



Network and Security Manager

Configuring J Series Services Routers and SRX Series Services Gateways Guide

Release
2012.2



Published: 2013-01-06
Revision 01

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

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

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.

Network and Security Manager Configuring J Series Services Routers and SRX Series Services Gateways Guide
2012.2

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

Revision History
January 2013 —01

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

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 this Guide	xv
	Objectives	xv
	Audience	xvi
	Conventions	xvi
	List of Technical Publications	xvii
	Requesting Technical Support	xviii
	Self-Help Online Tools and Resources	xix
	Opening a Case with JTAC	xix
Part 1	Getting Started	
Chapter 1	Understanding J Series Services Router and SRX Series Services Gateway Configuration	3
	NSM and Device Management Overview	3
	Communication Between NSM and a Device Overview	3
	Device Configurations Supported in NSM for the J Series Services Router and SRX Series Services Gateway	5
Chapter 2	J Series Services Routers and SRX Series Services Gateways and NSM Installation and Integration Overview	7
	J Series Services Router and SRX Series Services Gateway Installation and Configuration Overview	7
	NSM Installation Overview	8
	Adding J Series Services Routers or SRX Series Services Gateways in NSM Overview	8
	Adding J Series Services Router Clusters and SRX Series Services Gateway Clusters Overview	8
	Adding J Series Services Router Clusters and SRX Series Services Gateway Virtual Chassis Clusters Overview	9
	Using Templates and Configuration Groups in NSM Overview	10

Part 2	Configuring J Series Services Routers and SRX Series Services Gateways	
Chapter 3	Configuring Access in J Series Services Routers and SRX Series Services Gateways	13
	Configuring Address Assignment (NSM Procedure)	13
	Configuring Neighbor Discovery Router Advertisement	14
	Configuring Pool	14
	Configuring an Address Pool (NSM Procedure)	18
	Configuring a Group Profile (NSM Procedure)	19
	Configuring LDAP Options (NSM Procedure)	20
	Configuring Assemble	21
	Configuring the LDAP Server (NSM Procedure)	22
	Configuring a SecurID Server (NSM Procedure)	23
	Configuring RADIUS Options (NSM Procedure)	24
	Configuring a RADIUS Server (NSM Procedure)	24
	Configuring Firewall Authentication (NSM Procedure)	26
	Configuring Pass-Through	26
	Configuring Traceoptions	27
	Configuring Web Authentication	28
Chapter 4	Configuring Access Profile in J Series Services Routers and SRX Series Services Gateways	31
	Configuring the Access Profile (NSM Procedure)	31
Chapter 5	Configuring Accounting Options in J Series Services Routers and SRX Series Services Gateways	33
	Configuring Accounting Options (NSM Procedure)	33
	Configuring Class Usage Profiles (NSM Procedure)	33
	Configuring a Log File (NSM Procedure)	34
	Configuring the Filter Profile (NSM Procedure)	35
	Configuring the Interface Profile (NSM Procedure)	36
	Configuring the Policy Decision Statistics Profile (NSM Procedure)	37
	Configuring the MIB Profile (NSM Procedure)	38
	Configuring the Routing Engine Profile (NSM Procedure)	39
Chapter 6	Configuring Applications in J Series Services Routers and SRX Series Services Gateways	41
	Configuring the Application and Application Set (NSM Procedure)	41
Chapter 7	Configuring User Authentication in J Series Services Routers and SRX Series Services Gateways	43
	Configuring RADIUS Authentication (NSM Procedure)	43
	Configuring TACACS+ Authentication (NSM Procedure)	44
	Configuring Authentication Order (NSM Procedure)	45
	Configuring User Access (NSM Procedure)	46
	Configuring Login Classes	46
	Configuring User Accounts	48
	Configuring Template Accounts (NSM Procedure)	49
	Creating a Remote Template Account	50
	Creating a Local Template Account	51

Chapter 8	Configuring Chassis in J Series Services Routers and SRX Series Services Gateways	53
	Configuring Aggregated Devices (NSM Procedure)	53
	Configuring Chassis Alarms (NSM Procedure)	54
	Configuring Chassis FPC (NSM Procedure)	55
	Configuring a T640 Router on a Routing Matrix (NSM Procedure)	60
	Configuring Routing Engine Redundancy (NSM Procedure)	65
	Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors (NSM Procedure)	66
Chapter 9	Configuring USB Modem Interfaces in J Series Services Routers and SRX Series Services Gateways	67
	Configuring a USB Modem Interface (NSM Procedure)	67
	Configuring a Dialer Interface (NSM Procedure)	68
	Configuring Dial-in Options on a Dialer Interface (NSM Procedure)	69
	Configuring a CHAP Access Profile on a Dialer Interface (NSM Procedure)	70
Chapter 10	Configuring Policy Options in J Series Services Routers and SRX Series Services Gateways	73
	Configuring an AS Path Group in a BGP Routing Policy (NSM Procedure)	73
	Configuring a Community for use in BGP Routing Policy Conditions (NSM Procedure)	74
	Configuring a BGP Export Policy Condition (NSM Procedure)	75
	Configuring Flap Damping to Reduce the Number of BGP Update Messages (NSM Procedure)	76
	Configuring a Routing Policy Statement (NSM Procedure)	78
	Configuring Prefix List (NSM Procedure)	79
Chapter 11	Configuring Routing Options in J Series Services Routers and SRX Series Services Gateways	81
	Configuring Maximum Prefixes (NSM Procedure)	81
	Configuring Multicast (NSM Procedure)	83
	Configuring Multipath (NSM Procedure)	86
	Configuring Options (NSM Procedure)	87
	Configuring Route Resolution (NSM Procedure)	88
	Configuring Routing Table Groups (NSM Procedure)	89
	Configuring Routing Tables (NSM Procedure)	91
	Configuring Source Routing (NSM Procedure)	93
	Configuring Static Routes (NSM Procedure)	94
	Configuring Generated Routes (NSM Procedure)	95
	Configuring Graceful Restart (NSM Procedure)	96
	Configuring Forwarding Table (NSM Procedure)	97
	Configuring Flow Route (NSM Procedure)	99
	Configuring Fate Sharing (NSM Procedure)	101
	Configuring Martian Addresses (NSM Procedure)	102
	Configuring Interface Routes (NSM Procedure)	104
	Configuring Instance Export (NSM Procedure)	105
	Configuring Instance Import (NSM Procedure)	105

Chapter 12

Configuring Protocols for J Series Services Routers and SRX Series Services Gateways	107
Configuring BGP (NSM Procedure)	107
Configuring 802.1X Authentication (NSM Procedure)	110
Configuring 802.1X Interface Settings	111
Configuring Static MAC Bypass	112
Configuring GVRP (NSM Procedure)	112
Configuring IGMP (NSM Procedure)	113
Configuring MPLS (NSM Procedure)	115
Configuring MPLS (NSM Procedure)	116
Configuring Auto Policing (NSM Procedure)	118
Configuring Bandwidth (NSM Procedure)	119
Configuring Differentiated Services Traffic Engineering (NSM Procedure)	119
Configuring Interfaces (NSM Procedure)	120
Configuring Label Switched Path (NSM Procedure)	122
Configuring an Admin Group (NSM Procedure)	124
Configuring Auto Bandwidth (NSM Procedure)	125
Configuring Fast Reroute (NSM Procedure)	126
Configuring Install (NSM Procedure)	127
Configuring P2MP (NSM Procedure)	128
Configuring Policing (NSM Procedure)	128
Configuring Primary (NSM Procedure)	129
Configuring Priority (NSM Procedure)	131
Configuring Secondary (NSM Procedure)	131
Configuring Traceoptions (NSM Procedure)	132
Configuring Log Updown (NSM Procedure)	133
Configuring OAM (NSM Procedure)	134
Configuring Path (NSM Procedure)	137
Configuring Path MTU (NSM Procedure)	138
Configuring Static Label Switched Path (NSM Procedure)	139
Configuring Statistics (NSM Procedure)	142
Configuring Traceoptions (NSM Procedure)	143
Configuring MSDP (NSM Procedure)	144
Configuring Active Source Limit (NSM Procedure)	145
Configuring Export (NSM Procedure)	145
Configuring Group (NSM Procedure)	146
Configuring Import (NSM Procedure)	150
Configuring Peer (NSM Procedure)	150
Configuring RIB Group (NSM Procedure)	152
Configuring Source (NSM Procedure)	153
Configuring Traceoptions (NSM Procedure)	153
Configuring MSTP (NSM Procedure)	154
Configuring OSPF (NSM Procedure)	156
Configuring RIP (NSM Procedure)	160
Configuring RIPng (NSM Procedure)	162
Configuring Graceful Restart (NSM Procedure)	163
Configuring Groups (NSM Procedure)	164
Configuring Import (NSM Procedure)	166

Chapter 13

Configuring Receive (NSM Procedure)	166
Configuring Send (NSM Procedure)	167
Configuring Traceoptions (NSM Procedure)	167
Configuring Router Advertisement (NSM Procedure)	168
Configuring Router Discovery (NSM Procedure)	171
Configuring VSTP (NSM Procedure)	173
Configuring VRRP (NSM Procedure)	175
Configuring Security for J Series Services Routers and SRX Series Services Gateways	177
Configuring Certificates (NSM Procedure)	177
Configuring Certification Authority (NSM Procedure)	178
Configuring the Local Certificate (NSM Procedure)	179
Configuring Firewall Authentication (NSM Procedure)	180
Configuring a Flow (NSM Procedure)	181
Configuring a Bridge (NSM Procedure)	181
Configuring the TCP MSS Option (NSM Procedure)	182
Configuring the TCP Session Option (NSM Procedure)	183
Configuring Traceoptions (NSM Procedure)	184
Configuring File Options (NSM Procedure)	185
Configuring Flag Options (NSM Procedure)	186
Configuring Packet Filter Options (NSM Procedure)	186
Configuring Forwarding Options (NSM Procedure)	187
Configuring IKE (NSM Procedure)	188
Configuring a Gateway (NSM Procedure)	189
Configuring a Policy (NSM Procedure)	191
Configuring a Respond Bad SPI (NSM Procedure)	193
Configuring Traceoptions (NSM Procedure)	193
Configuring the File Options (NSM Procedure)	194
Configuring Flag Options (NSM Procedure)	195
Configuring IPsec (NSM Procedure)	195
Configuring a Policy (NSM Procedure)	196
Configuring Traceoptions (NSM Procedure)	197
Configuring a VPN (NSM Procedure)	198
Configuring VPN Monitor Options (NSM Procedure)	200
Configuring a PKI (NSM Procedure)	201
Configuring Auto Re-enrollment (NSM Procedure)	202
Configuring a CA Profile (NSM Procedure)	202
Configuring Traceoptions (NSM Procedure)	204
Configuring the File Options (NSM Procedure)	205
Configuring Flag Options (NSM Procedure)	206
Configuring NAT (NSM Procedure)	206
Configuring a Destination (NSM Procedure)	207
Configuring Destination NAT (NSM Procedure)	208
Configuring the Interface (NSM Procedure)	210
Configuring a Proxy Address Resolution Protocol (NSM Procedure)	212
Configuring a Source (NSM Procedure)	213
Configuring the Source Nat (NSM Procedure)	216

	Configuring the Static Nat (NSM Procedure)	217
	Configuring Traceoptions (NSM Procedure)	218
	Configuring the File Options (NSM Procedure)	219
	Configuring Flag Options (NSM Procedure)	220
Chapter 14	Configuring Services for J Series Services Routers and SRX Series Services Gateways	221
	Configuring Captive Portal (NSM Procedure)	221
	Configuring Custom Options (NSM Procedure)	222
	Configuring the Interface (NSM Procedure)	223
	Configuring Traceoptions (NSM Procedure)	224
	Configuring File Options (NSM Procedure)	224
	Configuring Flag Options (NSM Procedure)	225
	Configuring Mobile IP (NSM Procedure)	226
	Configuring Access Type (NSM Procedure)	226
	Configuring the Authenticate Mechanism (NSM Procedure)	227
	Configuring Dynamic Home Assignment (NSM Procedure)	228
	Configuring the Home Agent (NSM Procedure)	229
	Configuring Enable Service (NSM Procedure)	229
	Configuring Pool Match Order (NSM Procedure)	230
	Configuring the Virtual Network (NSM Procedure)	230
	Configuring the Peer (NSM Procedure)	231
	Configuring Traceoptions (NSM Procedure)	234
	Configuring File (NSM Procedure)	235
	Configuring Flag (NSM Procedure)	236
	Configuring RPM (NSM Procedure)	237
	Configuring BGP (NSM Procedure)	237
	Configuring Routing Instances (NSM Procedure)	238
	Configuring Probe (NSM Procedure)	239
	Configuring Probe Server (NSM Procedure)	242
	Configuring Service Interface Pools (NSM Procedure)	243
	Configuring Unified Access Control (NSM Procedure)	244
	Configuring Infranet Controller (NSM Procedure)	245
	Configuring Traceoptions (NSM Procedure)	246
Chapter 15	Configuring SNMP for Network Management in J Series Services Routers and SRX Series Services Gateways	247
	Configuring Basic System Identification for SNMP (NSM Procedure)	247
	Configuring SNMP Communities (NSM Procedure)	248
	Configuring SNMP Trap Groups (NSM Procedure)	250
	Configuring SNMP Views (NSM Procedure)	252
	Configuring Client Lists (NSM Procedure)	253
	Configuring the SNMP Local Engine ID (NSM Procedure)	255
	Configuring SNMP Health Monitoring (NSM Procedure)	256
	Configuring the Interfaces on Which SNMP Requests Can Be Accepted (NSM Procedure)	258
	Configuring the SNMP Commit Delay Timer (NSM Procedure)	259
	Configuring SNMP RMON Alarms and Events (NSM Procedure)	260
	Enabling SNMP Access over Routing Instances (NSM Procedure)	264
	Configuring Tracing of SNMP Activity (NSM Procedure)	266

	Configuring SNMP Trap Options (NSM Procedure)	268
	Configuring SNMPv3 (NSM Procedure)	270
Chapter 16	Configuring System for J Series Services Routers and SRX Series Services Gateways	277
	Configuring Accounting (NSM Procedure)	278
	Configuring Destination	278
	Configuring Events	280
	Configuring Traceoptions	280
	Configuring Archival (NSM Procedure)	281
	Configuring ARP (NSM Procedure)	282
	Configuring Authentication Order (NSM Procedure)	283
	Configuring Auto Configuration (NSM Procedure)	284
	Configuring a Backup Router (NSM Procedure)	285
	Configuring a Commit (NSM Procedure)	286
	Configuring Diag Port Authentication (NSM Procedure)	287
	Configuring a Domain Search (NSM Procedure)	287
	Configuring Extensions (NSM Procedure)	288
	Configuring Providers	289
	Configuring Resource Limits	289
	Configuring an Inet6 Backup Router (NSM Procedure)	291
	Configuring Internet Options (NSM Procedure)	292
	Configuring Location (NSM Procedure)	294
	Configuring Login (NSM Procedure)	296
	Configuring Class	297
	Configuring Password	298
	Configuring Retry Options	299
	Configuring User	300
	Configuring a Name Server (NSM Procedure)	301
	Configuring PIC Console Authentication (NSM Procedure)	302
	Configuring Ports (NSM Procedure)	302
	Configuring RADIUS Options (NSM Procedure)	303
	Configuring RADIUS Server (NSM Procedure)	304
	Configuring Root Authentication (NSM Procedure)	305
	Configuring Static Host Mapping (NSM Procedure)	306
	Configuring TACACS+ Options (NSM Procedure)	307
	Configuring TACACS+ Server (NSM Procedure)	308
Chapter 17	Configuring J Series Services Routers and SRX Series Services Gateways for DHCP	311
	Configuring the Device as a DHCP Server (NSM Procedure)	311
	Configuring the Device as a DHCP Client (NSM Procedure)	313
Chapter 18	Configuring Class of Service in J Series Services Routers and SRX Series Services Gateways	315
	Configuring CoS Classifiers (NSM Procedure)	316
	Configuring CoS Code Point Aliases (NSM Procedure)	318
	Configuring CoS Drop Profile (NSM Procedure)	319
	Configuring CoS Forwarding Classes (NSM Procedure)	321
	Configuring CoS Forwarding Policy (NSM Procedure)	323

	Configuring CoS Fragmentation Maps (NSM Procedure)	324
	Configuring CoS Host Outbound Traffic (NSM Procedure)	325
	Configuring CoS Interfaces (NSM Procedure)	326
	Configuring CoS Rewrite Rules (NSM Procedure)	332
	Configuring CoS Schedulers (NSM Procedure)	335
	Configuring CoS and Applying Scheduler Maps (NSM Procedure)	336
	Configuring CoS Traffic Control Profiles (NSM Procedure)	338
Chapter 19	Configuring Event Options in J Series Services Routers and SRX Series Services Gateways	341
	Configuring Event Script (NSM Procedure)	341
	Generating Internal Events (NSM Procedure)	342
	Configuring Event Policy (NSM Procedure)	343
	Configuring Event Policy Tracing Operations (NSM Procedure)	346
Chapter 20	Configuring Firewall in J Series Services Routers and SRX Series Services Gateways	349
	Configuring the Firewall Filter for Any Family Type (NSM Procedure)	349
	Configuring the Firewall Filter for Bridge Family Type (NSM Procedure)	351
	Configuring the Firewall Filter for Ccc Family Type (NSM Procedure)	353
	Configuring Filters for inet Family Type (NSM Procedure)	355
	Configuring Firewall Filter for inet Family Type (NSM Procedure)	355
	Configuring Prefix-specific Actions (NSM Procedure)	357
	Configuring Service Filters (NSM Procedure)	358
	Configuring Simple Filters (NSM Procedure)	359
Chapter 21	Configuring Application Layer Gateways in J Series Services Routers and SRX Series Services Gateways	361
	Configuring H.323 ALG (NSM Procedure)	361
	Configuring SIP ALG (NSM Procedure)	363
	Configuring SCCP ALG (NSM Procedure)	366
	Configuring MGCP ALG (NSM Procedure)	368
	Enabling or Disabling ALGs (NSM Procedure)	371
Chapter 22	Configuring Unified Threat Management Features in J Series Services Routers and SRX Series Services Gateways	375
	Configuring Server-Based Antispam (NSM Procedure)	375
	Configuring Local List Antispam (NSM Procedure)	376
	Configuring Whitelist and Blacklist Entries	376
	Configuring a Custom URL Category List Custom Object	377
	Configuring Server-Based Antispam	377
	Configuring a UTM Policy for SNMP	378
	Configuring Antivirus Protection (NSM Procedure)	379
	Configuring a MIME Pattern List Custom Object	379
	Configuring a Filename Extension List Custom Object	379
	Configuring a URL Pattern List Custom Object	380
	Configuring a Custom URL Category List Custom Object	380
	Configuring an Antivirus Feature Profile	381
	Configuring a UTM Policy for Express Antivirus	383

	Configuring Content Filtering (NSM Procedure)	384
	Configuring a Protocol Command Custom Object	384
	Configuring a Filename Extension List Custom Object	385
	Configuring a MIME Pattern List Custom Object	385
	Configuring a Content–Filtering Feature Profile	385
	Configuring a UTM Policy for Content–Filtering	387
	Configuring Web Filtering (NSM Procedure)	387
	Configuring a URL Pattern List Custom Object	388
	Configuring a Custom URL Category List Custom Object	388
	Configuring a Web Filtering Feature Profile	389
	Configuring a UTM Policy for Web Filtering	391
Chapter 23	Configuring Network Address Translation in J Series Services Routers and SRX Series Services Gateways	393
	Configuring Source NAT Objects on JUNOS OS (NSM Procedure)	393
Chapter 24	Configuring Bridge Domains in J Series Services Routers and SRX Series Services Gateways	397
	Configuring Bridge Domains Properties (NSM Procedure)	397
	Configuring Logical Interfaces (NSM Procedure)	397
	Configuring Multicast Monitoring Options (NSM Procedure)	398
	Configuring VLAN ID (NSM Procedure)	401
Chapter 25	Configuring Forwarding Options in J Series Services Routers and SRX Series Services Gateways	403
	Configuring Accounting Options (NSM Procedure)	403
	Specifying Address Family for Filters (NSM Procedure)	405
	Configuring Load Balancing Using Hash Key (NSM Procedure)	406
	Configuring Helpers (NSM Procedure)	407
	Configuring a Router or Interface to Act as a Bootstrap Protocol Relay Agent	408
	Enabling DNS Request Packet Forwarding	411
	Configuring a Port for a DHCP or BOOTP Relay Agent	413
	Configuring Tracing Operations for BOOTP, DNS, and TFTP Packet Forwarding	415
	Configuring Per–Flow and Per–Prefix Load Balancing (NSM Procedure)	416
	Configuring Port Mirroring (NSM Procedure)	417
Chapter 26	Configuring Interfaces in J Series Services Routers and SRX Series Services Gateways	421
	Configuring Interfaces on the Routing Platform (NSM Procedure)	421
	Configuring Interface Properties (NSM Procedure)	421
	Damping Interface Transitions (NSM Procedure)	423
	Configuring Receive Bucket Properties on Interfaces (NSM Procedure)	424
	Configuring Tracing Operations of an Individual Router Interface (NSM Procedure)	424
	Configuring Transmit Leaky Bucket Properties (NSM Procedure)	425
	Configuring Logical Interface Properties (NSM Procedure)	426
	Configuring Logical Unit Properties (NSM Procedure)	426
	Configuring an IP Demux Underlying Interface (NSM Procedure)	427

	Configuring the Logical Demux Source Family Type on the IP Demux Underlying Interface (NSM Procedure)	428
	Configuring Epd Threshold for the Logical Interface (NSM Procedure)	428
	Configuring Protocol Family Information for the Logical Interface (NSM Procedure)	429
	Configuring Protocol Family (Ccc) Information for the Logical Interface (NSM Procedure)	430
	Configuring Protocol Family (Inet) Information for the Logical Interface (NSM Procedure)	431
	Configuring Protocol Family (Inet6) Information for the Logical Interface (NSM Procedure)	437
	Configuring Protocol Family (ISO) Information for the Logical Interface (NSM Procedure)	444
	Configuring Protocol Family (MPLS) Information for the Logical Interface (NSM Procedure)	445
	Configuring Protocol Family (TCC) Information for the Logical Interface (NSM Procedure)	447
	Configuring the Traffic Shaping Profile (NSM Procedure)	447
	Configuring Interface set on the Routing Platform (NSM Procedure)	449
Chapter 27	Configuring Multicast Snooping Options in J Series Services Routers and SRX Series Services Gateways	451
	Configuring Multicast Monitoring Options (NSM Procedure)	451
Part 3	Managing J Series Services Routers and SRX Series Services Gateways	
Chapter 28	Using System Management Features in J Series Services Routers and SRX Series Services Gateways	457
	Managing J Series and SRX Series Device Software Versions Overview	457
	Viewing and Reconciling Device Inventory Overview	457
	Viewing Device Inventory in NSM (NSM Procedure)	458
	Removing a J Series or SRX Series Device from NSM Management (NSM Procedure)	459
Chapter 29	Topology Manager	461
	Overview of the NSM Topology Manager	461
	Requisites for a Topology Discovery Overview	461
	Understanding the NSM Topology Manager Toolbar	462
Chapter 30	IDP Management in J Series Services Routers and SRX Series Services Gateways	465
	Updating the NSM Attack Database (NSM Procedure)	465
	Loading the IDP Detector Engine on a J Series or SRX Series Device (NSM Procedure)	466
	Updating the Deep Inspection Attack Database on a J Series or SRX Series Device (NSM Procedure)	466

Part 4	Monitoring J Series Services Routers and SRX Series Services Gateways	
Chapter 31	Real Time Monitoring of J Series Services Routers and SRX Series Services Gateways	471
	Realtime Monitor Overview	471
	Viewing Device Status	471
	Viewing Device Monitor Alarm Status (NSM Procedure)	474
	Configuring the Polling Interval for Device Alarm Status (NSM Procedure)	475
Part 5	Index	
	Index	479

About this Guide

- [Objectives on page xv](#)
- [Audience on page xvi](#)
- [Conventions on page xvi](#)
- [List of Technical Publications on page xvii](#)
- [Requesting Technical Support on page xviii](#)

Objectives

Network and Security Manager (NSM) is a software application that centralizes control and management of your Juniper Networks devices. With NSM, Juniper Networks delivers integrated, policy-based security and network management for all security devices.



NOTE: NSM supports only the domestic version of JUNOS on J Series and SRX Series platforms.

