readvertise	
option.....	19
NSM API.....	12
NSM architecture	
distributed data collection.....	7
NSM modules	
Log Viewer.....	32
Realtime Monitor.....	32, 579
NSM UI	
about.....	7
navigation tree.....	7
O	
option	
no-readvertise.....	19
retain.....	19
Options	
configuring.....	384
OSPF.....	334
P	
parentheses, in syntax descriptions.....	xxix
PGCP	
gateway, configuring.....	461
H248 options, configuring.....	465
H248 properties, configuring.....	471
H248 timers, configuring.....	482
media service, configuring.....	485
monitor, configuring.....	483
overload control, configuring.....	484
rule set, configuring.....	487

- rule, configuring.....486
- session mirroring, configuring.....485, 487
- traceoptions, configuring.....488
- virtual interface, configuring.....489
- PGCP, configuring.....460
- PGCP, gateway
 - context indications, configuring.....467
 - control association indications,,
 - configuring.....467
 - data inactivity detection, configuring.....462
 - gateway controller, configuring.....463
 - graceful restart, configuring.....464
 - virtual BGF, configuring.....461
 - virtual interface indications, configuring.....470
- PIC operations, tracing.....454
- ping command
 - network
 - connectivity, checking.....18
- policer
 - configuring.....178
- policers, configuring.....302
- port mirroring
 - configuring.....203
- primary point-to-multipoint, configuring.....301
- protocol
 - ILMI.....257
 - label distribution.....267
 - link management.....278
 - RSVP.....358
- protocol tunneling/BPDU protection,
 - configuring.....265
- protocols
 - BGP.....254
 - OSPF.....334
 - RIP.....338
 - VRRP.....355
 - VSTP.....356
- Protocols
 - MSTP.....332
- R**
- RADIUS, configuring.....71
- Realtime Monitor
 - using.....579
- reroute path
 - automatic bandwidth, configuring.....295
- retain
 - option.....19
- rewrite rules.....134
- rib
 - configuring.....385
- rib groups
 - configuring.....387
- RIP.....338
- RIPng
 - neighbor properties, configuring.....345
 - traceoptions, configuring.....349
- RIPng protocol
 - graceful restart, configuring.....341
 - router, configuring.....340
- RIPng protocol, configuring.....340
- RIPng send update messages, configuring.....348
- RIPng update messages, configuring.....347
- RIPng, routes export
 - policies, applying.....344
- RIPng, routes import
 - policies, applying.....344, 346
- role-based administration
 - about.....4
- route
 - static.....18
- router advertisement, configuring.....350
- router discovery, configuring.....352
- routers
 - check network connectivity.....18
- routing engine
 - reboot or halt, configuring.....105
- routing engine redundancy, configuring.....104
- routing options
 - confederation.....366
 - fate sharing.....368
 - flow.....370
 - forwarding table.....372
 - generated routes.....373
 - instance export.....374
 - instance import.....375
 - interface routes.....376
 - martian addresses.....377
 - maximum paths.....378
 - maximum prefixes.....379
 - multicast.....381
 - Options.....384
 - rib.....385
 - rib groups.....387
 - source routing.....388
 - Static Routes.....389
 - Traceoptions.....390
- RSVP, configuring.....358

S

scheduler maps.....	140
schedulers.....	138
schema See device schema	
secondary paths	
administrative group, configuring.....	310
SecurID server, configuring.....	72
service set, configuring.....	493
services	
class of service, configuring.....	447
show route command.....	18
SNMP	
communities.....	524
trap groups.....	526
views.....	528
source routing	
configuring.....	388
stateful firewall, configuring.....	491
static LSP, configuring.....	321
static route.....	18
Static Routes	
configuring.....	389
status	
device.....	16
support, technical See technical support	
syntax conventions.....	xxviii

T

T640 router, configuring.....	99
TCP See Transmission Control Protocol	
technical overview.....	3
technical support	
contacting JTAC.....	xxix
topologies, configuring.....	391, 393
Traceoptions	
configuring.....	390
Transmission Control Protocol.....	13
trap groups	
configuring.....	526

U

unreachable workflow	
importing device.....	16

V

views	
configuring.....	528
VRRP.....	355
VSTP.....	356

W

workflows	
supported.....	26