This guide provides the information you need to understand, configure, and maintain J Series Services Routers and SRX Series Services Gateways using NSM. The J Series and SRX Series device configuration features that are detailed in this guide are as follows:

- User Authentication
- Chassis
- USB Modem Interfaces
- Policy Options
- Routing Options
- Protocols
- Integrated Convergence Services
- SNMP
- DHCP
- Class of Service
- Application Layer Gateway (ALG)
- Unified Threat Management (UTM)



NOTE: Because the NSM device-side configuration guides are not updated on the same release schedule as the JUNOS releases, consult the [JUNOS Software Documentation](#) for information about configuration settings that might occur in NSM and not in the device-side configuration guides or vice versa.

Audience

This guide is for the system administrator responsible for configuring J Series Services Routers and SRX Series Services Gateways.

Conventions

Table 1 on page xvi 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 xvi defines text conventions used in this guide.

Table 2: Text Conventions

Convention	Description	Examples
Bold typeface like this	<ul style="list-style-type: none"> Represents commands and keywords in text. Represents keywords Represents UI elements 	<ul style="list-style-type: none"> Issue the clock source command. Specify the keyword exp-msg. Click User Objects
Bold typeface like this	Represents text that the user must type.	user input

Table 2: Text Conventions (*continued*)

Convention	Description	Examples
fixed-width font	Represents information as displayed on the terminal screen.	host1# show ip ospf Routing Process OSPF 2 with Router ID 5.5.0.250 Router is an area Border Router (ABR)
Key names linked with a plus (+) sign	Indicates that you must press two or more keys simultaneously.	Ctrl + d
<i>Italics</i>	<ul style="list-style-type: none"> Emphasizes words Identifies variables 	<ul style="list-style-type: none"> The product supports two levels of access, <i>user</i> and <i>privileged</i>. <i>clusterID</i>, <i>ipAddress</i>.
The angle bracket (>)	Indicates navigation paths through the UI by clicking menu options and links.	Object Manager > User Objects > Local Objects

Table 3 on page xvii defines syntax conventions used in this guide.

Table 3: Syntax Conventions

Convention	Description	Examples
Words in plain text	Represent keywords	terminal length
Words in italics	Represent variables	<i>mask</i> , <i>accessListName</i>
Words separated by the pipe () symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. The keyword or variable can be optional or required.	diagnostic line
Words enclosed in brackets ([])	Represent optional keywords or variables.	[internal external]
Words enclosed in brackets followed by and asterisk ([]*)	Represent optional keywords or variables that can be entered more than once.	[level1 level2 11]*
Words enclosed in braces ({ })	Represent required keywords or variables.	{ permit deny } { in out } { clusterId ipAddress }

List of Technical Publications

Table 4 on page xviii lists the manuals supporting Network and Security Manager and JUNOS software for J Series and SRX Series platforms. All documents are available at <http://www.juniper.net/techpubs/>.

Table 4: Technical Documentation for NSM and J Series Services Routers and SRX Series Services Gateways

Network and Security Manager Installation Guide	Details the steps to install the NSM management system on a single server or on separate servers. It also includes information on how to install and run the NSM user interface. This guide is intended for IT administrators responsible for the installation and/or upgrade of NSM.
Network and Security Manager Administration Guide	<p>Describes how to use and configure key management features in the NSM. It provides conceptual information, suggested workflows, and examples where applicable. This guide is best used in conjunction with the NSM Online Help, which provides step-by-step instructions for performing management tasks in the NSM UI.</p> <p>This guide is intended for application administrators or those individuals responsible for owning the server and security infrastructure and configuring the product for multi-user systems. It is also intended for device configuration administrators, firewall and VPN administrators, and network security operation center administrators.</p>
Network and Security Manager Configuring Firewall/VPN Devices Guide	Describes NSM features that relate to device configuration and management. It also explains how to configure basic and advanced NSM functionality, including deploying new device configurations, managing Security Policies and VPNs, and general device administration.
Network and Security Manager Online Help	Provides task-oriented procedures describing how to perform basic tasks in the NSM user interface. It also includes a brief overview of the NSM system and a description of the GUI elements.
JUNOS Software Interfaces and Routing Configuration Guide	Explains how to configure SRX Series and J Series interfaces for basic IP routing with standard routing protocols, ISDN service, firewall filters (access control lists), and class-of-service (CoS) traffic classification.
JUNOS Software Security Configuration Guide	Explains how to configure and manage SRX Series and J Series security services such as stateful firewall policies, IPsec VPNs, firewall screens, Network Address Translation (NAT), Public Key Cryptography, chassis clusters, Application Layer Gateways (ALGs), and Intrusion Detection and Prevention (IDP).
JUNOS Software Administration Guide	Shows how to monitor SRX Series and J Series devices and routing operations, firewall and security services, system alarms and events, and network performance. This guide also shows how to administer user authentication and access, upgrade software, and diagnose common problems.

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

Getting Started

- [Understanding J Series Services Router and SRX Series Services Gateway Configuration on page 3](#)
- [J Series Services Routers and SRX Series Services Gateways and NSM Installation and Integration Overview on page 7](#)

CHAPTER 1

Understanding J Series Services Router and SRX Series Services Gateway Configuration

- [NSM and Device Management Overview on page 3](#)
- [Communication Between NSM and a Device Overview on page 3](#)
- [Device Configurations Supported in NSM for the J Series Services Router and SRX Series Services Gateway on page 5](#)

NSM and Device Management Overview

NSM is the Juniper Networks network management tool that allows distributed administration of network appliances. You can use the NSM application to centralize status monitoring, logging, and reporting, and to administer device configurations.

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 device's admin console. The configuration screens rendered through NSM are similar to the screens in the device's admin console.

NSM incorporates a broad configuration management framework that allows co-management 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

- [Communication Between NSM and a Device Overview on page 3](#)
- [Device Configurations Supported in NSM for the J Series Services Router and SRX Series Services Gateway on page 5](#)

Communication Between NSM and a Device Overview

The NSM application and a device communicate through the Device Management Interface (DMI). DMI is a collection of schema-driven protocols that run on a common transport (that is, TCP). DMI is designed to work with Juniper Networks platforms to

make device management consistent across all administrative realms. Supported DMI protocols include:

- NetConf (for inventory management, XML-based configuration, text-based configuration, alarm monitoring, and device specific commands)
- Structured syslog
- 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 device's configuration is represented as a hierarchical tree of configuration items. This structure is expressed in XML and can be manipulated with NetConf. NetConf is a network management protocol that uses XML. DMI uses NetConf's generic configuration management capability to allow remote configuration of the device.

To allow NSM to manage the device using the DMI protocol, NSM must import the schema and metadata files from the Juniper Networks Schema Repository, a publicly accessible resource that is updated with each device release. In addition to downloading the device's current schema, NSM may also download upgraded software.

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

Before attempting to communicate with NSM, you must first complete the initial configuration of the device. Initial configuration includes network interface settings, DNS settings, licensing, and password administration.

If you have several devices that will be configured in a clustering environment, the cluster abstraction must first be created in the NSM Cluster Manager. Then you can add individual nodes.

After you have completed the initial network configuration, you can configure the device to communicate with NSM using the appropriate network information. Once the device has been configured to communicate with NSM, the device contacts NSM and establishes a DMI session through an initial TCP handshake.

All communications between the device and NSM occur over SSH to ensure data integrity.

After the device initially contacts NSM and a TCP session is established, interaction between the device and NSM is driven from NSM, which issues commands to get hardware, software, and license details of the device. NSM connects to the Schema Repository to download the configuration schema that is specific to the device.

NSM then issues a command to retrieve configuration information from the device. If NSM is contacted by more than one device as a member of a cluster, information from only one of the cluster devices is gathered. NSM attempts to validate the configuration received from the device against the schema from Juniper Networks.

Once the device and NSM are communicating, the device delivers syslog and event information to NSM.

After NSM and the device are connected, you can make any configuration changes directly on the device, bypassing NSM. NSM automatically detects these changes and imports the new configuration data. Changes to device cluster members will similarly be detected by NSM.

When you make changes to the device's configuration through NSM, you must push the changes to the device by performing an Update Device operation.

When you double-click the device icon in the Device Manager and select the **Configuration** tab, the configuration tree appears in the main display area in the same orientation as items appear on the device's admin console.

**Related
Documentation**

- [NSM and Device Management Overview on page 3](#)
- [Device Configurations Supported in NSM for the J Series Services Router and SRX Series Services Gateway on page 5](#)

Device Configurations Supported in NSM for the J Series Services Router and SRX Series Services Gateway

NSM supports the following services for J Series Services Router and SRX Series services gateway platforms:

- Inventory management service—Enables management of the software, hardware, and licensing details for the J Series Services Router and the SRX Series services gateway. Adding or deleting licenses and upgrading or downgrading software are not supported.
- Status monitoring service—Allows the status of the J Series Services Router and the SRX Series services gateway to be obtained, including name, domain, OS version, synchronization status, connection details, and current alarms.
- Logging service—Allows logs to be obtained in a time-generated order for the J Series Services Router and the SRX Series services gateway device. Logging configuration details that are set on the J Series Services Router and the SRX Series services gateway will apply to NSM.
- XML-based configuration management service—Enables NSM to manage the configuration of the J Series Services Router and the SRX Series services gateway. NSM uses the same XML schema as the J Series Services Router and the SRX Series services gateway, so you can troubleshoot NSM using XML files downloaded from either device.



NOTE: NSM supports only the domestic version of JUNOS on J Series and SRX Series platforms.

The following device configurations are not supported:

- Editing licensing information, although licenses can be viewed
- Packaging log files or debug files for remote analysis

- Related Documentation**
- [NSM and Device Management Overview on page 3](#)
 - [Communication Between NSM and a Device Overview on page 3](#)

CHAPTER 2

J Series Services Routers and SRX Series Services Gateways and NSM Installation and Integration Overview

- J Series Services Router and SRX Series Services Gateway Installation and Configuration Overview on page 7
- NSM Installation Overview on page 8
- Adding J Series Services Routers or SRX Series Services Gateways in NSM Overview on page 8
- Adding J Series Services Router Clusters and SRX Series Services Gateway Clusters Overview on page 8
- Adding J Series Services Router Clusters and SRX Series Services Gateway Virtual Chassis Clusters Overview on page 9
- Using Templates and Configuration Groups in NSM Overview on page 10

J Series Services Router and SRX Series Services Gateway Installation and Configuration Overview



NOTE: For important safety information, read the *Juniper Networks Security Products Safety Guide*.

Before you can add either a J Series Services Router or an SRX Series services gateway to NSM, the device must be installed and configured, and logon credentials for an NSM administrator must be configured for it. Follow these steps:

1. Connect the device to the network and configure one of the interfaces so that the device can reach the NSM device server.
2. Add a user for NSM that has full administrative rights.

For complete details on installing and configuring J Series Services Routers, see the corresponding Hardware Guide for your device.

For complete details on installing and configuring SRX Series services gateway, see the corresponding Hardware Guide for your device.

- Related Documentation**
- [NSM Installation Overview on page 8](#)
 - [NSM and Device Management Overview on page 3](#)
 - [Communication Between NSM and a Device Overview on page 3](#)

NSM Installation Overview

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).

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

- Related Documentation**
- [J Series Services Router and SRX Series Services Gateway Installation and Configuration Overview on page 7](#)
 - [NSM and Device Management Overview on page 3](#)

Adding J Series Services Routers or SRX Series Services Gateways in NSM Overview

Before NSM can manage devices, you must first add those devices to the management system using the NSM 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.

For complete details on adding J Series Services Routers or SRX Series services gateways, see the *Network and Security Manager Administration Guide*.

- Related Documentation**
- [NSM and Device Management Overview on page 3](#)
 - [Communication Between NSM and a Device Overview on page 3](#)
 - [Device Configurations Supported in NSM for the J Series Services Router and SRX Series Services Gateway on page 5](#)
 - [Adding J Series Services Router Clusters and SRX Series Services Gateway Clusters Overview on page 8](#)

Adding J Series Services Router Clusters and SRX Series Services Gateway Clusters Overview

A cluster consists of multiple devices joined together in a high availability configuration to ensure continued network uptime. The device configurations are synchronized, meaning

all cluster members share the same configuration settings, enabling a device to handle traffic for another if one device fails.

Adding a cluster is a two-stage process:

- Add the cluster device object.
- Add the members of the cluster to the cluster device object.

For complete details on adding J Series Services Router clusters or SRX Series services gateway clusters, see the *Network and Security Manager Administration Guide*.

**Related
Documentation**

- [NSM and Device Management Overview on page 3](#)
- [Communication Between NSM and a Device Overview on page 3](#)
- [Device Configurations Supported in NSM for the J Series Services Router and SRX Series Services Gateway on page 5](#)
- [Adding J Series Services Routers or SRX Series Services Gateways in NSM Overview on page 8](#)

Adding J Series Services Router Clusters and SRX Series Services Gateway Virtual Chassis Clusters Overview

Network and Security Manager (NSM) supports a single connection between two cluster members of SRX Series Services Gateway cluster through the **fxp0** interface on the device. These clusters are represented by a virtual chassis.

Adding an SRX Series Services Gateway virtual chassis cluster is similar to adding an SRX Series Services Gateway chassis cluster. In NSM, select the **Virtual Chassis** check box when you add a device either through an unreachable workflow or while modeling the device.

For complete information about how to add J Series Services Router clusters or SRX Series Services Gateway virtual chassis clusters, see the *Network and Security Manager Administration Guide*.

**Related
Documentation**

- [NSM and Device Management Overview on page 3](#)
- [Communication Between NSM and a Device Overview on page 3](#)
- [Device Configurations Supported in NSM for the J Series Services Router and SRX Series Services Gateway on page 5](#)
- [Adding J Series Services Routers or SRX Series Services Gateways in NSM Overview on page 8](#)
- [Adding J Series Services Router Clusters and SRX Series Services Gateway Clusters Overview on page 8](#)

Using Templates and Configuration Groups in NSM Overview

Use templates to define a common device configuration and then reuse that configuration information across multiple devices. In a template, you need to define only those configuration parameters that you want to set; you do not need to specify a complete device configuration.

Templates provide these benefits:

- You can configure parameter values for a device by referring to one or more templates when configuring the device.
- When you change a parameter value in a template and save the template, the value also changes for all device configurations that refer to that template, unless specifically overridden in the device object.

For complete details on using device templates and configuration groups, see the *Network and Security Manager Administration Guide*.

Related Documentation

- [Adding J Series Services Routers or SRX Series Services Gateways in NSM Overview on page 8](#)
- [Adding J Series Services Router Clusters and SRX Series Services Gateway Clusters Overview on page 8](#)

PART 2

Configuring J Series Services Routers and SRX Series Services Gateways



NOTE: Because the NSM device-side configuration guides are not updated on the same release schedule as the JUNOS releases, consult the [JUNOS Software Documentation](#) for information about configuration settings that might occur in NSM and not in the device-side configuration guides or vice versa.

- [Configuring Access in J Series Services Routers and SRX Series Services Gateways on page 13](#)
- [Configuring Access Profile in J Series Services Routers and SRX Series Services Gateways on page 31](#)
- [Configuring Accounting Options in J Series Services Routers and SRX Series Services Gateways on page 33](#)
- [Configuring Applications in J Series Services Routers and SRX Series Services Gateways on page 41](#)
- [Configuring User Authentication in J Series Services Routers and SRX Series Services Gateways on page 43](#)
- [Configuring Chassis in J Series Services Routers and SRX Series Services Gateways on page 53](#)
- [Configuring USB Modem Interfaces in J Series Services Routers and SRX Series Services Gateways on page 67](#)
- [Configuring Policy Options in J Series Services Routers and SRX Series Services Gateways on page 73](#)
- [Configuring Routing Options in J Series Services Routers and SRX Series Services Gateways on page 81](#)
- [Configuring Protocols for J Series Services Routers and SRX Series Services Gateways on page 107](#)
- [Configuring Security for J Series Services Routers and SRX Series Services Gateways on page 177](#)
- [Configuring Services for J Series Services Routers and SRX Series Services Gateways on page 221](#)

- [Configuring SNMP for Network Management in J Series Services Routers and SRX Series Services Gateways on page 247](#)
- [Configuring System for J Series Services Routers and SRX Series Services Gateways on page 277](#)
- [Configuring J Series Services Routers and SRX Series Services Gateways for DHCP on page 311](#)
- [Configuring Class of Service in J Series Services Routers and SRX Series Services Gateways on page 315](#)
- [Configuring Event Options in J Series Services Routers and SRX Series Services Gateways on page 341](#)
- [Configuring Firewall in J Series Services Routers and SRX Series Services Gateways on page 349](#)
- [Configuring Application Layer Gateways in J Series Services Routers and SRX Series Services Gateways on page 361](#)
- [Configuring Unified Threat Management Features in J Series Services Routers and SRX Series Services Gateways on page 375](#)
- [Configuring Network Address Translation in J Series Services Routers and SRX Series Services Gateways on page 393](#)
- [Configuring Bridge Domains in J Series Services Routers and SRX Series Services Gateways on page 397](#)
- [Configuring Forwarding Options in J Series Services Routers and SRX Series Services Gateways on page 403](#)
- [Configuring Interfaces in J Series Services Routers and SRX Series Services Gateways on page 421](#)
- [Configuring Multicast Snooping Options in J Series Services Routers and SRX Series Services Gateways on page 451](#)

CHAPTER 3

Configuring Access in J Series Services Routers and SRX Series Services Gateways

- [Configuring Address Assignment \(NSM Procedure\) on page 13](#)
- [Configuring an Address Pool \(NSM Procedure\) on page 18](#)
- [Configuring a Group Profile \(NSM Procedure\) on page 19](#)
- [Configuring LDAP Options \(NSM Procedure\) on page 20](#)
- [Configuring the LDAP Server \(NSM Procedure\) on page 22](#)
- [Configuring a SecurID Server \(NSM Procedure\) on page 23](#)
- [Configuring RADIUS Options \(NSM Procedure\) on page 24](#)
- [Configuring a RADIUS Server \(NSM Procedure\) on page 24](#)
- [Configuring Firewall Authentication \(NSM Procedure\) on page 26](#)

Configuring Address Assignment (NSM Procedure)

The address assignment feature allows you to configure the neighbor discovery router advertisement and the pool address.

To configure address 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 the address assignment feature.
3. Click the **Configuration** tab. In the configuration tree, select **Access > Address Assignment**.
4. Enter a comment for the address assignment in **Comment**.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

- **Apply**—Applies the address assignment parameters.
- [Configuring Neighbor Discovery Router Advertisement on page 14](#)
- [Configuring Pool on page 14](#)

Configuring Neighbor Discovery Router Advertisement

To configure neighbor discovery router advertisement (NDRA):

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 NDRA feature.
3. Click the **Configuration** tab. In the configuration tree, select **Access > Address Assignment > Neighbor Discovery Router Advertisement**.
4. Add or modify settings as specified in [Table 5 on page 14](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the NDRA settings.

Table 5: Neighbor Discovery Router Advertisement Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the NDRA.	(Optional) Enter a comment.
Ndra Name	Specifies the designated NDRA pool name.	Enter the NDRA pool name.

Configuring Pool

To configure the address pool 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 address pool feature.
3. Click the **Configuration** tab. In the configuration tree, select **Access > Address Assignment > Pool**.
4. Click + to configure address pool settings.
5. Enter an address pool name, in the **Name** field.
6. Enter a comment for the address pool in **Comment**.
7. Enter an address pool link name in **Link**.
8. In the configuration tree, select **Access > Address Assignment > Pool > pool > Family**.
9. Click **Enable Feature** to configure the address pool family details.

10. Add or modify settings as specified in [Table 6 on page 15](#).

11. Click one:

- **OK**—Saves the changes.
- **Cancel**—Cancels the modifications.
- **Apply**—Applies the address pool settings.

Table 6: Pool Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the address pool.	(Optional) Enter a comment.
pool > Family > Inet		
None	Specifies that neither inet nor inet6 is chosen.	Select the option.
pool > Family > inet > Inet		
Comment	Supplies a descriptive comment for the Inet address pool.	(Optional) Enter a comment.
Network	Specifies the Inet network address.	Enter the Inet network address.
pool > Family > inet > Inet > Dhcp Attributes		
Comment	Supplies a descriptive comment for the Inet Dynamic Host Configuration Protocol (DHCP) attributes.	(Optional) Enter a comment.
Maximum Lease Time	Specifies the maximum lease time advertised to clients.	Select the maximum lease time from the list.
Server Identifier	Specifies the server IP address value.	Enter the server IP address value.
Grace Period	Specifies the grace period for the leases.	Select the grace period time. Range: 0 through 4,294,967,295.
Domain Name	Specifies the domain name advertised to clients.	Enter the domain name.
Boot File	Specifies the boot filename advertised to clients.	Enter the boot filename.
Boot Server	Specifies the boot server advertised to clients.	Enter the boot server name.
Tftp Server	Specifies the Trivial File Transfer Protocol (TFTP) server advertised to clients.	Enter the TFTP server name.
Netbios Node Type	Specifies the type of Network Basic Input/Output System (NetBIOS) node advertised to clients.	Select the NetBIOS node type from the list.
Sip Server Domain Name	Specifies the Session Initiation Protocol (SIP) server domain name available to clients.	Enter the SIP server domain name.

Table 6: Pool Configuration Details (*continued*)

Option	Function	Your Action
pool > Family > inet > Inet > Dhcp Attributes > Dns Server		
Name	Specifies the Domain Name System (DNS) server's Internet Protocol Version 6 (IPv6) address.	Enter the DNS server IPv4 address name.
Comment	Supplies a descriptive comment for the DNS server IPv4 name.	(Optional) Enter a comment.
pool > Family > inet > Inet > Dhcp Attributes > Name Server		
Name	Specifies the DNS server's Internet Protocol Version 4 (IPv4) address.	Enter the DNS server IPv4 address name.
Comment	Supplies a descriptive comment for the DNS server IPv4 name.	(Optional) Enter a comment.
pool > Family > inet > Inet > Dhcp Attributes > Option		
Name	Specifies the DHCP option identifier code.	Select the DHCP option identifier code. Range: 0 through 4,294,967,295.
Comment	Supplies a descriptive comment for the option.	(Optional) Enter a comment.
pool > Family > inet > Inet > Dhcp Attributes > Option > Flag		
Flag	Specifies the flag option setting.	Select and enter flag option settings from the list.
pool > Family > inet > Inet > Dhcp Attributes > Option Match		
Comment	Supplies a descriptive comment for the option match.	(Optional) Enter a comment.
pool > Family > inet > Inet > Dhcp Attributes > Option Match > Option 82 > Circuit Id		
Name	Specifies the circuit identifier name.	Enter the circuit identifier name.
Comment	Supplies a descriptive comment for the circuit identifier.	(Optional) Enter a comment.
Range	Specifies the range name for the circuit identifier.	Enter the range name for the circuit identifier.
pool > Family > inet > Inet > Dhcp Attributes > Option Match > Option 82 > Remote Id		
Name	Specifies the remote identifier name.	Enter the remote identifier name.
Comment	Supplies a descriptive comment for the remote identifier.	(Optional) Enter a comment.

Table 6: Pool Configuration Details (*continued*)

Option	Function	Your Action
Range	Specifies the range name for the remote identifier.	Enter the range name for the remote identifier.
pool > Family > inet > Inet > Dhcp Attributes > Router		
Name	Specifies the name of the IPv4 address of the device.	Enter the device IPv4 address name.
Comment	Supplies a descriptive comment for the device.	(Optional) Enter a comment.
pool > Family > inet > Inet > Dhcp Attributes > Sip Server Address		
Name	Specifies the SIP server's IPv4 address name.	Enter the SIP server's IPv4 address name.
Comment	Supplies a descriptive comment for the SIP server's IPv4 address.	(Optional) Enter a comment.
pool > Family > inet > Inet > Dhcp Attributes > Wins Server		
Name	Specifies the Windows Internet Name Service (WINS) server's IPv4 address name.	Enter the WINS server's IPv4 address name.
Comment	Supplies a descriptive comment for the WINS server's IPv4 address.	(Optional) Enter a comment.
pool > Family > inet > Inet > Host		
Name	Specifies the hostname.	Enter the hostname.
Comment	Supplies a descriptive comment for the host.	(Optional) Enter a comment.
Hardware Address	Specifies the hardware address.	Enter the hardware address.
Ip Address	Specifies the reserved address.	Enter the reserved address.
pool > Family > inet > Inet > Range		
Name	Specifies the range name.	Enter the range name.
Comment	Supplies a descriptive comment for the range.	(Optional) Enter a comment.
Low	Specifies the lower limit of the address range.	Enter the lower limit of the address range.
High	Specifies the upper limit of the address range.	Enter the upper limit of the address range.
pool > Family > inet6 > Inet6 > Dhcp Attributes		
Follow the similar procedure of configuring Inet DHCP attributes (Table 6 on page 15) to configure the Inet DHCP attributes too.		

Table 6: Pool Configuration Details (*continued*)

Option	Function	Your Action
pool > Family > inet6 > Inet6 > Range		
Name	Specifies the IPv6 range name.	Enter the IPv6 range name.
Comment	Supplies a descriptive comment for the IPv6 range.	(Optional) Enter a comment.
Low	Specifies the lower limit of the IPv6 address range.	Enter the lower limit of the IPv6 address range.
High	Specifies the upper limit of the IPv6 address range.	Enter the upper limit of the IPv6 address range.
Prefix Length	Specifies the IPv6 delegated prefix length.	Choose the IPv6 delegated prefix length. Range: 1 through 128.

Related Documentation

- [Configuring an Address Pool \(NSM Procedure\) on page 18](#)
- [Configuring a Group Profile \(NSM Procedure\) on page 19](#)
- [Configuring LDAP Options \(NSM Procedure\) on page 20](#)

Configuring an Address Pool (NSM Procedure)

You can configure an address pool.

To configure an address pool:

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 address pool feature.
3. Click the **Configuration** tab. In the configuration tree, select **Access > Address Pool**.
4. Click + to configure the address pool options as specified in [Table 7 on page 18](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the address pool parameters.

Table 7: Address Pool Configuration Details

Option	Function	Your Action
Name	Specifies the address pool name.	Enter a name for the address pool.
Primary Dns	Specifies the primary Domain Name System (DNS) server name.	Enter the primary DNS name.

Table 7: Address Pool Configuration Details (*continued*)

Option	Function	Your Action
Comment	Supplies a descriptive comment for the address pool.	(Optional) Enter a comment.
Secondary Dns	Specifies the secondary DNS server name.	Enter the secondary DNS name.
Primary Wins	Specifies the primary WINS server.	Enter the primary WINS server name.
Secondary Wins	Specifies the secondary WINS server.	Enter the secondary WINS server name.

Related Documentation

- [Configuring Address Assignment \(NSM Procedure\) on page 13](#)
- [Configuring a Group Profile \(NSM Procedure\) on page 19](#)
- [Configuring LDAP Options \(NSM Procedure\) on page 20](#)

Configuring a Group Profile (NSM Procedure)

You can configure a group profile to define the Point-to-Point Protocol (PPP) attributes.

To configure a group 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 group profile feature.
3. Click the **Configuration** tab. In the configuration tree, select **Access > Group Profile**.
4. Click + to configure the group profile options as specified in [Table 8 on page 19](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the group profile parameters.

Table 8: Group Profile Configuration Details

Option	Function	Your Action
Name	Specifies the group profile name.	Enter a name for the group profile.
Comment	Supplies a descriptive comment for the group profile.	(Optional) Enter a comment.
group-profile > Ppp		
Enable Feature	Specifies that you can enable this feature to configure the PPP.	Select the check box to enable the feature.
Comment	Supplies a descriptive comment for the PPP.	(Optional) Enter a comment.

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

Option	Function	Your Action
Framed Pool	Specifies the address pool used to assign an address for the user.	Select an option from the list.
Idle Timeout	Specifies the idle timeout before termination of the session.	Enter the idle timeout value. Range: 1 - 4,294,967,295.
Keepalive	Specifies the PPP keepalive interval.	Enter the PPP keepalive interval time. Range: 1 - 32,767.
Primary Dns	Specifies the primary Domain Name System (DNS) server name.	Enter the primary DNS server name.
Secondary Dns	Specifies the secondary DNS server name.	Enter the secondary DNS server name.
Primary Wins	Specifies the primary Windows Internet Name Service (WINS) server name.	Enter the primary WINS server name.
Secondary Wins	Specifies the secondary WINS server name.	Enter the secondary WINS server name.
Encapsulation Overhead	Specifies the encapsulation overhead for class of service calculation.	Enter an encapsulation overhead value. Range: -63 through 64.
Cell Overhead	Specifies the ATM cell overhead for the class of service calculation.	Select the check box to enable this feature.
Interface Id	Specifies the interface identifier to look up the session information.	Enter the interface identifier.

Related Documentation

- [Configuring Address Assignment \(NSM Procedure\) on page 13](#)
- [Configuring an Address Pool \(NSM Procedure\) on page 18](#)
- [Configuring LDAP Options \(NSM Procedure\) on page 20](#)

Configuring LDAP Options (NSM Procedure)

You can configure Lightweight Directory Access Protocol (LDAP) authentication options.

To configure LDAP 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 LDAP options.
3. Click the **Configuration** tab. In the configuration tree, select **Access > Ldap Options**.
4. Enter a comment for the LDAP option in **Comment**.

5. Enter the amount of time that elapses before the primary server is contacted, if backup server is being used in **Revert Interval**.
6. Enter a distinguished name (DN) in **Base Distinguished Name**.

**NOTE:**

The base distinguished name can be used in one of the following ways:

- If you are using the *assemble* statement so that the user's distinguished name is being assembled, the base distinguished name is appended to a username to generate the user's distinguished name. The resulting distinguished name is used in the LDAP bind call.
- If you are using the *search* statement so that the user's distinguished name is found by a search, the search is restricted to the subtree of the base distinguished name.

7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the LDAP option parameters.
- [Configuring Assemble on page 21](#)

Configuring Assemble

To configure an assemble:

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 assemble feature.
3. Click the **Configuration** tab. In the configuration tree, select **Access > Ldap Options > Assemble**.
4. Select an option to configure the assemble feature.
5. Add or modify settings as specified in [Table 9 on page 21](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the assemble settings.

Table 9: Assemble Configuration Details

Option	Function	Your Action
Ldap Options > Assemble > assemble		

Table 9: Assemble Configuration Details (*continued*)

Option	Function	Your Action
Comment	Supplies a descriptive comment for the assemble option.	(Optional) Enter a comment.
Common Name	Specifies the prefix for the user distinguished name.	Enter a common name.
Ldap Options > Assemble > search		
Comment	Supplies a descriptive comment for the search option.	(Optional) Enter a comment.
Search Filter	Specifies the filter to use in the search.	Enter the search filter.
Ldap Options > Assemble > search > Admin Search		
Enable Search	Specifies configuration of the admin search.	Select the check box to enable the feature.
Comment	Supplies a descriptive comment for the admin search.	(Optional) Enter a comment.
Distinguished Name	Specifies the administrator's distinguished name.	Enter the administrator's distinguished name.
Password	Specifies the administrator password.	Enter the password.

Related Documentation

- [Configuring an Address Pool \(NSM Procedure\) on page 18](#)
- [Configuring a Group Profile \(NSM Procedure\) on page 19](#)
- [Configuring Address Assignment \(NSM Procedure\) on page 13](#)

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 23](#).
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 \(NSM Procedure\) on page 20](#)

Configuring a SecurID Server (NSM Procedure)

You can configure a securID server to authenticate clients for remote virtual private network (VPN) access.

To configure a securID 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 securID server feature.
3. Click the **Configuration** tab. In the configuration tree, select **Access > Securid Server**.
4. Click + to configure the securID server options as specified in [Table 11 on page 24](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the securID server parameters.

Table 11: SecurID Server Configuration Details

Option	Function	Your Action
Name	Specifies the name of the securID server.	Enter a securID server name.
Comment	Supplies a descriptive comment for the securID server.	(Optional) Enter a comment.
Configuration File	Specifies the path to the securID server configuration file.	Enter the path to the securID server configuration file.

Related Documentation

- [Configuring an Address Pool \(NSM Procedure\) on page 18](#)
- [Configuring a Group Profile \(NSM Procedure\) on page 19](#)
- [Configuring the LDAP Server \(NSM Procedure\) on page 22](#)

Configuring RADIUS Options (NSM Procedure)

You can configure RADIUS options.

To configure RADIUS 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 RADIUS options feature.
3. Click the **Configuration** tab. In the configuration tree, select **Access > Radius Options**.
4. Enter a comment that describes the RADIUS options in **Comment**.
5. Enter the amount of time for the router to wait after the server has become unreachable in **Revert Interval**.
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the RADIUS options parameters.

Related Documentation

- [Configuring a RADIUS Server \(NSM Procedure\) on page 24](#)
- [Configuring Firewall Authentication \(NSM Procedure\) on page 26](#)
- [Configuring a SecurID Server \(NSM Procedure\) on page 23](#)

Configuring a RADIUS Server (NSM Procedure)

You can configure RADIUS server.

To configure a RADIUS 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 RADIUS server feature.
3. Click the **Configuration** tab. In the configuration tree, select **Access > Radius Server**.
4. Click + to configure RADIUS server options as described in [Table 12 on page 25](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the RADIUS server parameters.

Table 12: RADIUS Server Configuration Details

Option	Function	Your Action
Name	Specifies the RADIUS server internet protocol (IP) address name.	Enter a RADIUS server IP address name.
Comment	Supplies a descriptive comment about the RADIUS sever.	(Optional) Enter a comment.
Port	Specifies the RADIUS server authentication port number.	Set the RADIUS server authentication port number. Range: 1 through 65535.
Accounting Port	Specifies the port number for sending the RADIUS server messages.	Set the accounting port number. Range: 1 through 65535.
Secret	Specifies the shared secret password with the RADIUS server.	Enter the shared secret password value.
Timeout	Specifies the request timeout period.	Set the timeout period. Range: 1 through 90.
Retry	Specifies the number of retry attempts.	Set the retry attempts. Range: 1 through 10.
Source Address	Specifies the source address of the RADIUS server.	Enter the source address for the RADIUS server.
Routing Instance	Specifies the collection of routing tables used to send RADIUS packets to the RADIUS server.	Select the routing instance from the list.

Related Documentation

- [Configuring RADIUS Options \(NSM Procedure\) on page 24](#)
- [Configuring Firewall Authentication \(NSM Procedure\) on page 26](#)

- [Configuring a SecurID Server \(NSM Procedure\) on page 23](#)

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 26](#)
 - [Configuring Traceoptions on page 27](#)
 - [Configuring Web Authentication on page 28](#)

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 13 on page 27](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the pass-through settings.

Table 13: 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 14 on page 27](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the traceoptions settings.

Table 14: Traceoptions Configuration Details

Option	Function	Your Action
Firewall Authentication > Traceoptions > File		
Comment	Supplies a descriptive comment for the file traceoptions.	(Optional) Enter a comment.

Table 14: Traceoptions Configuration Details (*continued*)

Option	Function	Your Action
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.
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 15 on page 29](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the Web authentication settings.

Table 15: 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 \(NSM Procedure\) on page 24](#)
- [Configuring RADIUS Options \(NSM Procedure\) on page 24](#)
- [Configuring a SecurID Server \(NSM Procedure\) on page 23](#)

Configuring Access Profile in J Series Services Routers and SRX Series Services Gateways

- [Configuring the Access Profile \(NSM Procedure\)](#) on page 31

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 16 on page 31](#).
5. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 16: 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 \(NSM Procedure\)](#)
 - [Configuring the RADIUS Parameters \(NSM Procedure\)](#)

CHAPTER 5

Configuring Accounting Options in J Series Services Routers and SRX Series Services Gateways

- [Configuring Accounting Options \(NSM Procedure\) on page 33](#)

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 33](#)
- [Configuring a Log File \(NSM Procedure\) on page 34](#)
- [Configuring the Filter Profile \(NSM Procedure\) on page 35](#)
- [Configuring the Interface Profile \(NSM Procedure\) on page 36](#)
- [Configuring the Policy Decision Statistics Profile \(NSM Procedure\) on page 37](#)
- [Configuring the MIB Profile \(NSM Procedure\) on page 38](#)
- [Configuring the Routing Engine Profile \(NSM Procedure\) on page 39](#)

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 17 on page 34](#).
6. Click one:
 - **OK**—Saves the changes.

- **Cancel**—Cancels the modifications.

Table 17: 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 18 on page 35](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 18: 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 19 on page 36](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 19: 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 20 on page 37](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 20: 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 21 on page 38](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 21: 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 22 on page 39](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 22: 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 23 on page 40](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 23: 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.

Configuring Applications in J Series Services Routers and SRX Series Services Gateways

- [Configuring the Application and Application Set \(NSM Procedure\)](#) on page 41

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 24 on page 42](#).
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 24: 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 7

Configuring User Authentication in J Series Services Routers and SRX Series Services Gateways

- [Configuring RADIUS Authentication \(NSM Procedure\) on page 43](#)
- [Configuring TACACS+ Authentication \(NSM Procedure\) on page 44](#)
- [Configuring Authentication Order \(NSM Procedure\) on page 45](#)
- [Configuring User Access \(NSM Procedure\) on page 46](#)
- [Configuring Template Accounts \(NSM Procedure\) on page 49](#)

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 25 on page 44](#).
5. Click one:
 - **New**—Adds a new RADIUS server.
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 25: 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.
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 44](#)
- [Configuring Authentication Order \(NSM Procedure\) on page 45](#)
- [Configuring User Access \(NSM Procedure\) on page 46](#)

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 26 on page 44](#).
5. Click one:
 - **New**—Adds a new TACACS+ server.
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 26: 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.

Table 26: TACACS+ Authentication Configuration Details (*continued*)

Option	Function	Your Action
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.
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 43](#)
- [Configuring Authentication Order \(NSM Procedure\) on page 45](#)
- [Configuring User Access \(NSM Procedure\) on page 46](#)

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 43](#)
- [Configuring TACACS+ Authentication \(NSM Procedure\) on page 44](#)
- [Configuring User Access \(NSM Procedure\) on page 46](#)

Configuring User Access (NSM Procedure)

This section includes the following topics:

- [Configuring Login Classes on page 46](#)
- [Configuring User Accounts on page 48](#)

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 27 on page 46](#).
5. Click one:
 - **New**—Adds a new login class.
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Search**—Search a login class.

Table 27: 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 27: 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 27: 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 28 on page 48](#).
5. Click one:
 - **New**—Adds a new user account.
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Search**—Search the available login classes.

Table 28: 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 28: 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 43](#)
- [Configuring TACACS+ Authentication \(NSM Procedure\) on page 44](#)
- [Configuring Authentication Order \(NSM Procedure\) on page 45](#)

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 50](#)
- [Creating a Local Template Account on page 51](#)

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 29 on page 50](#).
5. Click one:
 - **New**—Creates a new remote template account.
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 29: 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 30 on page 51](#).
5. Click one:
 - **New**—Creates a new local template account.
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 30: 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 43](#)
- [Configuring TACACS+ Authentication \(NSM Procedure\) on page 44](#)
- [Configuring Authentication Order \(NSM Procedure\) on page 45](#)

CHAPTER 8

Configuring Chassis in J Series Services Routers and SRX Series Services Gateways

- [Configuring Aggregated Devices \(NSM Procedure\) on page 53](#)
- [Configuring Chassis Alarms \(NSM Procedure\) on page 54](#)
- [Configuring Chassis FPC \(NSM Procedure\) on page 55](#)
- [Configuring a T640 Router on a Routing Matrix \(NSM Procedure\) on page 60](#)
- [Configuring Routing Engine Redundancy \(NSM Procedure\) on page 65](#)
- [Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors \(NSM Procedure\) on page 66](#)

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 31 on page 54](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 31: 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 54](#)
- [Configuring a T640 Router on a Routing Matrix \(NSM Procedure\) on page 60](#)
- [Configuring Routing Engine Redundancy \(NSM Procedure\) on page 65](#)
- [Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors \(NSM Procedure\) on page 66](#)

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 32 on page 55](#).
5. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 32: 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 53](#)
- [Configuring Chassis FPC \(NSM Procedure\) on page 55](#)
- [Configuring Routing Engine Redundancy \(NSM Procedure\) on page 65](#)

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 33 on page 55](#).
5. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 33: 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 33: 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 33: 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 33: 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 33: 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 53](#)
- [Configuring Chassis Alarms \(NSM Procedure\) on page 54](#)
- [Configuring a T640 Router on a Routing Matrix \(NSM Procedure\) on page 60](#)

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 34 on page 60](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 34: 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 34: 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 34: 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 34: 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 34: 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 53](#)
- [Configuring Routing Engine Redundancy \(NSM Procedure\) on page 65](#)
- [Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors \(NSM Procedure\) on page 66](#)

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 35 on page 65](#).
5. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 35: 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 35: 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 53](#)
 - [Configuring a T640 Router on a Routing Matrix \(NSM Procedure\) on page 60](#)
 - [Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors \(NSM Procedure\) on page 66](#)

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 36 on page 66](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 36: 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 53](#)
 - [Configuring a T640 Router on a Routing Matrix \(NSM Procedure\) on page 60](#)
 - [Configuring Routing Engine Redundancy \(NSM Procedure\) on page 65](#)

CHAPTER 9

Configuring USB Modem Interfaces in J Series Services Routers and SRX Series Services Gateways

- [Configuring a USB Modem Interface \(NSM Procedure\) on page 67](#)
- [Configuring a Dialer Interface \(NSM Procedure\) on page 68](#)
- [Configuring Dial-in Options on a Dialer Interface \(NSM Procedure\) on page 69](#)
- [Configuring a CHAP Access Profile on a Dialer Interface \(NSM Procedure\) on page 70](#)

Configuring a USB Modem Interface (NSM Procedure)

To configure a USB modem interface for the device:

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 USB modem interface.
3. Click the **Configuration** tab. In the configuration tree, select **Interfaces > Interfaces List**.
4. Add or modify interface settings as specified in [Table 37 on page 67](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 37: USB Modem Interface Configuration Details

Option	Function	Your Action
Name	Specifies the name of the new interface.	Enter a name for the new interface.

Dialer Options > Pool

Table 37: USB Modem Interface Configuration Details (*continued*)

Option	Function	Your Action
Name	Specifies the name of the dialer pool configured on the dialer interface you want to use for USB modem connectivity.	Enter a name for the dialer pool.
Priority	Specifies the dialer pool priority.	Set the dialer pool priority.
Modem Options		
Init Command String	Configures the modem to automatically answer calls after a specified number of rings.	Enter the modem initialization command string. For example, enter ATSO=2 .

- Related Documentation**
- [Configuring a Dialer Interface \(NSM Procedure\) on page 68](#)
 - [Configuring Dial-in Options on a Dialer Interface \(NSM Procedure\) on page 69](#)

Configuring a Dialer Interface (NSM Procedure)

To configure a dialer interface for the device:

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 dialer interface.
3. Click the **Configuration** tab. In the configuration tree, select **Interfaces > Interfaces List**.
4. Add or modify interface settings as specified in [Table 38 on page 68](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 38: Dialer Interface Configuration Details

Option	Function	Your Action
Name	Specifies the name of the new interface.	Enter a name for the new interface.
Description	Differentiates between different dialer interfaces.	Enter a description for the new interface.
Encapsulation	Specifies the encapsulation.	Select PPP from the encapsulation list.

Table 38: Dialer Interface Configuration Details (*continued*)

Option	Function	Your Action
Unit		
Unit	Specifies the logical unit.	Enter the unit number.
Unit > Dialer Options		
Pool	Specifies the name of the dialer pool to use for USB modem connectivity.	Enter the name of the dialer pool.
Unit > Family > Inet > Address		
Name	Specifies the source IP address for the dialer interface.	Enter the source IP address.
Destination	Specifies the destination IP address for the dialer interface.	Enter the destination IP address.

Related Documentation

- [Configuring a USB Modem Interface \(NSM Procedure\) on page 67](#)
- [Configuring Dial-in Options on a Dialer Interface \(NSM Procedure\) on page 69](#)

Configuring Dial-in Options on a Dialer Interface (NSM Procedure)

To configure dial-in options on a dialer 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 dial-in options.
3. Click the **Configuration** tab. In the configuration tree, select **Interfaces > Interfaces List**.
4. Select the dialer interface and add or modify interface settings as specified in [Table 39 on page 69](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 39: Dialer Interface for Dial-in Configuration Details

Option	Function	Your Action
Unit > Dialer Options > Incoming Map		
Caller	Specifies the incoming map options for the dialer interface.	<ul style="list-style-type: none"> • Select accept-all to accept all incoming calls. • Select caller to accept calls from a specific caller ID.

Table 39: Dialer Interface for Dial-in Configuration Details (*continued*)

Option	Function	Your Action
Caller		
Name	Specifies the caller ID to be accepted on the dialer interface.	Enter the caller ID.

Related Documentation

- [Configuring a Dialer Interface \(NSM Procedure\) on page 68](#)
- [Configuring a USB Modem Interface \(NSM Procedure\) on page 67](#)

Configuring a CHAP Access Profile on a Dialer Interface (NSM Procedure)

To configure a CHAP access profile on a dialer 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 CHAP.
3. Click the **Configuration** tab. In the configuration tree, select **Access > Profile** to define a CHAP access profile.
4. Add or modify CHAP access settings as specified in [Table 40 on page 70](#).
5. Click the **Configuration** tab. In the configuration tree, select **Interfaces > Interfaces List** to configure CHAP on the dialer interface.
6. Select the appropriate dialer interface level, and add or modify interface settings as specified in [Table 41 on page 71](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 40: CHAP Access Profile Configuration Details

Option	Function	Your Action
Name	Specifies a name for the profile.	Enter a name for the profile.
Client		
Name	Specifies a name for the client.	Enter a name for the client.
Chap Secret	Specifies the CHAP secret.	Enter the CHAP secret. NOTE: Enter the client name and CHAP secret for each client to be included in the CHAP profile.

Table 41: CHAP Dialer Interface Configuration Details

Option	Function	Your Action
Unit		
Unit	Specifies the logical unit.	Enter the unit number.
Unit > Ppp Options > Chap		
Access profile	Specifies the profile name.	Enter a unique profile name containing a client list and access parameters.

**Related
Documentation**

- [Configuring a Dialer Interface \(NSM Procedure\) on page 68](#)
- [Configuring a USB Modem Interface \(NSM Procedure\) on page 67](#)

CHAPTER 10

Configuring Policy Options in J Series Services Routers and SRX Series Services Gateways

- [Configuring an AS Path Group in a BGP Routing Policy \(NSM Procedure\) on page 73](#)
- [Configuring a Community for use in BGP Routing Policy Conditions \(NSM Procedure\) on page 74](#)
- [Configuring a BGP Export Policy Condition \(NSM Procedure\) on page 75](#)
- [Configuring Flap Damping to Reduce the Number of BGP Update Messages \(NSM Procedure\) on page 76](#)
- [Configuring a Routing Policy Statement \(NSM Procedure\) on page 78](#)
- [Configuring Prefix List \(NSM Procedure\) on page 79](#)

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 42 on page 74](#).
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 42: 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 43 on page 75](#).
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 43: 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 44 on page 76](#).
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 44: 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 45 on page 77](#).
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 45: 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 46 on page 78](#).
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 46: 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 46: 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 47 on page 80](#).
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 47: 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.

CHAPTER 11

Configuring Routing Options in J Series Services Routers and SRX Series Services Gateways

- [Configuring Maximum Prefixes \(NSM Procedure\) on page 81](#)
- [Configuring Multicast \(NSM Procedure\) on page 83](#)
- [Configuring Multipath \(NSM Procedure\) on page 86](#)
- [Configuring Options \(NSM Procedure\) on page 87](#)
- [Configuring Route Resolution \(NSM Procedure\) on page 88](#)
- [Configuring Routing Table Groups \(NSM Procedure\) on page 89](#)
- [Configuring Routing Tables \(NSM Procedure\) on page 91](#)
- [Configuring Source Routing \(NSM Procedure\) on page 93](#)
- [Configuring Static Routes \(NSM Procedure\) on page 94](#)
- [Configuring Generated Routes \(NSM Procedure\) on page 95](#)
- [Configuring Graceful Restart \(NSM Procedure\) on page 96](#)
- [Configuring Forwarding Table \(NSM Procedure\) on page 97](#)
- [Configuring Flow Route \(NSM Procedure\) on page 99](#)
- [Configuring Fate Sharing \(NSM Procedure\) on page 101](#)
- [Configuring Martian Addresses \(NSM Procedure\) on page 102](#)
- [Configuring Interface Routes \(NSM Procedure\) on page 104](#)
- [Configuring Instance Export \(NSM Procedure\) on page 105](#)
- [Configuring Instance Import \(NSM Procedure\) on page 105](#)

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 48 on page 82](#).
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 48: 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 49 on page 83](#).
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 49: 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 49: 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 49: 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 49: 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 Multipath (NSM Procedure)

You can configure protocol-independent load balancing for Layer 3 virtual private networks (VPNs) with load sharing among multiple external BGP paths and multiple internal BGP paths. You can use forwarding next hops for both the active route and alternative paths for load balancing.

To configure multipath load balancing 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 **Multipath**.
6. Enter the parameters as specified in [Table 50 on page 87](#).
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 50: Configuring Multipath Fields

Option	Function	Your Action
Comment	Specifies the comment for the multipath configuration.	Enter the comment.
Vpn Unequal Cost	Applies protocol-independent load balancing to VPN routes.	<ol style="list-style-type: none"> 1. Expand the Multipath tree and select Vpn Unequal Cost. 2. Enter the comment for the vpn unequal cost configuration and specify whether both external and internal BGP paths should be selected for the multipath configuration by selecting the Equal External Internal check box.

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 51 on page 88](#).
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 51: 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 Route Resolution (NSM Procedure)

You can configure a routing table to accept routes from specific routing tables to enable the device to manage and route the traffic effectively between a source host and destination host. You can configure a routing table to use specific import policies to produce a route resolution table to resolve routes.

To configure a route resolution 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 **Resolution**.
6. Add or modify the parameters as specified in [Table 52 on page 89](#).
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 52: Route Resolution Fields

Option	Function	Your Action
Comment	Specifies the comment for the route resolution.	Enter a comment.
Rib	Specifies the name of the routing table for which the import policies and the resolution routes are configured.	<ol style="list-style-type: none"> 1. Expand the Resolution tree and select Rib. 2. Click the New button or select a routing table and click the Edit button. 3. Enter the name and comment for the routing table and specify the route import policies and the resolution routes.
Tracefilter	Specifies the filter policy for the resolution routes.	<ol style="list-style-type: none"> 1. Expand the Resolution tree and select Tracefilter. 2. Specify the filter policies for the routing table.
Traceoptions	Defines tracing options for route resolution.	<ol style="list-style-type: none"> 1. Expand the Resolution tree and select Traceoptions. 2. Expand the Traceoptions tree and set up the file and flag parameters.

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 53 on page 90](#).
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 53: 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.

Table 53: Rib Group Fields (*continued*)

Option	Function	Your Action
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 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 54 on page 92](#).
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 54: 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 54: 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 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 55 on page 93](#).
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 55: Source Routing Fields

Option	Function	Your Action
Comment	Specifies the comment for the source routing configuration.	Enter the comment.

Table 55: Source Routing Fields (*continued*)

Option	Function	Your Action
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 56 on page 95](#).
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 56: 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 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 57 on page 96](#).
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 57: 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 Graceful Restart (NSM Procedure)

Graceful restart allows a device undergoing a restart to inform its adjacent neighbors and peers of its condition. The restarting device requests a grace period from the neighbor or peer, which can then cooperate with the restarting device. With a graceful restart, the restarting device can still forward traffic during the restart period, and convergence in the network is not disrupted. The restart is not visible to the rest of the network, and the restarting device is not removed from the network topology.

The graceful restart request occurs only if the following conditions are met:

- The network topology is stable.
- The neighbor or peer cooperates.
- The restarting device is not already cooperating with another restart already in progress.
- The grace period does not expire.

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. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Graceful Restart**.
6. Enter the parameters as specified in [Table 58 on page 97](#).
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 58: Graceful Restart Fields

Option	Function	Your Action
Comment	Specifies the comment for the graceful restart.	Enter a comment.
Disable	Specifies whether graceful restart is enabled for the device.	<ul style="list-style-type: none"> • Select the check box to disable graceful restart. • Clear the check box to enable graceful restart.
Restart Duration	Specifies the duration of the grace period for the device to restart.	Enter a value for the duration or select a value from the list.

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 59 on page 98](#).
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 59: 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 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 60 on page 99](#).
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 60: Flow Route Fields

Option	Function	Your Action
Comment	Specifies the comment for the flow route.	Enter a comment.
Route		

Table 60: Flow Route Fields (*continued*)

Option	Function	Your Action
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	<p>Specifies the conditions that the packet must match for the packet to be included in flow route. Match conditions are:</p> <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.
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 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 61 on page 101](#).
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 61: Fate Sharing Fields

Option	Function	Your Action
Comment	Specifies the comment for the fate sharing.	Enter a comment.
Group		

Table 61: Fate Sharing Fields (*continued*)

Option	Function	Your Action
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.
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 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 62 on page 103](#).
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 62: 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 • Or longer • 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 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 63 on page 104](#).
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 63: Interface Routes Fields

Option	Function	Your Action
Comment	Specifies the comment for the interface route.	Enter a comment.
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.

Table 63: Interface Routes Fields (*continued*)

Option	Function	Your Action
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 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.

CHAPTER 12

Configuring Protocols for J Series Services Routers and SRX Series Services Gateways

- [Configuring BGP \(NSM Procedure\) on page 107](#)
- [Configuring 802.1X Authentication \(NSM Procedure\) on page 110](#)
- [Configuring GVRP \(NSM Procedure\) on page 112](#)
- [Configuring IGMP \(NSM Procedure\) on page 113](#)
- [Configuring MPLS \(NSM Procedure\) on page 115](#)
- [Configuring MSDP \(NSM Procedure\) on page 144](#)
- [Configuring MSTP \(NSM Procedure\) on page 154](#)
- [Configuring OSPF \(NSM Procedure\) on page 156](#)
- [Configuring RIP \(NSM Procedure\) on page 160](#)
- [Configuring RIPng \(NSM Procedure\) on page 162](#)
- [Configuring Router Advertisement \(NSM Procedure\) on page 168](#)
- [Configuring Router Discovery \(NSM Procedure\) on page 171](#)
- [Configuring VSTP \(NSM Procedure\) on page 173](#)
- [Configuring VRRP \(NSM Procedure\) on page 175](#)

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 64 on page 108](#).
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 64: 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 64: 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 64: 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 802.1X Authentication (NSM Procedure)

IEEE 802.1X authentication provides network edge security, protecting Ethernet LANs from denial-of-service (DoS) attacks and preventing unauthorized user access.

802.1X works by using an *Authenticator Port Access Entity* (the device) to block all traffic to and from a supplicant (client) at the interface until the supplicant's credentials are presented and matched on the *Authentication server* (a RADIUS server). When authenticated, the switch stops blocking and opens the interface to the supplicant.

To configure 802.1X authentication:

- Specify 802.1X interface settings on the switch.
 - Specify the 802.1X exclusion list, used to specify which supplicants can bypass 802.1X authentication and be automatically connected to the LAN.
1. [Configuring 802.1X Interface Settings on page 111](#)
 2. [Configuring Static MAC Bypass on page 112](#)

Configuring 802.1X Interface Settings

To configure 802.1X interface settings:

1. In the navigation tree, select **Device Manager > Devices**. In Device Manager, select the device for which you want to configure 802.1X settings.
2. In the Configuration tree, expand **Protocols > Dot1x**.
4. Select **Authenticator > Interface**.
5. Click the Add icon.
6. Add/modify member settings for the interface as specified in [Table 65 on page 111](#).



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 65: 802/1X Authentication for an Interface

Option	Function	Your Action
Authentication Profile Name	Specifies the name for the profile.	Enter the name
Interface	Specifies the interface for which 802.1X authentication is being configured.	Select Interface . Click the Add icon.
Name	Specifies the interface name.	Enter the interface name.
Disable	Disables 802.1X authentication on the interface.	Select to disable authentication.
Supplicant	Specifies the mode to be adopted for supplicants: <ul style="list-style-type: none"> • Single — allows only one host for authentication. • Multiple — allows multiple hosts for authentication. Each host is checked before being admitted to the network. • Single authentication for multiple hosts — Allows multiple hosts but only the first is authenticated. 	Select the required mode.
Retries	Maximum number of retries	Select a value from the list.
Quiet Period	Specifies the port waiting time after an authentication failure.	Select a value from the list.
Transmit Period	Specifies the retransmit interval.	Select a value from the list.
Supplicant Timeout	Port timeout value for the response from the supplicant.	Select a value from the list.

Table 65: 802.1X Authentication for an Interface (*continued*)

Option	Function	Your Action
Server Timeout	Port timeout value for the response from the RADIUS server	Select a value from the list.
Maximum Requests	Specifies the maximum number of authentication requests to be made to the server.	Select a value from the list.
Guest Vlan	Specifies the guest VLAN to move the interface to in case of an authentication failure.	Enter the VLAN name.
Reauthentication	Specifies enabling reauthentication on the selected interface.	Select Reauthentication . Select one: <ul style="list-style-type: none"> • none • reauthentication • no-reauthentication

Configuring Static MAC Bypass

Configure any MAC addresses, supplicants, or interfaces to be excluded from 802.1X authentication—that is, they will be authenticated.

To configure the 802.1X exclusion:

1. Specify a MAC address to be excluded from 802.1X authentication in the field **Name**.
2. Specify the interface for the supplicant to bypass authentication if connected through that interface.
3. Specify the VLAN to move the supplicant to once it is authenticated.



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.

Configuring GVRP (NSM Procedure)

As a network expands and the number of clients and VLANs increases, VLAN administration becomes complex, and the task of efficiently configuring VLANs on multiple switches becomes increasingly difficult. To automate VLAN administration, you can enable GARP VLAN Registration Protocol (GVRP) on the network.

GVRP learns VLANs on a particular 802.1Q trunk port, and adds the corresponding trunk port to the VLAN if the advertised VLAN is preconfigured or existing already on the switch. For example, a VLAN named “sales” is advertised to trunk port 1 on the GVRP-enabled device. The device adds trunk port 1 to the sales VLAN if the sales VLAN already exists on the switch.

As individual ports become active and send a request to join a VLAN, the VLAN configuration is updated and propagated among the switches. Limiting the VLAN configuration to active participants reduces the network overhead. GVRP also provides the benefit of pruning VLANs to limit the scope of broadcast, unknown unicast, and multicast (BUM) traffic to interested devices only.

To configure GVRP:

1. In the navigation tree, select **Device Manager > Devices**. In Device Manager, select the device.
2. In the configuration tree, expand **Protocols**.
3. Select **GVRP**.
4. Click the Add icon.
5. Add/modify GVRP settings for the interface as specified in [Table 66 on page 113](#).



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 66: GVRP Configuration Fields

Option	Function	Your Action
Disable	Select this option to disable GVRP on the interface.	Click to select.
Join Timer	Specifies the maximum number of milliseconds the interfaces wait before sending VLAN advertisements.	Select a value.
Leave Times	Specifies the number of milliseconds an interface must wait after receiving a leave message to remove the interface from the VLAN specified in the message.	Select a value.
Leaveall Times	Specifies the interval at which Leave All messages are sent on interfaces. Leave All messages help to maintain current GVRP VLAN membership information in the network.	Select a value.

Configuring IGMP (NSM Procedure)

Internet Group Management Protocol (IGMP) is an Internet protocol that provides a way for an IP host to report its multicast group membership to adjacent devices. This feature enables you to associate the IGMP with an interface and allocate it to a multicast group.

To configure IGMP 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 **IGMP**.
5. Add/Modify the parameters as specified in [Table 67 on page 114](#).
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 67: IGMP Configuration Fields

Option	Function	Your Action
IGMP		
Comment	Specifies the comment for IGMP.	Enter a comment.
Query Interval	Defines how often the device sends general host-query messages. .	Select the query interval.
Query Response Interval	Defines how long the query router/switch waits to receive a response to a host-query message from a host.	Enter the query response interval.
Query Last Member Interval	Defines how often the device sends group-specific query messages.	Enter the query last member interval.
Robust Count	Defines the number of intervals the device waits before removing a multicast group from the multicast forwarding table.	Select the robust count.
Accounting	Specifies whether accounting is enabled for IGMP.	Select to enable accounting.

Table 67: IGMP Configuration Fields (*continued*)

Option	Function	Your Action
Interfaces	Specifies the interface and the multicast group that has to be associated with IGMP.	<ol style="list-style-type: none"> 1. Expand the IGMP tree and select Interfaces. 2. Click the New button or select an interface and click Edit button. 3. Select Disable to disable IGMP on the interface. 4. Select the version. 5. Specify the Ssm Map. 6. You can enable Immediate Leave and Promiscuous Mode. 7. You can enable accounting on the interface. 8. Select the option Interface > Static to configure the multicast group to be associated with the interface.
Traceoptions	Defines trace options for IGMP .	<ol style="list-style-type: none"> 1. Expand IGMP tree and select Traceoptions. 2. Enter a comment for traceoptions. 3. Expand the Traceoptions tree, select File and set up the file parameters. 4. In the Traceoptions tree select Flag and set up or edit the file parameters.

Configuring MPLS (NSM Procedure)

- [Configuring MPLS \(NSM Procedure\) on page 116](#)
- [Configuring Auto Policing \(NSM Procedure\) on page 118](#)
- [Configuring Bandwidth \(NSM Procedure\) on page 119](#)
- [Configuring Differentiated Services Traffic Engineering \(NSM Procedure\) on page 119](#)
- [Configuring Interfaces \(NSM Procedure\) on page 120](#)
- [Configuring Label Switched Path \(NSM Procedure\) on page 122](#)
- [Configuring Log Updown \(NSM Procedure\) on page 133](#)
- [Configuring OAM \(NSM Procedure\) on page 134](#)
- [Configuring Path \(NSM Procedure\) on page 137](#)
- [Configuring Path MTU \(NSM Procedure\) on page 138](#)
- [Configuring Static Label Switched Path \(NSM Procedure\) on page 139](#)
- [Configuring Statistics \(NSM Procedure\) on page 142](#)
- [Configuring Traceoptions \(NSM Procedure\) on page 143](#)

Configuring MPLS (NSM Procedure)

You can configure an MPLS protocol.

To configure MPLS:

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 MPLS.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls**.
4. Click + to configure MPLS options as described in [Table 68 on page 116](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the MPLS parameters.

Table 68: MPLS Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the MPLS protocol.	(Optional) Enter a comment.
Disable	Specifies that MPLS can be disabled.	Select the check box to enable this feature.
Traffic Engineering	Specifies the protocols to perform traffic engineering.	Select an option from the list.
Advertisement Hold Time	Specifies the time that an LSP down message will be delayed.	Set the advertisement hold time. Range: 0 through 65535.
Rsvp Error Hold Time	Specifies the time that the Resource Reservation Protocol (RSVP) path error will be remembered.	Set the RSVP path error hold time. Range: 0 through 240.
Optimize Aggressive	Specifies that an aggressive optimization algorithm can be run based on the Interior Gateway Protocol (IGP) metric only.	Select the check box to enable this feature.
Smart Optimize Timer	Specifies the path optimization interval link for when a link traversed by the path goes down. NOTE: When a link fails and traffic is moved to an alternate path, the smart optimize timer waits for the specified period of time and then switches the traffic back to the original path (if that path is back up). If the original path fails again, the traffic is shifted to an alternate path and the smart optimization timer is disabled for one hour.	Set the smart optimize timer value. Range: 0 through 65535.

Table 68: MPLS Configuration Details (*continued*)

Option	Function	Your Action
No Propagate Ttl	Specifies the time-to-live (TTL) propagation from IP to MPLS (on push) and MPLS to IP (on pop).	Select the check box to enable this feature.
Explicit Null	Specifies that the EXPLICIT_NULL label can be advertised when the device is the egress.	Select the check box to enable this feature.
Ipv6 Tunneling	Specifies that the MPLS label-switched-paths to be used for tunneling IPv6 traffic are allowed.	Select the check box to enable this feature.
Icmp Tunneling	Specifies that the MPLS label-switched-paths to be used for tunneling Internet Control Message Protocol (ICMP) error packets are allowed.	Select the check box to enable this feature.
Revert Timer	Specifies the range within which you can revert to the primary path.	Set the revert time. Range: 0 through 65535.
Expand Loose Hop	Specifies use of Constraint Shortest Path First (CSPF) path computation to expand loose hops.	Select the check box to enable this feature.
Class Of Service	Specifies the class-of-service value.	Set the class-of-service value. Range: 0 through 7.
No Decrement Ttl	Specifies that you cannot decrement the TTL within an LSP.	Select the check box to enable this feature.
Hop Limit	Specifies the maximum number of device hops allowed.	Set the maximum number of device hops. Range: 2 through 255.
No Cspf	Specifies that you can disable automatic path computation.	Select the check box to enable this feature.
Admin Down	Specifies that you can set Generalized Multi-Protocol Label Switching (GMPLS) label-switched-path to the administratively down state.	Select the check box to enable this feature.
Optimize Timer	Specifies the periodical path reoptimization.	Set the reoptimization time. Range: 0 through 65535.
Preference	Specifies the preference value.	Set the preference value. Range: 0 through 4,294,967,295.
record / no-record	Specifies whether an LSP should actively record the routes in the path or not.	Select the option.

Table 68: MPLS Configuration Details (*continued*)

Option	Function	Your Action
Standby	Specifies whether to keep backup paths in continuous standby mode.	Select the check box to enable this feature.

Related Documentation

- [Configuring an Admin Group \(NSM Procedure\) on page 124](#)
- [Configuring Auto Policing \(NSM Procedure\) on page 118](#)
- [Configuring Bandwidth \(NSM Procedure\) on page 119](#)

Configuring Auto Policing (NSM Procedure)

You can enable the automatic policing of all the MPLS layered service providers on the device or logical system.

To configure automatic policing:

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 automatic policing.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls > Auto Policing**.
4. Enter a descriptive comment for the automatic policing in **Comment**.
5. In the configuration tree, select **Protocols > Mpls > Auto Policing > Class**.
6. Click + to configure automatic policing as described in [Table 69 on page 118](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the automatic policing parameters.

Table 69: Auto Policing Configuration Details

Option	Function	Your Action
Name	Specifies the automatic policing class name.	Enter an automatic policing class name.
Comment	Supplies a descriptive comment for the automatic policing class.	(Optional) Enter a comment.
drop	Specifies all the packets to be dropped.	Select the option.
loss-priority-high	Specifies that a packet has high loss priority.	Select the option.
loss-priority-low	Specifies that a packet has low loss priority.	Select the option.

- Related Documentation**
- [Configuring Bandwidth \(NSM Procedure\) on page 119](#)
 - [Configuring Differentiated Services Traffic Engineering \(NSM Procedure\) on page 119](#)
 - [Configuring an Admin Group \(NSM Procedure\) on page 124](#)

Configuring Bandwidth (NSM Procedure)

You can set bandwidth constraints.

To configure bandwidth requirements:

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 bandwidth requirements.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls > Bandwidth**.
4. Add or modify settings as described in [Table 70 on page 119](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the bandwidth parameters.

Table 70: Bandwidth Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the bandwidth.	(Optional) Enter a comment.
Per Traffic Class Bandwidth	Specifies the bandwidth for reserving a traffic class.	Enter the bandwidth for reserving a traffic class.
Ct0	Specifies the bandwidth for traffic class 0.	Enter a bandwidth.
Ct1	Specifies the bandwidth for traffic class 1.	Enter a bandwidth.
Ct2	Specifies the bandwidth for traffic class 2.	Enter a bandwidth.
Ct3	Specifies the bandwidth for traffic class 3.	Enter a bandwidth.

- Related Documentation**
- [Configuring an Admin Group \(NSM Procedure\) on page 124](#)
 - [Configuring MPLS \(NSM Procedure\) on page 116](#)

Configuring Differentiated Services Traffic Engineering (NSM Procedure)

You can configure Differentiated Services (DiffServ) traffic engineering.

To configure differentiated services traffic engineering:

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 differentiated services traffic engineering.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls > Diffserv Te**.
4. Enter a descriptive comment for the differentiated services traffic engineering in **Comment**.
5. Select the supported bandwidth constraint model in **Bandwidth Model**.
6. In the configuration tree, select **Protocols > Mpls > Diffserv Te > Te Class Matrix**.
7. Enter a descriptive comment for the traffic engineering class matrix in **Comment**.
8. Add or modify the traffic engineering class matrix for a multiclass layered service provider or a differentiated services-aware traffic engineering layered service provider as described in [Table 71 on page 120](#).
9. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the differentiated services traffic engineering parameters.

Table 71: Traffic Engineering Configuration Details

Option	Function	Your Action
Te0 / Te1 / Te2 / Te3 / Te4 / Te5 / Te6 / Te7		
Comment	Supplies a descriptive comment for the traffic engineering.	(Optional) Enter a comment.
Traffic Class	Specifies the traffic class.	Select the traffic class from the list.
Priority	Specifies the preemption priority for the selected traffic class.	Set the preemption priority for the traffic class. Range: 0 through 7.

- Related Documentation**
- [Configuring Interfaces \(NSM Procedure\) on page 120](#)
 - [Configuring Bandwidth \(NSM Procedure\) on page 119](#)
 - [Configuring Auto Policing \(NSM Procedure\) on page 118](#)

Configuring Interfaces (NSM Procedure)

You can configure information about MPLS-enabled interfaces.

To configure interfaces:

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 interfaces.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls > Interface**.
4. Click + to configure an MPLS-enabled interface feature.
5. Add or modify settings as described in [Table 72 on page 121](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the interface parameters.

Table 72: Interface Configuration Details

Option	Function	Your Action
Name	Specifies the interface name.	Enter a name for the interface.
Comment	Supplies a descriptive comment for the interface.	(Optional) Enter a comment.
Disable	Specifies that you can disable MPLS on this interface.	Select the check box to enable this feature.
Always Mark Connection Protection Tlv	Allows you to switch a layered service provider away from a network node using a bypass layered service provider.	Select the check box to enable this feature.
Switch Away Lsps	Allows you to switch away protected layered service providers to their bypass layered service providers.	Select the check box to disable layered service providers.
Protocols > Mpls > Interface > Admin Group		
New admin-group	Specifies the new administrative group name.	Enter a new administrative group name.
Protocols > Mpls > Interface > Static		
Comment	Supplies a descriptive comment for the static interface.	(Optional) Enter a comment.
Protection Revert Time	Specifies the amount of time that a static layered service provider must wait before traffic reverts from the bypass path to the original path.	Set the protection revert time. Range: 0 through 65535.

Related Documentation

- [Configuring Auto Policing \(NSM Procedure\) on page 118](#)
- [Configuring Differentiated Services Traffic Engineering \(NSM Procedure\) on page 119](#)
- [Configuring Label Switched Path \(NSM Procedure\) on page 122](#)

Configuring Label Switched Path (NSM Procedure)

You can configure a label-switched path to use in a dynamic MPLS.

To configure label-switched paths:

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 label-switched paths.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls > Label Switched Path**.
4. Click + to configure label-switched paths.
5. Add or modify settings as described in [Table 73 on page 122](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the label-switched path parameters.

Table 73: Label-Switched Path Configuration Details

Option	Function	Your Action
Name	Specifies the path name.	Enter a path name.
Comment	Supplies a descriptive comment for the label-switched path.	(Optional) Enter a comment.
Disable	Specifies that you can disable MPLS label-switched path.	Select the check box to enable this feature.
No Install to Address	Specifies that you cannot install host route to address into the routing tables.	Select the check box to enable this feature.
Backup	Specifies to use a label-switched path for Interior Gateway Protocol (IGP) backup.	Select the check box to enable this feature.
From	Specifies the address of an ingress device.	Enter the address of an ingress device.
Metric	Specifies a metric value.	Set the metric value. Range: 1 through 16777215.
Ldp Tunneling	Specifies that the LDP is allowed to use this a label-switched path for tunneling.	Select the check box to enable this feature.
Soft Preemption	Specifies to attempt make-before-break service while preempting this a label-switched path.	Select the check box to enable this feature.

Table 73: Label-Switched Path Configuration Details (*continued*)

Option	Function	Your Action
Retry Timer	Specifies the time before retrying the primary path.	Set the retry timer. Range: 1 through 600.
Retry Limit	Specifies the maximum number of times to retry the primary path.	Set the retry limit. Range: 0 through 10000.
Revert Timer	Specifies the hold-down window before reverting to the primary path.	Set the revert timer. Range: 0 through 65535.
Class of Service	Specifies the class-of-service value.	Set the class-of-service value. Range: 0 through 7.
No Decrement Ttl	Specifies that you cannot decrement the time to live (TTL) within a label-switched path.	Select the check box to enable this feature.
Hop Limit	Specifies the maximum allowed device hops.	Set the hop limit. Range: 2 through 255.
No Cspf	Specifies that the Constrained Shortest Path First (CSPF) path computation is disabled.	Select the check box to enable this feature.
Admin Down	Specifies that the Generalized MPLS label-switched path is set to the administratively down state.	Select the check box to enable this feature.
Optimize Timer	Specifies the periodical path reoptimizations.	Set the periodical path reoptimization value. Range: 0 through 65535.
Preference	Specifies the preference value.	Set the preference value. Range: 0 through 4,294,967,295.
record / no-record	Specifies whether a label-switched path should actively record the routes in the path or not.	Select one option.
Standby	Specifies that the path remains up at all times to provide instant switchover if connectivity problems occur.	Select the check box to enable this feature.
random / least-fill / most-fill	Specifies the preferred path when several equal-cost candidate paths to a destination exist, and prefers the path with the highest available bandwidth (with the largest minimum available bandwidth ratio).	Select an option.
Description	Specifies the description for the label switch.	Enter a description.

Table 73: Label-Switched Path Configuration Details (*continued*)

Option	Function	Your Action
link-protection	Specifies that you can enable link protection on the specified label-switched path.	Select the option.
node-link-protection	Specifies that you can enable link protection on the specified interface.	Select the option.
Inter Domain	Specifies the interdomain label-switched path.	Select the check box to enable this feature.
Adaptive	Specifies that the label-switched path can smoothly cut over to the new routes.	Select the check box to enable this feature.
Associate Backup Pe Groups	Specifies that you can associate this label-switched path with backup-pe groups.	Select the check box to enable this feature.
Egress Protection	Specifies that you can use this label-switched path for egress protection data transport.	Select the check box to enable this feature.

Configuring Label-Switched Path includes the following topics:

- [Configuring an Admin Group \(NSM Procedure\) on page 124](#)
- [Configuring Auto Bandwidth \(NSM Procedure\) on page 125](#)
- [Configuring Fast Reroute \(NSM Procedure\) on page 126](#)
- [Configuring Install \(NSM Procedure\) on page 127](#)
- [Configuring P2MP \(NSM Procedure\) on page 128](#)
- [Configuring Policing \(NSM Procedure\) on page 128](#)
- [Configuring Primary \(NSM Procedure\) on page 129](#)
- [Configuring Priority \(NSM Procedure\) on page 131](#)
- [Configuring Secondary \(NSM Procedure\) on page 131](#)
- [Configuring Traceoptions \(NSM Procedure\) on page 132](#)

[Configuring an Admin Group \(NSM Procedure\)](#)

You can configure an administrative group for MPLS.

To configure an administrative group:

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 an administrative group.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls > Admin Group**.
4. Enter a descriptive comment for the administrative group in **Comment**.

5. An administrative group is typically named with a color and a numeric value, and is applied to the MPLS interface for the appropriate links. You can enter links in **Exclude**, or **Include All**, or **Include Any**.
6. To configure administrative groups, in the configuration tree, select **Protocols > Mpls > Admin Groups**.
7. Click + to configure administrative groups as described in [Table 74 on page 125](#).
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the administrative group and administrative groups parameters.

Table 74: Admin Groups Configuration Details

Option	Function	Your Action
Name	Specifies the name for the administrative groups.	Enter the name for the administrative groups.
Comment	Supplies a descriptive comment for the administrative groups.	(Optional) Enter a comment.
Group Value	Specifies the group bit position.	Set the group value. Range: 0 through 31.

Configuring Auto Bandwidth (NSM Procedure)

To configure automatic bandwidth:

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 an automatic bandwidth.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls > Label Switched Path > Auto Bandwidth**.
4. Select the **Enable Feature** check box to configure automatic bandwidth.
5. Add or modify settings as described in [Table 75 on page 126](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the automatic bandwidth parameters.

Table 75: Auto Bandwidth Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the automatic bandwidth.	(Optional) Enter a comment.
Adjust Interval	Specifies the time interval for adjusting the label-switched path bandwidth.	Set the adjust interval time. Range: 300 through 4,294,967,295.
Adjust Threshold	Specifies the change in average label-switched path utilization to trigger automatic adjustment.	Set the adjust threshold value. Range: 0 through 50.
Minimum Bandwidth	Specifies the minimum label-switched path bandwidth.	Enter the minimum label-switched path bandwidth.
Maximum Bandwidth	Specifies the maximum label-switched path bandwidth.	Enter the maximum label-switched path bandwidth.
Monitor Bandwidth	Specifies that you can monitor label-switched path bandwidth without adjustments.	Select the check box to enable this feature.
Adjust Threshold Overflow Limit	Specifies the number of consecutive overflow samples to trigger automatic adjustment.	Set the adjust threshold overflow limit. Range: 1 through 65535.

Configuring Fast Reroute (NSM Procedure)

To configure a fast reroute:

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 fast reroute.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls > Label Switched Path > Fast Reroute**.
4. Enter a descriptive comment for the reroute in **Comment**.
5. Set the maximum allowed hop routes in **Hop Limit**.
6. Add or modify settings as described in [Table 76 on page 127](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the fast reroute parameters.

Table 76: Fast Reroute Configuration Details

Option	Function	Your Action
label-switched-path > Fast Reroute > Bandwidth		
bandwidth	Specifies the bandwidth for the reroute path.	Select the option.
bandwidth-percent	Specifies the percentage of bandwidth to reserve for the detour path in case the primary path fails for a traffic engineered label-switched path or a multiclass label-switched path.	Select the option.
label-switched-path > Fast Reroute > Exclude		
exclude	Specifies the administrative groups to exclude for a label-switched path of a primary path or a secondary path.	Enter an administrative group name to exclude for a label-switched path of a primary path or a secondary path.
no-exclude	Specifies the administrative groups to exclude for a fast reroute.	Select the option.
label-switched-path > Fast Reroute > Include All		
include-all	Specifies that the label-switched path is required to traverse links that include all the defined administrative groups.	Select the option and enter the administrative group name.
no-include-all	Specifies that you can disable administrative group inclusion.	Select the option.
label-switched-path > Fast Reroute > Include Any		
include-any	Specifies that you can define any administrative group to include for a label-switched path of a primary path and a secondary path.	Select the option.
no-include-any	Specifies that you can disable any administrative group inclusion.	Select the option.

Configuring Install (NSM Procedure)

To configure an install:

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 an install.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls > Label Switched Path > Install**.
4. Enter a name for the install in **Name**.
5. Enter a descriptive comment for the install in **Comment**.

6. Select the **Active** check box to install a prefix into the forwarding table.
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the install parameters.

Configuring P2MP (NSM Procedure)

You can configure a Point-to-Multipoint (P2MP) label-switched path.

To configure a P2MP label-switched path:

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 P2MP label-switched path.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls > Label Switched Path > P2mp**.
4. Select the check box to enable the feature in **Enable Feature**.
5. Enter a descriptive comment for the P2MP label-switched path in **Comment**.
6. Enter a name for the P2MP label-switched path in **Path_name**.
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the P2MP parameters.

Configuring Policing (NSM Procedure)

You can configure policing (also known as rate limiting) to limit the amount of traffic that passes into or out of an interface.

To configure policing:

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 policing.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls > Label Switched Path > Policing**.
4. Enter a descriptive comment for the policing in **Comment**.
5. Select the name of the filter used for policing the label-switched path traffic in **Filter**.

6. Enable the check box to turn off automatic policing for this label-switched path in **No Auto Policing**.
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the policing parameters.

Configuring Primary (NSM Procedure)

You can configure the primary path to use for a label-switched path.

To configure a primary label-switched path:

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 primary label-switched path.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls > Label Switched Path > Primary**.
4. Click + to configure the primary label-switched path.
5. Add or modify settings as described in [Table 77 on page 129](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the primary parameters.

Table 77: Primary LSP Configuration Details

Option	Function	Your Action
Name	Specifies the name of the primary path.	Enter a primary path name.
Comment	Supplies a descriptive comment for the primary path label-switched path.	(Optional) Enter a comment.
Class of Service	Specifies the class-of-service value.	Set the class-of-service value. Range: 0 through 7.
No Decrement Ttl	Specifies that you cannot decrement the TTL within a label-switched path.	Select the check box to enable this feature.
Hop Limit	Specifies the maximum allowed device hops.	Set the maximum allowed device hops. Range: 2 through 255.

Table 77: Primary LSP Configuration Details (*continued*)

Option	Function	Your Action
No Cspf	Specifies that the automatic path computation is disabled.	Select the check box to enable this feature.
Admin Down	Specifies that the Generalized MPLS (GMPLS) label-switched path is set to administrative down state.	Select the check box to enable this feature.
Optimize Timer	Specifies the periodical path reoptimization.	Set the periodical path reoptimization value. Range: 0 through 65535.
Preference	Specifies the preference value.	Set the preference value. Range: 0 through 4,294,967,295.
record / no-record	Specifies whether a label-switched path should actively record the routes in the path or not.	Select one option.
Standby	Specifies that the path remains up at all times to provide instant switchover if connectivity problems occur.	Select the check box to enable this feature.
Adaptive	Specifies that the Resource Reservation Protocol (RSVP) uses the shared explicit (SE) reservation styles and assists in smooth transition during rerouting.	Select the check box to enable this feature.
Select	Specifies a way of selection. You cannot specify both options.	Select an option from the list.
label-switched-path > Primary > Admin Group		
To configure an administrative group, see “Configuring an Admin Group (NSM Procedure)” on page 124.		
label-switched-path > Primary > Bandwidth		
To configure a bandwidth, see “Configuring Bandwidth (NSM Procedure)” on page 119.		
label-switched-path > Primary > Oam		
label-switched-path > Primary > Priority		
Enable Feature	Specifies that you can configure the priority settings.	Select the check box to enable this feature.
Comment	Supplies a descriptive comment for the priority settings.	(Optional) Enter a comment.

Table 77: Primary LSP Configuration Details (*continued*)

Option	Function	Your Action
Setup Priority	Specifies the setup priority that is set.	Set the setup priority value. Range: 0 through 7.
Reservation Priority	Specifies the reservation priority which is used to keep a reservation after it has been set up.	Set the reservation priority value. Range: 0 through 7.

Configuring Priority (NSM Procedure)

When there is insufficient bandwidth to establish a more important label-switched path, you might want to tear down a less important existing label-switched path to free the bandwidth, by setting priorities.

To configure a priority:

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 priority.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls > Label Switched Path > Priority**.
4. Select the check box to configure priority in **Enable Feature**.
5. Enter a descriptive comment for the priority setting in **Comment**.
6. Specify whether a new label-switched path that preempts an existing label-switched path needs to be established in **Setup Priority**. Range: 0 through 7.
7. Specify the degree to which a label-switched path holds onto its session reservation after the label-switched path has been set up successfully in **Reservation Priority**. Range: 0 through 7.
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the priority parameters.

Configuring Secondary (NSM Procedure)

You can configure a secondary path to use for a label-switched path.

To configure a secondary label-switched path:

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 secondary label-switched path.

3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls > Label Switched Path > Secondary**.
4. Click + to configure the secondary label-switched path.
5. To configure administrative groups, see “[Configuring an Admin Group \(NSM Procedure\)](#)” on page 124.
6. To configure bandwidth, see “[Configuring Bandwidth \(NSM Procedure\)](#)” on page 119.
7. To configure priority, see “[Configuring Priority \(NSM Procedure\)](#)” on page 131.
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the secondary parameters.

Configuring Traceoptions (NSM Procedure)

You can configure 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 traceoptions.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls > Label Switched Path > Traceoptions**.
4. Enter a descriptive comment for the traceoption.
5. Add or modify settings as described in [Table 78 on page 132](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the traceoption parameters.

Table 78: Traceoptions Configuration Details

Option	Function	Your Action
label-switched-path > Traceoptions > File		
Comment	Supplies a descriptive comment for the file traceoption.	(Optional) Enter a comment.
Filename	Specifies the name of the file in which to write the trace information.	Enter the filename.
Size	Specifies the maximum trace file size.	Enter the trace file size.

Table 78: Traceoptions Configuration Details (*continued*)

Option	Function	Your Action
Files	Specifies the maximum number of trace files.	Set the maximum number of trace files. Range: 2 through 1000.
world-readable	Specifies unrestricted file access.	Select the option.
no-world-readable	Specifies that file access is restricted to the owner only.	Select the option.
label-switched-path > Traceoptions > Flag		
Name	Specifies the flag name.	Enter a flag name.
Comment	Supplies a descriptive comment for the flag traceoption.	(Optional) Enter a comment.

- Related Documentation**
- [Configuring Interfaces \(NSM Procedure\) on page 120](#)
 - [Configuring MPLS \(NSM Procedure\) on page 116](#)

Configuring Log Updown (NSM Procedure)

You can log a message whenever a BGP peer makes a state transition.

To configure log updown:

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 log updown.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls > Log Updown**.
4. Click + to configure log updown as described in [Table 79 on page 134](#).
5. Select **Protocols > Mpls > Log Updown > Trap**.
6. Configure settings as described in [Table 79 on page 134](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the log updown parameters.

Table 79: Log Updown Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the log updown.	(Optional) Enter a comment.
syslog / no-syslog	Specifies whether to log or not log a message to the system log file. <ul style="list-style-type: none"> syslog—Logs a message to the system log file. no-syslog—Does not log a message to the system log file. 	Select an option.
Trap Path Down	Specifies to send SNMP traps when a path goes down.	Select the check box to enable this feature.
Trap Path Up	Specifies to send SNMP traps when a path goes up.	Select the check box to enable this feature.
Mpls > Log Updown > Trap		
trap / no-trap	Specifies whether to send SNMP trap or not. <ul style="list-style-type: none"> trap—Sends an SNMP trap. no-trap—Does not send an SNMP trap. 	Select an option.
Mpls > Log Updown > Trap > No Trap		
Comment	Supplies a descriptive comment for path that does not send an SNMP trap.	(Optional) Enter a comment.
Mpls Lsp Traps	Specifies not to send MPLS label switch path up or down traps.	Select the check box to enable this feature.
Rfc3812 Traps	Specifies not to send RFC3812 traps.	Select the check box to enable this feature.

Related Documentation

- [Configuring OAM \(NSM Procedure\) on page 134](#)
- [Configuring Path \(NSM Procedure\) on page 137](#)
- [Configuring Path MTU \(NSM Procedure\) on page 138](#)

Configuring OAM (NSM Procedure)

You can configure Operation, Administration, and Maintenance (OAM) for devices.

To configure OAM:

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 OAM.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls > Oam**.

4. Enter a description for OAM in **Comment**.
5. Enter a time interval between LSP ping messages in **Lsp Ping Interval**. Range value is from 30 through 3600.
6. Configure OAM settings as described in [Table 80 on page 135](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the OAM parameters.

Table 80: OAM Configuration Details

Option	Function	Your Action
Mpls > Oam > Bfd Liveness Detection		
Comment	Supplies a descriptive comment of Bidirectional Forwarding Detection (BFD) protocol detection.	(Optional) Enter a comment.
Version	Specifies the BFD protocol version number.	Select a value from the list.
Minimum Interval	Specifies the minimum transmit and receive interval.	Enter a minimum interval value. Range vary from 1 through 255,000.
Minimum Receive Interval	Specifies the minimum receive interval.	Enter a minimum receive interval value. Range vary from 1 through 255,000.
Multiplier	Specifies the detection time multiplier.	Enter the multiplier value. Range vary from 1 through 255.
No Adaptation	Specifies to disable adaptation.	Select the check box to enable this feature.
Mpls > Oam > Bfd Liveness Detection > Detection Time		
Comment	Supplies a descriptive comment of BFD protocol detection time.	(Optional) Enter a comment.
Threshold	Specifies the high detection time triggering a trap.	Enter a threshold value. Range vary from 0 through 4,294,967,295.
Mpls > Oam > Bfd Liveness Detection > Failure Action		
Comment	Supplies a descriptive comment of BFD protocol failure action.	(Optional) Enter a comment.
Mpls > Oam > Bfd Liveness Detection > Failure Action > Teardown		

Table 80: OAM Configuration Details (*continued*)

Option	Function	Your Action
teardown / make-before-break	<p>Specifies the route path options.</p> <ul style="list-style-type: none"> teardown—When a BFD session fails for an RSVP label switch path, the associated label switch path is taken down and resigned immediately. make-before-break—When a BFD session fails for an RSVP label switch path, an attempt is made to signal a new label switch path before tearing down the old label switch path. 	Select an option.
Mpls > Oam > Bfd Liveness Detection > Failure Action > Teardown > Make Before Break		
Comment	Supplies a descriptive comment of BFD teardown.	(Optional) Enter a comment.
Teardown Timeout	Specifies the time to wait before teardown.	Enter a teardown timeout value. Range vary from 0 through 30.
Mpls > Oam > Bfd Liveness Detection > Transmit Interval		
Comment	Supplies a descriptive comment of the transmit interval.	(Optional) Enter a comment.
Minimum Interval	Specifies the minimum transmit and receive interval.	Enter a minimum interval value. Range vary from 1 through 255,000.
Threshold	Specifies high transmit interval triggering a trap.	Enter a threshold value. Range vary from 0 through 4,294,967,295.
Mpls > Oam > Traceoptions		
Comment	Supplies a descriptive comment of the traceoption.	(Optional) Enter a comment.
No remote Trace	Specifies to disable remote tracing.	Select the check box to enable this feature.
Mpls > Oam > Traceoptions > File		
Comment	Supplies a descriptive comment of the file traceoption.	(Optional) Enter a comment.
Filename	Specifies the name of file in which to write 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.	Enter the maximum number of trace files.
world-readable / no-world-readable	<p>Specifies file restriction access.</p> <ul style="list-style-type: none"> no-world-readable—Restricts file access to owner. world-readable—Enables unrestricted file access. 	Select an option.
Match	Specifies the regular expression for lines to be logged.	Enter the match criteria.

Table 80: OAM Configuration Details (*continued*)

Option	Function	Your Action
Mpls > Oam > Traceoptions > Flag		
Name	Specifies the name of the flag traceoption.	Enter a name for the flag traceoption.
Comment	Supplies a descriptive comment of the flag traceoption.	(Optional) Enter a comment.

- Related Documentation**
- [Configuring Path \(NSM Procedure\) on page 137](#)
 - [Configuring Static Label Switched Path \(NSM Procedure\) on page 139](#)
 - [Configuring Path MTU \(NSM Procedure\) on page 138](#)

Configuring Path (NSM Procedure)

To configure a path:

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 path.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls > Path**.
4. Click + to configure path as described in [Table 81 on page 137](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the path parameters.

Table 81: Path Configuration Details

Option	Function	Your Action
Mpls > Oam > Path		
Name	Specifies the name of label switch path.	Enter a name for the label switch path.
Comment	Supplies a descriptive comment for the label switch path.	(Optional) Enter a comment.
Mpls > Oam > Path > Path List		
Name	Specifies the name of the next system which is in the path.	Enter the name of the next path list.
Comment	Supplies a descriptive comment for the next path list.	(Optional) Enter a comment.

Table 81: Path Configuration Details (*continued*)

Option	Function	Your Action
loose / strict	<p>Specifies the source route option to direct traffic along a specific path.</p> <ul style="list-style-type: none"> • loose—Each incoming packet's source address is tested against the forwarding table. The packet is dropped only if the source address is not reachable via any interface on that device. • strict—Each incoming packet is tested against the forwarding table. If the incoming interface is not the best reverse path, the packet check will fail. 	Select an option.

Related Documentation

- [Configuring Path MTU \(NSM Procedure\) on page 138](#)
- [Configuring Static Label Switched Path \(NSM Procedure\) on page 139](#)
- [Configuring OAM \(NSM Procedure\) on page 134](#)

Configuring Path MTU (NSM Procedure)

You can configure a path MTU (maximum transmission unit) which prevents fragmentation.

To configure a path MTU :

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 path MTU.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls > Path Mtu**.
4. To configure path MTU, select **Enable Feature**.
5. Enter a descriptive comment about the path MTU in **Comment**.
6. To fragment IP before encapsulating in MPLS, select **Allow Fragmentation**.
7. Select **Protocols > Mpls > Path Mtu > Rsvp**.
8. To configure this feature, select **Enable Feature**.
9. Enter a descriptive comment about RSVP in **Comment**.
10. To enable RSVP path MTU signaling, select **Mtu Signaling**.
11. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the path MTU or RSVP parameters.

- Related Documentation**
- [Configuring Static Label Switched Path \(NSM Procedure\) on page 139](#)
 - [Configuring Path \(NSM Procedure\) on page 137](#)
 - [Configuring Statistics \(NSM Procedure\) on page 142](#)

Configuring Static Label Switched Path (NSM Procedure)

To configure a static label switched path:

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 static label switched path.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls > Static Label Switched Path**.
4. Click + to configure a static label switched path as described in [Table 82 on page 139](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the static label switch path parameters.

Table 82: Static Label Switched Path Configuration Details

Option	Function	Your Action
Mpls > Static Label Switched Path		
Name	Specifies the path name.	Enter a path name.
Comment	Supplies a descriptive comment for the path.	(Optional) Enter a comment.
Mpls > Static Label Switched Path > Bypass		
bypass / transit / ingress	Specifies the label switched path session status. <ul style="list-style-type: none"> • bypass—Sessions for bypass label switched paths. • transit—Sessions that transit through this device. • ingress—Sessions that originate from this device. 	Select an option.
Mpls > Static Label Switched Path > Bypass > bypass		
Comment	Supplies a descriptive comment for bypass.	(Optional) Enter a comment.
Bandwidth	Specifies the bandwidth to reserve.	Enter the bandwidth.
Description	Specifies the text description of the bypass label switched path.	Enter a description.

Table 82: Static Label Switched Path Configuration Details (*continued*)

Option	Function	Your Action
Next Hop	Specifies the address or interface of next-hop device.	Enter an address or interface.
Push	Specifies the label to push.	Enter the push value. Range vary from 0 through 1,048,575.
To	Specifies the address of the egress device.	Enter an address of the egress device.
Mpls > Static Label Switched Path > Bypass > transit		
Name	Specifies the name for transit.	Set the name as a value. Range vary from 1,000,000 through 1,048,575.
Comment	Supplies a descriptive comment for transit.	(Optional) Enter a comment.
Bandwidth	Specifies the bandwidth to reserve.	Enter the bandwidth.
Description	Specifies the text description of the transit label switched path.	Enter a description.
Next Hop	Specifies the address or interface of next-hop device.	Enter an address or interface.
Mpls > Static Label Switched Path > Bypass > transit > Link Protection		
Comment	Supplies a descriptive comment for transit link protection.	(Optional) Enter a comment.
Bypass Name	Specifies the bypass label switched path name.	Enter a bypass label switched path name.
Mpls > Static Label Switched Path > Bypass > transit > Node Protection		
Comment	Supplies a descriptive comment for transit node protection.	(Optional) Enter a comment.
Bypass Name	Specifies the bypass label switched path name.	Enter a bypass label switched path name.
Next Next Label	Specifies the label expected by next-next-hop device.	Enter the next next label value. Range vary from 0 through 1,048,575.
Mpls > Static Label Switched Path > Bypass > transit > Swap		
swap / pop	Specifies the virtual LAN tag operations.	Select an option. NOTE: If you select swap , enter a swap value. range vary from 0 through 1,048,575.
Mpls > Static Label Switched Path > Bypass > ingress		
Comment	Supplies a descriptive comment for bypass ingress.	(Optional) Enter a comment.
Bandwidth	Specifies the bandwidth to reserve.	Enter the bandwidth.

Table 82: Static Label Switched Path Configuration Details (*continued*)

Option	Function	Your Action
Class Of Service	Specifies the Class of Service value.	Enter the Class of Service value. Range vary from 0 through 7.
Description	Specifies the text description of the ingress label switched path.	Enter a description.
Metric	Specifies the metric value.	Enter the metric value. Range vary from 0 through 16,777,215.
Next Hop	Specifies the address or interface of next-hop device.	Enter an address or interface.
No Install To Address	Specifies not to install host route to address into routing tables.	Select the check box to enable this feature.
Preference	Specifies the preference value.	Enter the preference value. Range vary from 0 through 4,294,967,295.
To	Specifies the address of the egress device.	Enter an address of the egress device.
Push	Specifies the label to push.	Enter the push value. Range vary from 0 through 1,048,575.
Mpls > Static Label Switched Path > Bypass > Ingress > Install		
Name	Specifies the name of the destination prefix.	Enter the name for the destination prefix.
Comment	Supplies a descriptive comment for ingress install.	(Optional) Enter a comment.
Active	Specifies that you can install prefix into forwarding tables.	Select the check box to enable this feature.
Mpls > Static Label Switched Path > Bypass > Ingress > Link Protection		
Comment	Supplies a descriptive comment for ingress link protection.	(Optional) Enter a comment.
Bypass Name	Specifies the bypass label switch path name.	Enter a bypass name.
Mpls > Static Label Switched Path > Bypass > Ingress > Node Protection		
Comment	Supplies a descriptive comment for ingress node protection.	(Optional) Enter a comment.
Bypass Name	Specifies the bypass label switch path name.	Enter a bypass name.
Next Next Label	Specifies the label expected by next-next-hop device.	Enter the next-next label value. Range vary from 0 through 1,048,575.
Mpls > Static Label Switched Path > Bypass > Ingress > Policing		

Table 82: Static Label Switched Path Configuration Details (*continued*)

Option	Function	Your Action
Comment	Supplies a descriptive comment for ingress policing.	(Optional) Enter a comment.
Filter	Specifies the name of filter to use for policing label switch paths.	Select an option from the list.
No Auto Policing	Specifies to turn off automatic policing for this label switch path.	Select the check box to enable this feature.

Related Documentation

- [Configuring Path MTU \(NSM Procedure\) on page 138](#)
- [Configuring Statistics \(NSM Procedure\) on page 142](#)
- [Configuring Path \(NSM Procedure\) on page 137](#)

Configuring Statistics (NSM Procedure)

To configure statistics:

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 statistics.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls > Statistics**.
4. Enter a comment for the statistics in **Comment**.
5. Enter the time (in seconds) to collect statistics in **Interval**.
6. Select **Auto Bandwidth** to enable auto bandwidth allocation.
7. Configure file statistics as described in [Table 83 on page 142](#).
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the statistics parameters.

Table 83: File Statistics Configuration Details

Option	Function	Your Action
Mpls > Statistics > File		
Comment	Supplies a descriptive comment for the file traceoption.	(Optional) Enter a comment.
Filename	Specifies the name of a file in which to write trace information.	Enter the filename.
Size	Specifies the maximum trace file size.	Enter the maximum trace file size.

Table 83: File Statistics Configuration Details (*continued*)

Option	Function	Your Action
Files	Specifies the maximum number of trace files.	Enter the maximum number of trace files.
world-readable / no-world-readable	Specifies file restriction access. no-world-readable —restricts file access to owner. world-readable —enables unrestricted file access.	Select an option.

Related Documentation

- [Configuring Static Label Switched Path \(NSM Procedure\) on page 139](#)
- [Configuring Traceoptions \(NSM Procedure\) on page 143](#)
- [Configuring Path MTU \(NSM Procedure\) on page 138](#)

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 traceoptions.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Mpls > Traceoptions**.
4. Enter a comment for the traceoptions in **Comment**.
5. Configure traceoptions as described in [Table 84 on page 143](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the traceoptions parameters.

Table 84: Traceoptions Configuration Details

Option	Function	Your Action
Mpls > Traceoptions > File		
Comment	Supplies a descriptive comment for the file traceoption.	(Optional) Enter a comment.
Filename	Specifies the name of a file in which to write 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.	Enter the maximum number of trace files.

Table 84: Traceoptions Configuration Details (*continued*)

Option	Function	Your Action
world-readable / no-world-readable	Specifies file restriction access. no-world-readable —restricts file access to owner. world-readable —enables unrestricted file access.	Select an option.
Mpls > Traceoptions > Flag		
Name	Specifies the flag traceoption name.	Enter a flag traceoption name.
Comment	Supplies a descriptive comment for the flag traceoption.	(Optional) Enter a comment.

**Related
Documentation**

- [Configuring Statistics \(NSM Procedure\) on page 142](#)
- [Configuring Static Label Switched Path \(NSM Procedure\) on page 139](#)
- [Configuring Path MTU \(NSM Procedure\) on page 138](#)

Configuring MSDP (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 device establishes adjacencies with internal and external MSDP peers similar to the Border Gateway Protocol (BGP).

To configure MSDP:

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 MSDP.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Msdp**.
4. Enter a comment for MSDP in **Comment**.
5. Select a value from the list, **Data Encapsulation** to set encapsulation of data packets.
6. Select **MSDP** to disable MSDP.
7. Enter the local address of MSDP in **Local Address**.
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the MSDP parameters.

This topic includes the following sub topics:

- [Configuring Active Source Limit \(NSM Procedure\) on page 145](#)
- [Configuring Export \(NSM Procedure\) on page 145](#)

- [Configuring Group \(NSM Procedure\) on page 146](#)
- [Configuring Import \(NSM Procedure\) on page 150](#)
- [Configuring Peer \(NSM Procedure\) on page 150](#)
- [Configuring RIB Group \(NSM Procedure\) on page 152](#)
- [Configuring Source \(NSM Procedure\) on page 153](#)
- [Configuring Traceoptions \(NSM Procedure\) on page 153](#)

Configuring Active Source Limit (NSM Procedure)

To configure active source limit:

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 an active source limit.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Msdp > Active Source Limit**.
4. Enter a comment for the active source limit in **Comment**.
5. Enter the maximum number of active sources adapted in **Maximum**. Range vary from 1 through 1,000,000.
6. Enter the threshold for active source acceptance in **Threshold**. Range vary from 1 through 1,000,000.
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the active source limit parameters.

Configuring Export (NSM Procedure)

To export members:

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 export members.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Msdp > Export**.
4. Select the non-members from **Non-members**.
5. Click **Add** or **Remove** to add/remove non-members to members and members to non-members.



NOTE: Select all (required) records and click **Add All** or **Remove All** which will add the selected records to members or remove the selected records to non-members.

6. Click one:

- **OK**—Saves the changes.
- **Cancel**—Cancels the modifications.
- **Apply**—Applies the export parameters.

Configuring Group (NSM Procedure)

To configure groups:

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 groups.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Msdp > Group**.
4. Click **+** to configure groups as described in [Table 85 on page 146](#)
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the groups parameters.

Table 85: Groups Configuration Details

Option	Function	Your Action
Msdp > Group		
Name	Specifies the MSDP peer group name.	Enter a peer group name.
Comment	Supplies a descriptive comment for the peer group.	(Optional) Enter a comment.
Mode	Specifies the MSDP group source-active flooding mode.	Select an option from the list.
Disable	Specifies to disable MSDP.	Select the check box to enable this feature.
Local Address	Specifies the local address of the peer group.	Enter the local address of the peer group.
Msdp > Group > Export		

Table 85: Groups Configuration Details (*continued*)

Option	Function	Your Action
Non-members / Members	Adds or removes non-members to or from members list.	Click Add or Remove to add / remove non-members to members and members to non-members. NOTE: Select all (required) records and click Add All or Remove All which will add the selected records to members or remove the selected records to non-members.
Msdp > Group > Import		
Non-members / Members	Adds or removes non-members to or from members list.	Click Add or Remove to add / remove non-members to members and members to non-members. NOTE: Select all (required) records and click Add All or Remove All which will add the selected records to members or remove the selected records to non-members.
Msdp > Group > Peer		
Name	Specifies the peer address name.	Enter a peer address name.
Comment	Supplies a descriptive comment for the peer group.	(Optional) Enter a comment.
Disable	Specifies to disable MSDP.	Select the check box to enable this feature.
Local Address	Specifies the local address of the peer group.	Enter the local address of the peer group.
Default Peer	Specifies to disable default Reverse Path Forwarding (RPF) peer.	Select the check box to enable this feature.
Authentication Key	Specifies the MD5 authentication key.	Enter the MD5 authentication key.
Msdp > Group > Peer > Active Source Limit		
Comment	Supplies a descriptive comment for the active source limit.	(Optional) Enter a comment.
Maximum	Specifies the maximum number of active sources accepted.	Enter the maximum value. Range vary from 1 through 1,000,000.
Threshold	Specifies the threshold for active source acceptance.	Enter the threshold value. Range vary from 1 through 1,000,000.
Msdp > Group > Peer > Export		

Table 85: Groups Configuration Details (*continued*)

Option	Function	Your Action
Non-members / Members	Adds or removes non-members to or from members list.	Click Add or Remove to add / remove non-members to members and members to non-members. NOTE: Select all (required) records and click Add All or Remove All which will add the selected records to members or remove the selected records to non-members.
Msdp > Group > Peer > Import		
Non-members / Members	Adds or removes non-members to or from members list.	Click Add or Remove to add / remove non-members to members and members to non-members. NOTE: Select all (required) records and click Add All or Remove All which will add the selected records to members or remove the selected records to non-members.
Msdp > Group > Peer > Traceoptions		
Comment	Supplies a descriptive comment for the traceoptions.	(Optional) Enter a comment.
Msdp > Group > Peer > Traceoptions > File		
Comment	Supplies a descriptive comment for file traceoptions.	(Optional) Enter a comment.
Filename	Specifies the name of file in which to write 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.	Enter the maximum number of trace files.
world-readable / no-world-readable	Specifies file restriction access. no-world-readable —restricts file access to owner. world-readable —enables unrestricted file access.	Select an option.
Msdp > Group > Peer > Traceoptions > Flag		
Name	Specifies the flag traceoptions name.	Enter a flag traceoption name.
Comment	Supplies a descriptive comment for flag traceoptions.	(Optional) Enter a comment.
Send	Specifies to enable the trace transmitted packets.	Select the check box to enable this feature.
Receive	Specifies to enable the trace received packets.	Select the check box to enable this feature.

Table 85: Groups Configuration Details (*continued*)

Option	Function	Your Action
Detail	Specifies to enable the trace detailed information.	Select the check box to enable this feature.
Disable	Specifies to disable the trace flag.	Select the check box to enable this feature.
Msdp > Group > Traceoptions		
Comment	Supplies a descriptive comment for traceoptions.	(Optional) Enter a comment.
Msdp > Group > Traceoptions > File		
Comment	Supplies a descriptive comment for file traceoptions.	(Optional) Enter a comment.
Filename	Specifies the name of file in which to write 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.	Enter the maximum number of trace files.
world-readable / no-world-readable	Specifies file restriction access. no-world-readable —restricts file access to owner. world-readable —enables unrestricted file access.	Select an option.
Msdp > Group > Traceoptions > Flag		
Name	Specifies the flag traceoptions name.	Enter a flag traceoption name.
Comment	Supplies a descriptive comment for flag traceoptions.	(Optional) Enter a comment.
Send	Specifies to enable the trace transmitted packets.	Select the check box to enable this feature.
Receive	Specifies to enable the trace received packets.	Select the check box to enable this feature.
Detail	Specifies to enable the trace detailed information.	Select the check box to enable this feature.
Disable	Specifies to disable the trace flag.	Select the check box to enable this feature.

Configuring Import (NSM Procedure)

To import members:

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 import members.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Msdp > Import**.
4. Select the non-members from **Non-members**.
5. Click **Add** or **Remove** to add / remove non-members to members and members to non-members.



NOTE: Select all (required) records and click **Add All** or **Remove All** which will add the selected records to members or remove the selected records to non-members.

6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the import parameters.

Configuring Peer (NSM Procedure)

To configure peers:

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 peers.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Msdp > Peer**.
4. Click + to configure peers as described in [Table 86 on page 150](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the peer parameters.

Table 86: Peer Configuration Details

Option	Function	Your Action
Msdp > Peer		
Name	Specifies the peer name.	Enter a peer name.

Table 86: Peer Configuration Details (*continued*)

Option	Function	Your Action
Comment	Supplies a descriptive comment for peer.	(Optional) Enter a comment.
Disable	Specifies to disable MSDP.	Select the check box to enable this feature.
Local Address	Specifies the local address of the peer.	Enter the local address of the peer.
Default Peer	Specifies to enable default RPF peer.	Select the check box to enable this feature.
Authentication Key	Specifies the MD5 authentication key.	Enter the MD5 authentication key.
Msdp > Peer > Active Source Limit		
Comment	Supplies a descriptive comment for the peer active source limit.	(Optional) Enter a comment.
Maximum	Specifies the maximum number of active sources accepted.	Enter the maximum value. Range vary from 1 through 1,000,000.
Threshold	Specifies the threshold for active source acceptance.	Enter the threshold value. Range vary from 1 through 1,000,000.
Msdp > Peer > Export		
Non-members / Members	Adds or removes non-members to or from members list.	Click Add or Remove to add / remove non-members to members and members to non-members. NOTE: Select all (required) records and click Add All or Remove All which will add the selected records to members or remove the selected records to non-members.
Msdp > Peer > Import		
Non-members / Members	Adds or removes non-members to or from members list.	Click Add or Remove to add / remove non-members to members and members to non-members. NOTE: Select all (required) records and click Add All or Remove All which will add the selected records to members or remove the selected records to non-members.
Msdp > Peer > Traceoptions		
Comment	Supplies a descriptive comment for the peer traceoptions.	(Optional) Enter a comment.
Msdp > Peer > Traceoptions > File		
Comment	Supplies a descriptive comment for the file traceoption.	(Optional) Enter a comment.

Table 86: Peer Configuration Details (*continued*)

Option	Function	Your Action
Filename	Specifies the name of file in which to write 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.	Enter the maximum number of trace files.
world-readable / no-world-readable	Specifies file restriction access. no-world-readable —restricts file access to owner. world-readable —enables unrestricted file access.	Select an option.
Msdp > Peer > Traceoptions > Flag		
Name	Specifies the flag traceoptions name.	Enter a flag traceoption name.
Comment	Supplies a descriptive comment for flag traceoptions.	(Optional) Enter a comment.
Send	Specifies to enable the trace transmitted packets.	Select the check box to enable this feature.
Receive	Specifies to enable the trace received packets.	Select the check box to enable this feature.
Detail	Specifies to enable the trace detailed information.	Select the check box to enable this feature.
Disable	Specifies to disable the trace flag.	Select the check box to enable this feature.

Configuring RIB Group (NSM Procedure)

A RIB (routing information base) group is a way to have a routing protocol, in most cases, place information in multiple route tables.

To configure a RIB group:

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 RIB groups.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Msdp > Rib Group**.
4. Enter a comment for the RIB group in **Comment**.
5. Enter a name for the routing table group in **Ribgroup Name**.
6. Click one:
 - **OK**—Saves the changes.

- **Cancel**—Cancels the modifications.
- **Apply**—Applies the RIB group parameters.

Configuring Source (NSM Procedure)

To configure source:

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 source.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Msdp > Source**.
4. Click + to configure source as described in [Table 87 on page 153](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the source parameters.

Table 87: Source Configuration Details

Option	Function	Your Action
Msdp > Source		
Name	Specifies the source address name.	Enter the source address name.
Comment	Supplies a descriptive comment for the source.	(Optional) Enter a comment.
Msdp > Source > Active Source Limit		
Comment	Supplies a descriptive comment for the source.	(Optional) Enter a comment.
Maximum	Specifies the maximum number of active sources accepted.	Enter the maximum value. Range vary from 1 through 1,000,000.
Threshold	Specifies the threshold for active source acceptance.	Enter the threshold value. Range vary from 1 through 1,000,000.

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 traceoptions.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Msdp > Traceoptions**.
4. Enter a comment for the traceoptions in **Comment**.

5. Configure traceoptions as described in [Table 88 on page 154](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the traceoptions parameters.

Table 88: Traceoptions Configuration Details

Option	Function	Your Action
Msdp > Traceoptions > File		
Comment	Supplies a descriptive comment for the file traceoption.	(Optional) Enter a comment.
Filename	Specifies the name of file in which to write 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.	Enter the maximum number of trace files.
world-readable / no-world-readable	Specifies file restriction access. no-world-readable —restricts file access to owner. world-readable —enables unrestricted file access.	Select an option.
Msdp > Traceoptions > Flag		
Name	Specifies the flag traceoptions name.	Enter a flag traceoption name.
Comment	Supplies a descriptive comment for flag traceoptions.	(Optional) Enter a comment.
Send	Specifies to enable the trace transmitted packets.	Select the check box to enable this feature.
Receive	Specifies to enable the trace received packets.	Select the check box to enable this feature.
Detail	Specifies to enable the trace detailed information.	Select the check box to enable this feature.
Disable	Specifies to disable the trace flag.	Select the check box to enable this feature.

Related Documentation

- [Configuring Statistics \(NSM Procedure\) on page 142](#)
- [Configuring Static Label Switched Path \(NSM Procedure\) on page 139](#)
- [Configuring Path MTU \(NSM Procedure\) on page 138](#)

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 89 on page 155](#).



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 89: 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 89: 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 90 on page 157](#).
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 90: OSPF Configuration Fields

Option	Function	Your Action
OSPF		

Table 90: 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 90: 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 91 on page 160](#).
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 91: RIP Configuration Fields

Option	Function	Your Action
RIP		

Table 91: 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.	<ol style="list-style-type: none"> 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.	<ol style="list-style-type: none"> 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.	<ol style="list-style-type: none"> 1. Expand the RIP tree and select Import. 2. Specify the import policies.
Receive	Enables you to configure RIP receive options.	<ol style="list-style-type: none"> 1. Expand the RIP tree and select Receive. 2. Specify the receive options.

Table 91: 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 (NSM Procedure)

The Routing Information Protocol next generation (RIPng) is an interior gateway protocol (IGP) that uses a distance-vector algorithm to determine the best route to a destination, using the hop count as the metric. RIPng is a routing protocol that exchanges routing information used to compute routes and is intended for Internet Protocol version 6 (IPv6)-based networks.

To configure RIPng:

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 RIPng.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Ripng**.
4. Configure settings as described in [Table 92 on page 162](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the RIPng parameters.

Table 92: RIPng Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the RIPng protocol.	(Optional) Enter a comment.
Metric In	Specifies the metric value to add to incoming routes.	Enter the metric value. Range vary from 1 through 15.

Table 92: RIPng Configuration Details (*continued*)

Option	Function	Your Action
Holddown	Specifies the estimated time to wait before making updates to the routing table.	Enter the hold-down time. Range vary from 10 through 180.
Route Timeout	Specifies the delay before routes time out.	Enter the route time out. Range vary from 30 through 360.
Update Interval	Specifies the interval between regular route updates.	Enter the update interval time. Range vary from 10 through 60.

This topic includes the following sub topics:

- [Configuring Graceful Restart \(NSM Procedure\) on page 163](#)
- [Configuring Groups \(NSM Procedure\) on page 164](#)
- [Configuring Import \(NSM Procedure\) on page 166](#)
- [Configuring Receive \(NSM Procedure\) on page 166](#)
- [Configuring Send \(NSM Procedure\) on page 167](#)
- [Configuring Traceoptions \(NSM Procedure\) on page 167](#)

Configuring Graceful Restart (NSM Procedure)

To configure graceful restart:

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 graceful restart.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Ripng > Graceful Restart**.
4. Select **Enable Feature** to enable the check box. This allows to configure graceful restart.
5. Enter a descriptive comment for the graceful restart in **Comment**.
6. Select **Disable** to disable graceful restart.
7. Enter the time after which RIPng is declared out of restart in **Restart Time**. Range vary from 1 through 600.
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the graceful restart parameters.

Configuring Groups (NSM Procedure)

To configure groups:

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 groups.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Ripng > Group**.
4. Click + to configure groups as described in [Table 93 on page 164](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the groups parameters.

Table 93: Groups Configuration Details

Option	Function	Your Action
Ripng > Group		
Name	Specifies the group name.	Enter the group name.
Comment	Supplies a descriptive comment for the RIPng group.	(Optional) Enter a comment.
Route Timeout	Specifies delay before routes time out.	Enter the route time out value. Range vary from 30 through 360.
Update Interval	Specifies the interval between regular route updates.	Enter the update interval time. Range vary from 10 through 60.
Preference	Specifies the preference of route learned from this group.	Enter the preference. Range vary from 0 through 4,294,967,295.
Metric Out	Specifies the default route of exported routes.	Enter the metric out value. Range vary from 1 through 15.
Ripng > Group > Export		
Non-members / Members	Adds or removes non-members to or from members list.	Click Add or Remove to add/remove non-members to members and members to non-members. NOTE: Select all (required) records and click Add All or Remove All which will add the selected records to members or remove the selected records to non-members.
Ripng > Group > Import		

Table 93: Groups Configuration Details (*continued*)

Option	Function	Your Action
Non-members / Members	Adds or removes non-members to or from members list.	Click Add or Remove to add/remove non-members to members and members to non-members. NOTE: Select all (required) records and click Add All or Remove All which will add the selected records to members or remove the selected records to non-members.
Ripng > Group > Neighbor		
Name	Specifies the neighbor interface name.	Enter the neighbor interface name.
Comment	Supplies a descriptive comment for the neighbor interface name.	(Optional) Enter a comment.
Route Timeout	Specifies delay before routes time out.	Enter the route time out value. Range vary from 30 through 360.
Update Interval	Specifies the interval between regular route updates.	Enter the update interval time. Range vary from 10 through 60.
Metric In	Specifies the metric value to add to incoming routes.	Enter the metric value. Range vary from 1 through 15.
Ripng > Group > Neighbor > Import		
Non-members / Members	Adds or removes non-members to or from members list.	Click Add or Remove to add/remove non-members to members and members to non-members. NOTE: Select all (required) records and click Add All or Remove All which will add the selected records to members or remove the selected records to non-members.
Ripng > Group > Neighbor > Receive		
Comment	Supplies a descriptive comment for the neighbor receive update.	(Optional) Enter a comment.
None	Specifies not to receive any RIPng packets.	Select the check box to enable this feature.
Ripng > Group > Neighbor > Send		
Comment	Supplies a descriptive comment for the neighbor send update.	(Optional) Enter a comment.
None	Specifies not to send any RIPng packets.	Select the check box to enable this feature.

Configuring Import (NSM Procedure)

To import members:

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 import members.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Ripng > Import**.
4. Select the non-members from **Non-members**.
5. Click **Add** or **Remove** to add/remove non-members to members and members to non-members.



NOTE: Select all (required) records and click **Add All** or **Remove All** which will add the selected records to members or remove the selected records to non-members.

6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the import parameters.

Configuring Receive (NSM Procedure)

To configure receive RIPng packets:

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 receive RIPng packets.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Ripng > Receive**.
4. Enter a descriptive comment for receiving RIPng packets in **Comment**.
5. Select **None** to not to receive any RIPng packets.
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the receive parameters.

Configuring Send (NSM Procedure)

To configure send RIPng packets:

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 send RIPng packets.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Ripng > Send**.
4. Enter a descriptive comment for sending RIPng packets in **Comment**.
5. Select **None** to not to send any RIPng updates.
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the send parameters.

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 traceoptions.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Ripng > Traceoptions**.
4. Enter a comment for the traceoptions in **Comment**.
5. Configure traceoptions as described in [Table 94 on page 167](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the traceoptions parameters.

Table 94: Traceoptions Configuration Details

Option	Function	Your Action
Msdp > Traceoptions > File		
Comment	Supplies a descriptive comment for the file traceoption.	(Optional) Enter a comment.
Filename	Specifies the name of file in which to write trace information.	Enter the filename.
Size	Specifies the maximum trace file size.	Enter the maximum trace file size.

Table 94: Traceoptions Configuration Details (*continued*)

Option	Function	Your Action
Files	Specifies the maximum number of trace files.	Enter the maximum number of trace files.
world-readable / no-world-readable	Specifies file restriction access. no-world-readable —restricts file access to owner. world-readable —enables unrestricted file access.	Select an option.
Msdp > Traceoptions > Flag		
Name	Specifies the flag traceoptions name.	Enter a flag traceoption name.
Comment	Supplies a descriptive comment for flag traceoptions.	(Optional) Enter a comment.
Send	Specifies to enable the trace transmitted packets.	Select the check box to enable this feature.
Receive	Specifies to enable the trace received packets.	Select the check box to enable this feature.
Detail	Specifies to enable the trace detailed information.	Select the check box to enable this feature.
Disable	Specifies to disable the trace flag.	Select the check box to enable this feature.

- Related Documentation**
- [Configuring MSDP \(NSM Procedure\) on page 144](#)
 - [Configuring Static Label Switched Path \(NSM Procedure\) on page 139](#)
 - [Configuring Path MTU \(NSM Procedure\) on page 138](#)

Configuring Router Advertisement (NSM Procedure)

To configure router advertisement:

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 router advertisement.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Router Advertisement**.
4. Enter a descriptive comment for the router advertisement in **Comment**.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the router advertisement parameters.

Table 95: Router Advertisement Configuration Details

Option	Function	Your Action
Router Advertisement > Interface		
Name	Specifies the router advertisement interface name.	Enter a router advertisement interface name.
Comment	Supplies a descriptive comment for the router advertisement interface.	(Optional) Enter a comment.
Max Advertisement Interval	Specifies the maximum advertisement interval.	Enter the maximum advertisement interval time. Range vary from 4 through 1,800.
Min Advertisement Interval	Specifies the minimum advertisement interval.	Enter the minimum advertisement interval time. Range vary from 3 through 1,350.
managed-configuration / no-managed-configuration	<p>Specifies whether to enable the host to use a stateful auto configuration protocol for address auto configuration, along with any stateless auto configuration already configured or not.</p> <ul style="list-style-type: none"> • managed-configuration—Enables host to use stateful auto configuration. • no-managed-configuration—Disables host from using stateful auto configuration. 	Select an option.
other-stateful-configuration / no-other-stateful-configuration	<p>Specifies whether to enable auto configuration of other non address-related information or not.</p> <ul style="list-style-type: none"> • other-stateful-configuration—Enables auto configuration of other non address-related information. • no-other-stateful-configuration—Disables auto configuration of other non address-related information. 	Select an option.
link-mtu / no-link-mtu	<p>Specifies whether to include the maximum transmission unit (MTU) option in router advertisement messages or not.</p> <ul style="list-style-type: none"> • link-mtu—Includes the MTU option in router advertisements. • no-link-mtu—Does not include the MTU option in router advertisements. 	Select an option.
Reachable Time	Specifies the length of time that a node considers a neighbor reachable, until another reachability confirmation is received from that neighbor.	Enter the reachable time. Range vary from 0 through 3,600,000.
Retransmit Timer	Specifies the retransmission frequency of neighbor solicitation messages.	Enter the retransmit time. Range vary from 0 through 4,294,967,295.

Table 95: Router Advertisement Configuration Details (*continued*)

Option	Function	Your Action
Virtual Router Only	Specifies that router advertisements are sent only for virtual router redundancy protocol (VRRP) IPv6 groups configured on the interface (if the groups are in the master state).	Select the check box to enable this feature.
Current Hop Limit	Specifies the default value placed in the hop count field of the IP header for outgoing packets.	Enter the current hop limit value. Range vary from 0 through 255.
Default Lifetime	Specifies the lifetime associated with a default router.	Enter a default lifetime value. range vary from 0 through 9,000.
Router Advertisement > Interface > Prefix		
Name	Name of the prefix to be advertised.	Enter a prefix name.
Comment	Supplies a descriptive comment for the prefix router advertisement.	(Optional) Enter a comment.
Valid Lifetime	Specifies how long the prefix remains valid for on-link determination.	Enter the valid lifetime value. Range vary from 0 through 4,294,967,295.
on-link / no-on-link	Specifies whether to enable prefixes to be used for on-link determination or not. <ul style="list-style-type: none"> • on-link—Enables prefixes to be used for on-link determination. • no-on-link—Disables prefixes from being used for on-link determination. 	Select an option.
Preferred Lifetime	Specifies the duration of the prefix generated by stateless auto configuration that remains preferred.	Enter the preferred lifetime value. Range vary from 0 through 4,294,967,295.
autonomous / no-autonomous	Specifies whether prefixes in the router advertisement messages are used for stateless address auto configuration or not. <ul style="list-style-type: none"> • autonomous—Uses prefixes for address auto configuration. • no-autonomous—Does not use prefixes for address auto configuration. 	Select an option.
Router Advertisement > Traceoptions		
Comment	Supplies a descriptive comment for the traceoption.	(Optional) Enter a comment.
Router Advertisement > Traceoptions > File		
Comment	Supplies a descriptive comment for the file traceoption.	(Optional) Enter a comment.
Filename	Specifies the name of file in which to write trace information.	Enter the filename.

Table 95: Router Advertisement Configuration Details (*continued*)

Option	Function	Your Action
Size	Specifies the maximum trace file size.	Enter the maximum trace file size.
Files	Specifies the maximum number of trace files.	Enter the maximum number of trace files.
world-readable / no-world-readable	Specifies file restriction access. no-world-readable —restricts file access to owner. world-readable —enables unrestricted file access.	Select an option.
Router Advertisement > Traceoptions > Flag		
Name	Specifies the flag traceoption name.	Enter a flag traceoption name.
Comment	Supplies a descriptive comment for the flag traceoption.	(Optional) Enter a comment.

**Related
Documentation**

- [Configuring MSDP \(NSM Procedure\) on page 144](#)
- [Configuring RIPv6 \(NSM Procedure\) on page 162](#)

Configuring Router Discovery (NSM Procedure)

Router discovery uses Internet Control Message Protocol (ICMP) router advertisements and router solicitation messages to allow a host to discover the addresses of operational routers on the subnet. Hosts must discover routers before they can send IP datagrams outside their subnet. Router discovery allows a host to discover the addresses of operational routers on the subnet.

To configure router discovery:

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 router discovery.
3. Click the **Configuration** tab. In the configuration tree, select **Protocols > Router Discovery**.
4. Enter a descriptive comment for the router discovery in **Comment**.
5. Select **Disable** to disable router discovery.
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the router discovery parameters.

Table 96: Router Discovery Configuration Details

Option	Function	Your Action
Router Discovery > Address		
Name	Specifies the Internet Protocol (IP) addresses to include in router advertisements.	Enter the IP address name.
Comment	Supplies a descriptive comment for the router discovery address.	(Optional) Enter a comment.
Advertise	Specifies to advertise the IP address.	Select the check box to enable this feature.
Ignore	Specifies not to advertise the IP address.	Select the check box to enable this feature.
Broadcast	Specifies to include IP address only in broadcast advertisements.	Select the check box to enable this feature.
Multicast	Specifies to include IP address only in multicast advertisements.	Select the check box to enable this feature.
Ineligible	Specifies that the IP address can never become a default router.	Select the check box to enable this feature.
Priority	Specifies the preference of the IP address to become a default router.	Enter the preference level. Range vary from -2,147,483,648 through 2,147,483,648.
Router Discovery > Interface		
Name	Specifies the interface name.	Enter the interface name.
Comment	Supplies a descriptive comment for the router discovery interface.	(Optional) Enter a comment.
Max Advertisement Interval	Specifies the maximum time before sending advertisements.	Enter the maximum advertisement interval time. Range vary from 4 through 1,800.
Min Advertisement Interval	Specifies the minimum time before sending advertisements.	Enter the minimum advertisement interval time. Range vary from 3 through 1,800.
Lifetime	Specifies how long the addresses in advertisements are valid.	Enter the time duration until the addresses in advertisements are valid. Range vary from 3 through 9,000.
Router Discovery > Traceoptions		
Comment	Supplies a descriptive comment for the traceoption.	(Optional) Enter a comment.
Router Discovery > Traceoptions > File		
Comment	Supplies a descriptive comment for the file traceoption.	(Optional) Enter a comment.
Filename	Specifies the name of file in which to write trace information.	Enter the filename.

Table 96: Router Discovery Configuration Details (*continued*)

Option	Function	Your Action
Size	Specifies the maximum trace file size.	Enter the maximum trace file size.
Files	Specifies the maximum number of trace files.	Enter the maximum number of trace files.
world-readable / no-world-readable	Specifies file restriction access. no-world-readable —restricts file access to owner. world-readable —enables unrestricted file access.	Select an option.
Router Discovery > Traceoptions > Flag		
Name	Specifies the flag traceoption name.	Enter a flag traceoption name.
Comment	Supplies a descriptive comment for the flag traceoption.	(Optional) Enter a comment.

**Related
Documentation**

- [Configuring Router Advertisement \(NSM Procedure\) on page 168](#)
- [Configuring RIPv6 \(NSM Procedure\) on page 162](#)

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 97 on page 174](#).
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 97: 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.

Table 97: VSTP Configuration Fields (*continued*)

Field	Function	Your Action
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 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 98 on page 175](#).
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 98: VRRP Configuration Fields

Field	Function	Your Action
VRRP		

Table 98: VRRP Configuration Fields (*continued*)

Field	Function	Your Action
Comment	Specifies comment for VRRP.	<ol style="list-style-type: none"> 1. Expand the Protocol tree and select VRRP. 2. Enter the comment.
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 Security for J Series Services Routers and SRX Series Services Gateways

- [Configuring Certificates \(NSM Procedure\) on page 177](#)
- [Configuring Firewall Authentication \(NSM Procedure\) on page 180](#)
- [Configuring a Flow \(NSM Procedure\) on page 181](#)
- [Configuring Forwarding Options \(NSM Procedure\) on page 187](#)
- [Configuring IKE \(NSM Procedure\) on page 188](#)
- [Configuring IPsec \(NSM Procedure\) on page 195](#)
- [Configuring a PKI \(NSM Procedure\) on page 201](#)
- [Configuring NAT \(NSM Procedure\) on page 206](#)

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 99 on page 178](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the certificates parameters.

Table 99: 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.
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 178](#)
- [Configuring the Local Certificate \(NSM Procedure\) on page 179](#)

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 100 on page 178](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the certification authority settings.

Table 100: 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.

Table 100: Certification Authority Configuration Details (*continued*)

Option	Function	Your Action
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 101 on page 179](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the local settings.

Table 101: 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 \(NSM Procedure\) on page 180](#)
- [Configuring a Flow \(NSM Procedure\) on page 181](#)
- [Configuring Forwarding Options \(NSM Procedure\) on page 187](#)

Configuring Firewall Authentication (NSM Procedure)

To configure firewall authentication 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 firewall authentication feature.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Firewall Authentication**.
4. Enter a comment in the Firewall Authentication workspace that describes the firewall authentication.
5. In the configuration tree, select **Security > Firewall Authentication > Traceoptions**.
6. Enter a comment in the Traceoptions workspace that describes the traceoptions.
7. In the configuration tree, select **Security > Firewall Authentication > Traceoptions > Flag**.
8. Add or modify settings as specified in [Table 102 on page 180](#).
9. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the traceoptions settings.

Table 102: Firewall Authentication Configuration Details

Option	Function	Your Action
Name	Specifies the trace flag name.	Select a flag name from the list.
Comment	Supplies a descriptive comment for the trace flag.	(Optional) Enter a comment.
None	Specifies that the flag options does not belong to any of the other options type such as terse, detail, or extensive.	Select the option.
Terse	Specifies brief traceoptions information.	Select the option.
Detail	Specifies detailed traceoptions information.	Select the option.
Extensive	Specifies extensive traceoptions information.	Select the option.

Related Documentation

- [Configuring Certificates \(NSM Procedure\) on page 177](#)
- [Configuring a Flow \(NSM Procedure\) on page 181](#)
- [Configuring Forwarding Options \(NSM Procedure\) on page 187](#)

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 103 on page 181](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the flow parameters.

Table 103: 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 181](#)
- [Configuring the TCP MSS Option \(NSM Procedure\) on page 182](#)
- [Configuring the TCP Session Option \(NSM Procedure\) on page 183](#)
- [Configuring Traceoptions \(NSM Procedure\) on page 184](#)

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 104 on page 182](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the bridge settings.

Table 104: 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 105 on page 183](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the TCP MSS settings.

Table 105: TCP MSS Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for TCP MSS.	(Optional) Enter a comment.
Tcp Mss > All Tcp		
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 106 on page 184](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the TCP session settings.

Table 106: 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 107 on page 185](#).
5. Click one:
 - **OK**—Saves the changes.

- **Cancel**—Cancels the modifications.
- **Apply**—Applies the traceoptions settings.

Table 107: 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 185](#)
- [Configuring Flag Options \(NSM Procedure\) on page 186](#)
- [Configuring Packet Filter Options \(NSM Procedure\) on page 186](#)

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 108 on page 185](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the file settings.

Table 108: 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.

Table 108: File Configuration Details (*continued*)

Option	Function	Your Action
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 > Flow > Traceoptions > Flag**.
4. Add or modify settings as specified in [Table 109 on page 186](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the flag settings.

Table 109: 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 110 on page 187](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the packet filter settings.

Table 110: 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 177](#)
- [Configuring Firewall Authentication \(NSM Procedure\) on page 180](#)
- [Configuring Forwarding Options \(NSM Procedure\) on page 187](#)

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 111 on page 188](#).
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the forwarding options.

Table 111: 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 177](#)
 - [Configuring Firewall Authentication \(NSM Procedure\) on page 180](#)
 - [Configuring a Flow \(NSM Procedure\) on page 181](#)

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 189](#)
- [Configuring a Policy \(NSM Procedure\) on page 191](#)
- [Configuring a Respond Bad SPI \(NSM Procedure\) on page 193](#)
- [Configuring Traceoptions \(NSM Procedure\) on page 193](#)

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 112 on page 189](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the gateway settings.

Table 112: 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.

Table 112: Gateway Configuration Details (*continued*)

Option	Function	Your Action
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.
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		

Table 112: Gateway Configuration Details (*continued*)

Option	Function	Your Action
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.
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 113 on page 191](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the policy settings.

Table 113: Policy Configuration Details

Option	Function	Your Action
Policy		
Name	Specifies the name of the policy.	Enter the policy name.

Table 113: Policy Configuration Details (*continued*)

Option	Function	Your Action
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.
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		

Table 113: Policy Configuration Details (*continued*)

Option	Function	Your Action
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 114 on page 193](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the respond bad SPI parameters.

Table 114: 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 115 on page 194](#).
5. Click one:

- **OK**—Saves the changes.
- **Cancel**—Cancels the modifications.
- **Apply**—Applies the traceoptions settings.

Table 115: 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 194](#)
- [Configuring Flag Options \(NSM Procedure\) on page 195](#)

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 116 on page 194](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the file settings.

Table 116: 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.

Table 116: 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 > Ike > Traceoptions > Flag**.
4. Add or modify setting as specified in [Table 117 on page 195](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the flag settings.

Table 117: 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 195](#)
 - [Configuring a PKI \(NSM Procedure\) on page 201](#)
 - [Configuring NAT \(NSM Procedure\) on page 206](#)

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 196](#)
- [Configuring Traceoptions \(NSM Procedure\) on page 197](#)
- [Configuring a VPN \(NSM Procedure\) on page 198](#)
- [Configuring VPN Monitor Options \(NSM Procedure\) on page 200](#)

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 118 on page 196](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the policy settings.

Table 118: 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.

Table 118: Policy Configuration Details (*continued*)

Option	Function	Your Action
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.
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 119 on page 197](#).
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 119: 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 120 on page 198](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the VPN settings.

Table 120: 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.

Table 120: VPN Configuration Details (*continued*)

Option	Function	Your Action
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.
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.

Table 120: VPN Configuration Details (*continued*)

Option	Function	Your Action
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		
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 121 on page 201](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the VPN monitor options.

Table 121: 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 188](#)
- [Configuring Forwarding Options \(NSM Procedure\) on page 187](#)
- [Configuring a Flow \(NSM Procedure\) on page 181](#)

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 202](#)
- [Configuring a CA Profile \(NSM Procedure\) on page 202](#)
- [Configuring Traceoptions \(NSM Procedure\) on page 204](#)

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 122 on page 202](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the auto re-enrollment parameters.

Table 122: 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 123 on page 203](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the CA profile parameters.

Table 123: 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.
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		

Table 123: CA Profile Configuration Details (*continued*)

Option	Function	Your Action
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		
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 124 on page 205](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

- **Apply**—Applies the traceoptions settings.

Table 124: 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 205](#)
- [Configuring Flag Options \(NSM Procedure\) on page 206](#)

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 125 on page 205](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the file settings.

Table 125: 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.

Table 125: File Configuration Details (*continued*)

Option	Function	Your Action
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 126 on page 206](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the flag settings.

Table 126: 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 195](#)
- [Configuring IKE \(NSM Procedure\) on page 188](#)
- [Configuring NAT \(NSM Procedure\) on page 206](#)

Configuring NAT (NSM Procedure)

The Network Address Translation (NAT) feature allows you to configure destination, source NAT, destination NAT, interface, proxy ARP, source, static, and traceoptions.

To configure the NAT 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 NAT.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Nat**.
4. Enter a comment in the NAT workspace that describes the NAT.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the NAT settings.

You can now configure the following options:

1. [Configuring a Destination \(NSM Procedure\) on page 207](#)
2. [Configuring Destination NAT \(NSM Procedure\) on page 208](#)
3. [Configuring the Interface \(NSM Procedure\) on page 210](#)
4. [Configuring a Proxy Address Resolution Protocol \(NSM Procedure\) on page 212](#)
5. [Configuring a Source \(NSM Procedure\) on page 213](#)
6. [Configuring the Source Nat \(NSM Procedure\) on page 216](#)
7. [Configuring the Static Nat \(NSM Procedure\) on page 217](#)
8. [Configuring Traceoptions \(NSM Procedure\) on page 218](#)

Configuring a Destination (NSM Procedure)

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 **Security > Nat > Destination**.
4. Configure the options as specified in [Table 127 on page 207](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the destination parameters.

Table 127: Traceoptions Configuration Details

Option	Function	Your Action
Destination > General		

Table 127: Traceoptions Configuration Details (*continued*)

Option	Function	Your Action
Comment	Supplies a descriptive comment for the destination.	(Optional) Enter a comment.
Destination > Pool > General		
Name	Specifies the name of the destination pool.	Enter a name.
Comment	Supplies a descriptive comment for the destination pool.	(Optional) Enter a comment.
Destination > Pool > Routing Instance		
Comment	Supplies a descriptive comment for the destination pool.	(Optional) Enter a comment.
Ri Name	Specifies the routing instance (RI) name.	Select the Ri Name from the list..
Destination > Pool > Address > IP Address		
Comment	Supplies a descriptive comment for the destination IP address.	(Optional) Enter a comment.
IP Address	Specifies the IP address or address range of the destination pool.	Enter the IP address or an address range.
Destination > Pool > Address > To Range/Port		
None	Specifies that neither the destination address nor the port option is selected.	Select the option.
To Address	Specifies the upper limit of the address range.	Select the option and enter the following: <ul style="list-style-type: none"> Comment—A descriptive comment about the destination address. To Address—The upper limit of the address range.
port	Specifies the port.	Select the option and set the port. Range: 0 - 65535.

Configuring Destination NAT (NSM Procedure)

To configure destination NAT:

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 NAT.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Nat > Destination Nat**.

4. Add or modify settings as specified in [Table 128 on page 209](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the destination NAT settings.

Table 128: Destination NAT Configuration Details

Option	Function	Your Action
destination-nat		
Name	Specifies a name for the destination NAT.	Enter a name.
destination-nat > From		
Zone/RI/Interface	Specifies the zone, routing instance or the interface selected for the destination NAT.	Select an option.
Match		
Source Address	Specifies the source address for the destination NAT.	Select the option and enter the following: <ul style="list-style-type: none"> • Comment—Descriptive comment for the destination address. • Prefix—Address prefix. • Port—Port number. Low—Lower limit of the address range. High—Higher limit of the address range.
Source Address Name	Specifies the source address name of the destination NAT.	Select the option and enter the following: <ul style="list-style-type: none"> • Comment—Descriptive comment for the address range. • Address Object—Address object pushed to the global address book. • Port—Port number. Low—Lower limit of the address range. High—Higher limit of the address range.
Destination Address	Specifies the destination address of the destination NAT.	Either Destination Address or Destination Address Name can be used for an instance.
Destination Address Name	Specifies the destination address name of the destination NAT.	Either Destination Address or Destination Address Name can be used for an instance.
Destination Port		<ul style="list-style-type: none"> • Port—Port number. Low—Lower limit of the address range. High—Higher limit of the address range.

Table 128: Destination NAT Configuration Details (*continued*)

Option	Function	Your Action
Action		<ul style="list-style-type: none"> • None—Specifies that no option is selected. • OFF—Specifies that the option is disabled. • Pool—Specifies the NAT pool. • Interface—Specifies the outgoing option.
Install On	Specifies the device on which the rulebase is installed.	—

Configuring the Interface (NSM Procedure)

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 **Security > Nat > Interface**.
4. Add or modify the interface settings as specified in [Table 129 on page 210](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the interface parameters.

Table 129: Interface Configuration Details

Option	Function	Your Action
interface		
Name	Specifies the name of the interface.	Select the name from the drop-down list.
Comment	Supplies a descriptive comment for the interface.	(Optional) Enter a comment.
Allow Incoming	Allows the interface pool to support the incoming traffic.	Select the Allow Incoming check box to enable this feature.
interface > Proxy Arp		
Comment	Supplies a descriptive comment for the proxy Address Resolution Protocol (ARP).	(Optional) Enter a comment.
interface > Proxy Arp > Address		
Name	Specifies the address prefix.	Enter the address prefix.

Table 129: Interface Configuration Details (*continued*)

Option	Function	Your Action
Comment	Supplies a descriptive comment for the address prefix. This is optional.	Enter a comment.
interface > Proxy Arp > Address Range		
Low	Specifies the lower limit of the address range.	Enter the lower limit of the address range.
High	Specifies the upper limit of the address range.	Enter the upper limit of the address range.
Comment	Supplies a descriptive comment for the address range.	(Optional) Enter a comment.
interface > Source Nat		
Comment	Supplies a descriptive comment for the source NAT.	(Optional) Enter a comment.
interface > Source Nat > Pool > pool		
Name	Specifies the pool name.	Enter the pool name.
Comment	Supplies a descriptive comment for the source NAT pool.	(Optional) Enter a comment.
Host Address Low	Specifies the lower limit of the host address.	Enter the lower limit of the host address.
No Port Translation	Specifies that the port translation is not performed.	Select the No Port Translation check box to enable this feature.
Allow Incoming	Allows the pool to support incoming traffic.	Select the Allow Incoming check box to enable this feature.
interface > Source Nat > Pool > pool > Address		
Name	Specifies the address prefix.	Enter the address prefix.
Comment	Supplies a descriptive comment for the address.	(Optional) Enter a comment.
interface > Source Nat > Pool > pool > Address Range		
Low	Specifies the lower limit of the address range.	Enter the lower limit of the address range.
High	Specifies the upper limit of the address range.	Enter the upper limit of the address range.
Comment	Supplies a descriptive comment for the address range.	(Optional) Enter a comment.
interface > Source Nat > Pool > pool > Overflow Pool		

Table 129: Interface Configuration Details (*continued*)

Option	Function	Your Action
Comment	Supplies a descriptive comment for the overflow pool.	(Optional) Enter a comment.
interface > Source Nat > Pool > pool > Overflow Pool > Pool Name		
None	Specifies that neither the pool-name or the interface options are enabled.	Select the option.
pool-name	Specifies the overflow pool name.	Select the option and enter the pool name.
interface	Specifies the overflow pool interface.	Select the option.
interface > Static Nat		
Name	Specifies the name of the static NAT.	Enter the mapped address.
Comment	Supplies a descriptive comment for the static NAT.	(Optional) Enter a comment.
Host	Specifies the host address.	Enter the host address.
Virtual Router	Specifies the virtual router to search route to host address.	Select the virtual router from the list.

Configuring a Proxy Address Resolution Protocol (NSM Procedure)

To a configure proxy Address Resolution Protocol (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 a proxy ARP.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Nat > Proxy Arp**.
4. Configure the options as specified in [Table 130 on page 212](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the proxy ARP options.

Table 130: Proxy ARP Configuration Details

Option	Function	Your Action
General		
Comment	Supplies a descriptive comment for the proxy ARP.	(Optional) Enter a comment.

Table 130: Proxy ARP Configuration Details (*continued*)

Option	Function	Your Action
Interface > interface		
Name	Specifies the proxy ARP interface name.	Enter the proxy ARP interface name.
Comment	Supplies a descriptive comment for the proxy ARP interface.	(Optional) Enter a comment.
Interface > interface > Address		
Name	Specifies the proxy ARP address.	Enter the proxy ARP interface address or address range.
Comment	Supplies a descriptive comment for the proxy ARP interface address.	(Optional) Enter a comment.
Interface > interface > Address > To		
Comment	Supplies a descriptive comment for the upper limit of the address range.	(Optional) Enter a comment.
IPAddr	Specifies the upper limit of the address range.	Enter the upper limit of the address range.

Configuring a Source (NSM Procedure)

To configure a source:

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 source.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Nat > Source**.
4. Configure the options as specified in [Table 131 on page 213](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the source options.

Table 131: Source Configuration Details

Option	Function	Your Action
General		
Comment	Supplies a descriptive comment for source configuration.	(Optional) Enter a comment.

Table 131: Source Configuration Details (*continued*)

Option	Function	Your Action
Address Persistent	Allows the source address to maintain the same translation.	Select the Address Persistent check box to enable this feature.
General > Pool Utilization Alarm		
Comment	Supplies a descriptive comment for the pool utilization alarm.	(Optional) Enter a comment.
Raise Threshold	Raises the threshold for the pool utilization alarm.	Set the threshold. Range: 50 - 100.
Clear Threshold	Specifies the threshold for the pool utilization alarm.	Set the threshold. Range: 40 - 100.
General > Port Randomization		
Comment	Supplies a descriptive comment for port randomization.	(Optional) Enter a comment.
Disable	Disables the source NAT port randomization.	Select the Disable check box to enable this feature.
General > Interface		
Comment	Supplies a descriptive comment for the port overloading interface.	(Optional) Enter a comment.
Off	Turns off the interface port overloading.	Select the Off check box to enable this feature.
Pool > General		
Name	Specifies the pool name.	Enter the pool name.
Comment	Supplies a descriptive comment for the pool. This is optional.	Enter a comment.
Pool > Routing Instances		
Comment	Supplies a descriptive comment for the routing instances.	(Optional) Enter a comment.
Ri Name	Specifies the name of the routing instance.	Select the name from the list.
Pool > Address > IP Address		
IP Address	Specifies the IP address or address range.	Enter the IP address or address range.
Comment	Supplies a descriptive comment for the IP address.	(Optional) Enter a comment.
Pool > Address > End of Range		

Table 131: Source Configuration Details (*continued*)

Option	Function	Your Action
Comment	Supplies a descriptive comment for the upper limit of the address range. This is optional.	Enter a comment.
IPAddr	Specifies the upper limit of the address range.	Enter the upper limit of the address range.
Pool > Host Address Base		
Comment	Supplies a descriptive comment for the host address base.	(Optional) Enter a comment.
IPAddr	Specifies the base IP address.	Enter the base IP address.
Pool > Port Translation > General		
Comment	Supplies a descriptive comment for the port translation.	(Optional) Enter a comment.
Pool > Port Translation > No Translation > General		
No Translation	Specifies that the port translation is not enabled.	Select the No Translation check box to enable this feature.
Pool > Port Translation > No Translation > Translation		
From	Specifies the lower limit of the port range.	Enter the following: <ul style="list-style-type: none"> Comment—A descriptive comment for the lower limit of the port range. Low—The lower limit of the port range. Range: -2147483648 - 2147483647.
To	Specifies the upper limit of the port range.	Enter the following: <ul style="list-style-type: none"> Comment—A descriptive comment for the upper limit of the port range. High—Specifies the upper limit of the port range. Range: -2147483648 - 2147483647.
Pool > Overflow Pool > General		
Comment	Supplies a descriptive comment for the overflow pool.	Enter a comment.
Pool > Overflow Pool > Pool Name		
None	Specifies that neither the pool-name nor the interface option is enabled.	Select the option.
pool-name	Specifies the overflow pool name.	Select the option and enter the pool name.

Table 131: Source Configuration Details (*continued*)

Option	Function	Your Action
interface	Specifies the interface for the overflow pool.	Select the option.

Configuring the Source Nat (NSM Procedure)

To configure source NAT:

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 source NAT.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Nat > Source Nat**.
4. Add or modify settings as specified in [Table 128 on page 209](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the source NAT settings.

Table 132: Source NAT Configuration Details

Option	Function	Your Action
source-nat		
Name	Specifies a name for the source NAT.	Enter a name.
source-nat > From		
Zone/RI/Interface	Specifies the zone, routing instance or the interface selected for the source NAT.	Select an option.
Source Address	Specifies source address of the destination NAT.	Select the option and enter the following: <ul style="list-style-type: none"> • Comment—Descriptive comment for the destination address. • Prefix—Address prefix. • Port—Port number. • Low—Lower limit of the address range. • High—Higher limit of the address range.

Table 132: Source NAT Configuration Details (*continued*)

Option	Function	Your Action
Source Address Name	Specifies source address name of the destination NAT.	Select the option and enter the following: <ul style="list-style-type: none"> • Comment—Descriptive comment for the address range. • Address Object—Address object pushed to the global address book. • Port—Port number. • Low—Lower limit of the address range. • High—Higher limit of the address range.
source-nat > To		
Zone/RI/Interface	Specifies the zone, routing instance or the interface selected for the destination NAT.	Select an option.
Destination Address	Specifies destination address of the destination NAT.	Either destination address or destination address name can be used for an instance.
Destination Address Name	Specifies destination address name of the destination NAT.	Either destination address or destination address name can be used at an instance.
Destination Port	Specifies destination port number.	The port options are: <ul style="list-style-type: none"> • Low—Lower limit of the address range. • High—Higher limit of the address range.
Action		<ul style="list-style-type: none"> • None—Specifies that no option is selected. • OFF—Specifies that the option is disabled. • Pool—Specifies the NAT pool. • Interface—Specifies the outgoing option.
Install On	Specifies the device on which the rulebase is installed.	—

Configuring the Static Nat (NSM Procedure)

To configure the static NAT:

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 static NAT.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Nat > Static Nat**.
4. Add or modify settings as specified in [Table 128 on page 209](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

- **Apply**—Applies the static NAT settings.

Table 133: Static NAT Configuration Details

Option	Function	Your Action
static-nat		
Name	Specifies a name for the static NAT.	Enter a name.
Zone/RI/Interface	Specifies the zone, routing instance or the interface selected for the destination NAT.	Select an option.
Destination Address	Specifies the destination address of the destination NAT.	Either Destination Address or Destination Address Name can be used for an instance.
Destination Address Name	Specifies the destination address name of the destination NAT.	Either Destination Address or Destination Address Name can be used for an instance.
Action		
Prefix	Specifies the prefix address.	—
Prefix Name	Specifies the prefix name.	—
Install On	Specifies the device on which the rulebase is installed.	—

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 > Nat > Traceoptions**.
4. Configure the options as specified in [Table 134 on page 219](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the traceoptions settings.

Table 134: Traceoptions Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the traceoptions.	(Optional) Enter a comment.
No Remote Trace	Disables the 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 219](#)
- [Configuring Flag Options \(NSM Procedure\) on page 220](#)

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 > Nat > Traceoptions > File**.
4. Configure the file options as specified in [Table 135 on page 219](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the file settings.

Table 135: 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 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.

Table 135: 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 flag options.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Nat > Traceoptions > Flag**.
4. Add or modify setting as specified in [Table 136 on page 220](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the flag settings.

Table 136: 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.
Syslog	Specifies that the NAT flow trace files are recorded to the system log.	Select the Syslog check box to enable this feature.

Related Documentation

- [Configuring IKE \(NSM Procedure\) on page 188](#)
- [Configuring IPsec \(NSM Procedure\) on page 195](#)
- [Configuring a PKI \(NSM Procedure\) on page 201](#)

Configuring Services for J Series Services Routers and SRX Series Services Gateways

- [Configuring Captive Portal \(NSM Procedure\) on page 221](#)
- [Configuring Mobile IP \(NSM Procedure\) on page 226](#)
- [Configuring RPM \(NSM Procedure\) on page 237](#)
- [Configuring Service Interface Pools \(NSM Procedure\) on page 243](#)
- [Configuring Unified Access Control \(NSM Procedure\) on page 244](#)

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 137 on page 221](#).
5. Click one:
 - **OK** — Saves the changes.
 - **Cancel** — Cancels the modifications.
 - **Apply**—Applies the captive portal parameters.

Table 137: Captive Portal Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the captive portal. This is optional.	Enter a comment.

Table 137: 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 222](#)
- [Configuring the Interface \(NSM Procedure\) on page 223](#)
- [Configuring Traceoptions \(NSM Procedure\) on page 224](#)

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 138 on page 222](#).
6. Click one:
 - **OK** — Saves the changes.
 - **Cancel** — Cancels the modifications.
 - **Apply**—Applies the custom option parameters.

Table 138: 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 138: 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 139 on page 223](#).
5. Click one:
 - **OK** — Saves the changes.
 - **Cancel** — Cancels the modifications.

Table 139: 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 139: 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 224](#)
- [Configuring Flag Options \(NSM Procedure\) on page 225](#)

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 140 on page 225](#).
5. Click one:

- **OK** — Saves the changes.
- **Cancel** — Cancels the modifications.
- **Apply**—Applies the file settings.

Table 140: 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 141 on page 226](#).
5. Click one:
 - **OK** — Saves the changes.
 - **Cancel** — Cancels the modifications.
 - **Apply**—Applies the flag settings.

Table 141: 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 226](#)
- [Configuring the Authenticate Mechanism \(NSM Procedure\) on page 227](#)
- [Configuring Dynamic Home Assignment \(NSM Procedure\) on page 228](#)
- [Configuring the Home Agent \(NSM Procedure\) on page 229](#)
- [Configuring the Peer \(NSM Procedure\) on page 231](#)
- [Configuring Traceoptions \(NSM Procedure\) on page 234](#)

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 142 on page 227](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the access type options.

Table 142: 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 143 on page 228](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the authenticate options.

Table 143: 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 144 on page 228](#).
9. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the Nai options.

Table 144: 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 229](#)
- [Configuring Pool Match Order \(NSM Procedure\) on page 230](#)
- [Configuring the Virtual Network \(NSM Procedure\) on page 230](#)

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 145 on page 230](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the enable service options.

Table 145: 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 146 on page 230](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the pool match order options.

Table 146: 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 147 on page 231](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the virtual network options.

Table 147: 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. NOTE: 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 148 on page 232](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 148: 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 148: 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 148: 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 149 on page 235](#).
5. Click one:
 - **OK** — Saves the changes.
 - **Cancel** — Cancels the modifications.
 - **Apply**—Applies the traceoptions settings.

Table 149: 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 235](#)
- [Configuring Flag \(NSM Procedure\) on page 236](#)

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 150 on page 236](#).
5. Click one:
 - **OK** — Saves the changes.
 - **Cancel** — Cancels the modifications.
 - **Apply**—Applies the file options.

Table 150: 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 151 on page 236](#).
5. Click one:
 - **OK** — Saves the changes.
 - **Cancel** — Cancels the modifications.
 - **Apply**—Applies the flag options.

Table 151: 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 152 on page 237](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the RPM options.

Table 152: 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 237](#)
- [Configuring Probe \(NSM Procedure\) on page 239](#)
- [Configuring Probe Server \(NSM Procedure\) on page 242](#)

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 153 on page 238](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the BGP parameters.

Table 153: 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 238](#)

[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 154 on page 239](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the routing instances options.

Table 154: 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 155 on page 239](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the probe options.

Table 155: 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 155: 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 155: 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 155: 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 156 on page 242](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the probe server settings.

Table 156: 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 156: 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 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 157 on page 243](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the service interface pool options.

Table 157: Service Interface Pools Configuration Details

Option	Function	Your Action
Name	Specifies the service interface pool name.	Enter a name.
Comment	Specifies the comment for the service interface pool.	Enter a comment.
pool > Interface		
Name	Specifies the services interface name.	Enter a name.

Table 157: Service Interface Pools Configuration Details (*continued*)

Option	Function	Your Action
Comment	Specifies the comment for the services interface.	Enter a comment.

Related Documentation

- [Configuring Captive Portal \(NSM Procedure\) on page 221](#)
- [Configuring Mobile IP \(NSM Procedure\) on page 226](#)
- [Configuring RPM \(NSM Procedure\) on page 237](#)
- [Configuring Unified Access Control \(NSM Procedure\) on page 244](#)

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 158 on page 244](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the UAC options.

Table 158: 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 158: 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 245](#)
- [Configuring Traceoptions \(NSM Procedure\) on page 246](#)

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 159 on page 245](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the infranet controller options.

Table 159: 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 159: 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 160 on page 246](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 160: 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.

Configuring SNMP for Network Management in J Series Services Routers and SRX Series Services Gateways

- [Configuring Basic System Identification for SNMP \(NSM Procedure\) on page 247](#)
- [Configuring SNMP Communities \(NSM Procedure\) on page 248](#)
- [Configuring SNMP Trap Groups \(NSM Procedure\) on page 250](#)
- [Configuring SNMP Views \(NSM Procedure\) on page 252](#)
- [Configuring Client Lists \(NSM Procedure\) on page 253](#)
- [Configuring the SNMP Local Engine ID \(NSM Procedure\) on page 255](#)
- [Configuring SNMP Health Monitoring \(NSM Procedure\) on page 256](#)
- [Configuring the Interfaces on Which SNMP Requests Can Be Accepted \(NSM Procedure\) on page 258](#)
- [Configuring the SNMP Commit Delay Timer \(NSM Procedure\) on page 259](#)
- [Configuring SNMP RMON Alarms and Events \(NSM Procedure\) on page 260](#)
- [Enabling SNMP Access over Routing Instances \(NSM Procedure\) on page 264](#)
- [Configuring Tracing of SNMP Activity \(NSM Procedure\) on page 266](#)
- [Configuring SNMP Trap Options \(NSM Procedure\) on page 268](#)
- [Configuring SNMPv3 \(NSM Procedure\) on page 270](#)

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 161 on page 248](#).
5. Click one:

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

Table 161: 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).
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 248](#)
- [Configuring SNMP Trap Groups \(NSM Procedure\) on page 250](#)
- [Configuring SNMP Views \(NSM Procedure\) on page 252](#)

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 162 on page 249](#).
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 162: 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 162: 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 \(NSM Procedure\) on page 253](#)

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 163 on page 251](#).
8. Click one:
 - **OK**—To save the changes.
 - **Cancel**—To cancel the modifications.
 - **Apply**—To apply the SNMP settings.

Table 163: 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 247](#)
 - [Configuring SNMP Communities \(NSM Procedure\) on page 248](#)
 - [Configuring SNMP Views \(NSM Procedure\) on page 252](#)

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 164 on page 252](#).
8. Click one:
 - **OK**—To save the changes.
 - **Cancel**—To cancel the modifications.
 - **Apply**—To apply the SNMP settings.

Table 164: 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 164: Configuring SNMP View Fields (*continued*)

Option	Function	Your Action
Include or Exclude	Specifies whether the view includes or excludes the set of MIB objects.	<p>Select exclude to exclude the subtree of MIB objects represented by the specified OID.</p> <p>Select include to include the subtree of MIB objects represented by the specified OID.</p>

Related Documentation

- [Configuring Basic System Identification for SNMP \(NSM Procedure\) on page 247](#)
- [Configuring SNMP Communities \(NSM Procedure\) on page 248](#)
- [Configuring SNMP Trap Groups \(NSM Procedure\) on page 250](#)

Configuring Client Lists (NSM Procedure)

You can configure a group of SNMP clients as a client list by providing either the IPv4 or IPv6 addresses for the individual clients that you want to assign to this client list. You can then specify that the members of the list be authorized to use a particular SNMP community. See [“Configuring SNMP Communities \(NSM Procedure\)” on page 248](#) for information about adding a client to a community. If a community is not configured with such specific client addresses in client lists as authorized, then all SNMP clients using this community string are authorized by default to access the device.

To configure client lists 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 **Client List**.
6. Click the **Add** or **Edit** icon.
7. Enter the parameters as specified in [Table 165 on page 254](#).
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 165: Configuring Client List Fields

Option	Function	Your Action
Name	<p>Specifies the names of the client list that you are configuring to have SNMP access privileges.</p> <p>Any SNMP requests entering the device from client lists other than the ones listed for the community are discarded.</p>	Enter a name for the client list.
Comment	Specifies the comment for the client list.	Enter the comment.
Client Address List	Specifies the addresses of SNMP clients that are authorized to access this device.	<ol style="list-style-type: none"> Click the New button or select a client address and click the Edit button. Configure the following to create and define a client address list: <ul style="list-style-type: none"> Name—Enter an IPv4 or IPv6 address for each client. Comment—Enter a comment for the IPv4 or IPv6 address you specified. Restrict—Select this check box to deny the specified SNMP client list access to the device. If you leave the Restrict check box cleared by default, access is permitted for this particular client list.

Related Documentation

- [Configuring SNMP Communities \(NSM Procedure\) on page 248](#)

Configuring the SNMP Local Engine ID (NSM Procedure)

You can configure a local engine identifier (engine ID) as the administratively unique ID of an SNMPv3 engine. The local engine ID is used only for identifying an SNMPv3 engine and not for addressing the engine. An engine ID has two parts: prefix and suffix. The prefix is formatted according to the specifications defined in RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*. You can specify the suffix to be generated from the media access control (MAC) address of the management interface.



NOTE: SNMPv3 authentication and encryption keys are generated based on the associated passwords and the engine ID. If you configure or change the engine ID, you must commit the new engine ID before you configure SNMPv3 users. Otherwise the keys generated from the configured passwords are based on the previous engine ID.

To configure a local engine ID for an SNMPv3 engine 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 **Engine Id**.
6. Enter the parameters as specified in [Table 166 on page 255](#).
7. 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 166: Configuring Engine Id Fields

Option	Function	Your Action
Comment	Specifies the comment for the engine ID.	Enter a comment.

Table 166: Configuring Engine Id Fields (*continued*)

Option	Function	Your Action
Use Mac Address	Specifies whether or not the SNMP engine ID is generated from the MAC address of the management interface on the device.	<ol style="list-style-type: none"> Expand the Engine Id tree and select Use Mac Address. Select an option for engine ID generation: <ul style="list-style-type: none"> None—The SNMP engine ID does not use the MAC address. use-mac-address—The SNMP engine ID is generated from the MAC address of the management interface on the device. use-default-ip-address—The engine ID suffix is generated from the default IP address of the management interface. local—The engine ID suffix is generated from the local IP address of the management interface. <p>For the engine ID, we recommend using the IP address of the device or using the MAC address of fxp0 or me0 if the device has only one Routing Engine.</p>

Related Documentation

- [Configuring SNMPv3 \(NSM Procedure\) on page 270](#)

Configuring SNMP Health Monitoring (NSM Procedure)

You can use SNMP health monitoring to minimize user configuration requirements. Health monitoring is a notification system that extends the RMON alarm infrastructure to provide predefined monitoring for a selected set of object instances (for file system usage, CPU usage, and memory usage) and includes support for unknown or dynamic object instances (such as JUNOS Software processes).

To configure health monitoring for SNMP in NSM:

- In the navigation tree, select **Device Manager > Devices**.
- In the **Devices** list, double-click the device to select it.
- Click the **Configuration** tab.
- In the configuration tree, expand **SNMP**.
- Select **Health Monitor**.
- Select the **Enable Feature** check box.
- Enter the parameters as specified in [Table 167 on page 257](#).
- 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 167: Configuring Health Monitor Fields

Option	Function	Your Action
Comment	Specifies the comment for the health monitoring configuration.	Enter a comment.
Interval	Specifies the interval. The interval represents the period of time, in seconds, over which the object instance is sampled. The sample value is then compared with the rising and falling threshold values.	Specify the interval between samples, in seconds. You can enter a value from 1 through 2147483647. The default is 300.
Rising Threshold	Specifies the upper threshold as a percentage of the maximum possible value for the monitored variable. When the current sampled value is greater than or equal to this threshold and the value at the last sampling interval is less than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is greater than or equal to this threshold. After a rising event is generated, another rising event is not generated until the sampled value falls below this threshold and reaches the falling threshold.	Enter the rising threshold value. You can enter a value from 1 through 100. The default value is 90.
Falling Threshold	Specifies the lower threshold as a percentage of the maximum possible value for the monitored variable. When the current sampled value is less than or equal to this threshold and the value at the last sampling interval is greater than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is less than or equal to this threshold. After a falling event is generated, another falling event is not generated until the sampled value rises above this threshold and reaches the rising threshold.	Enter the falling threshold value. You can enter a value from 0 through 100. The default value is 80.

Table 167: Configuring Health Monitor Fields (*continued*)

Option	Function	Your Action
Idp	Specifies that the enterprise-specific IDP MIB extends SNMP support to the key monitoring and threshold-crossing traps.	<ol style="list-style-type: none"> 1. Expand the Health Monitor tree and select Idp. 2. Click the New button or select an interface and click the Edit button. 3. Enter the comment, interval, and the rising and falling threshold values.

Related Documentation

- [Configuring SNMP RMON Alarms and Events \(NSM Procedure\) on page 260](#)

Configuring the Interfaces on Which SNMP Requests Can Be Accepted (NSM Procedure)

You can limit the access of SNMP requests through specific interfaces by configuring the interfaces on which SNMP requests can be accepted. If you do not configure specific interfaces, SNMP requests entering the device through any interface are accepted, because by default, all device interfaces have SNMP access privileges.

To configure interfaces on which SNMP requests can be accepted 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 **Interface**.
6. Enter the parameters as specified in [Table 168 on page 259](#).
7. 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 168: Configuring Interface Fields

Option	Function	Your Action
Interface	Specifies the name for the specific interface configuration.	<ol style="list-style-type: none"> 1. Click the New button or select an interface and click the Edit button. 2. Enter the names of one or more logical interfaces.

Related Documentation • [Configuring SNMP Communities \(NSM Procedure\) on page 248](#)

Configuring the SNMP Commit Delay Timer (NSM Procedure)

You can configure the SNMP commit delay timer to specify the length of time between when a device first receives an SNMP nonvolatile Set request and when the commit is requested for the candidate configuration. If the device receives new SNMP Set requests within this time, the commit delay timer resets to the configured time. If the device does not receive new SNMP Set requests within this time, the candidate configuration is committed and the JUNOScript session closes (the configuration lock is released). If the device receives a new SNMP Set request while the candidate configuration is being committed, the SNMP Set request is rejected and an error notification is generated.

To configure the SNMP commit delay timer for nonvolatile requests 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 **Nonvolatile**.
6. Enter the parameters as specified in [Table 169 on page 260](#).
7. 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 169: Configuring Nonvolatile Fields

Option	Function	Your Action
Comment	Specifies the comment for the nonvolatile commit delay configuration.	Enter a comment.
Commit Delay	Specifies the delay time between an affirmative SNMP Set reply and the start of commit.	Specify the delay time, in seconds. The default value is 5.

Related Documentation

- [Configuring the Interfaces on Which SNMP Requests Can Be Accepted \(NSM Procedure\) on page 258](#)

Configuring SNMP RMON Alarms and Events (NSM Procedure)

You can configure SNMP remote monitoring (RMON) alarms and events to monitor integer-valued MIB objects, standard or enterprise-specific, on the device. You can set the alarm values against thresholds and trigger events when the thresholds are crossed.

To configure the SNMP RMON alarms and events 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 **Rmon**.
6. Enter the parameters as specified in [Table 170 on page 261](#).
7. 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 170: Configuring Rmon Fields

Option	Function	Your Action
Comment	Specifies the comment for the RMON configuration.	Enter the comment.

Table 170: Configuring Rmon Fields (*continued*)

Option	Function	Your Action
Alarm	Specifies the attributes of the RMON alarm entry. An alarm entry monitors the value of a MIB variable. You can configure how often the value is sampled, the type of sampling to perform, and what event to trigger if a threshold is crossed.	<ol style="list-style-type: none"> 1. Expand the Rmon tree and select Alarm. 2. Click the New button or select a client address and click the Edit button. 3. Configure the following to create and define an RMON alarm entry: <ul style="list-style-type: none"> • Name—Enter a name for the alarm entry. • Comment—Enter a comment for the alarm entry. • Description—Enter a text description for the alarm entry. • Interval—Enter the interval (in seconds) over which data is sampled and compared with the rising and falling thresholds. • Falling Threshold Interval—Enter the interval (in seconds) between samples when the rising threshold is crossed. After the alarm crosses the falling threshold, the regular sampling interval is used. You can enter a value from 1 through 2,147,483,647. The default is 60. • Variable—Enter the variable with which you wish to identify the MIB object that is being monitored. • Sample Type—Choose the sample type to identify the method of sampling the selected variable and calculating the value to be compared against the thresholds: <ul style="list-style-type: none"> • none • absolute-value—The value of the selected variable is compared directly with the thresholds at the end of the sampling interval. • delta-value—The value of the selected variable at the last sample is subtracted from the current value, and the difference is compared with the thresholds. • Request Type—Specify the scope of the RMON alarm: <ul style="list-style-type: none"> • get-request—Monitor a specific object instance. • walk-request—Monitor all object instances belonging to a MIB branch. • get-next-request—Monitor the next object instance after the instance specified in the configuration. • Startup Alarm—Specify the type of alarm that can be sent when this entry is first activated: <ul style="list-style-type: none"> • falling-alarm—First sample after the alarm entry becomes active is less than or equal to the falling threshold. • rising-alarm—First sample after the alarm entry becomes active is greater than or equal to the rising threshold. • rising-or-falling-alarm—First sample after the alarm entry becomes active satisfies either of the corresponding thresholds.

Table 170: Configuring Rmon Fields (*continued*)

Option	Function	Your Action
		<ul style="list-style-type: none"> • Rising Threshold—Specify the upper threshold for the sampled variable. When the current sampled value is greater than or equal to this threshold and the value at the last sampling interval is less than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is greater than or equal to this threshold and the associated startup alarm is equal to the falling alarm or the rising-or-falling alarm. After a rising event is generated, another rising event cannot be generated until the sampled value falls below this threshold and reaches the falling threshold. You can enter a value from -2,147,483,648 through 2,147,483,647. • Falling Threshold—Specify the lower threshold for the sampled variable. When the current sampled value is less than or equal to this threshold and the value at the last sampling interval is greater than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is less than or equal to this threshold and the associated startup alarm is equal to the falling alarm or the rising-or-falling alarm. After a falling event is generated, another falling event cannot be generated until the sampled value rises above this threshold and reaches the rising threshold. You can enter a value from -2,147,483,648 through 2,147,483,647. The default is 20 percent less than the rising threshold. • Rising Event Index—Specify the event entry that is triggered when a rising threshold is crossed. You can enter a value from 0 through 65,535. The default is 0. • Falling Event Index—Specify the event entry that is triggered when a falling threshold is crossed. You can enter a value from 0 through 65,535. The default is 0. • Syslog Subtag—Specify the tag to be added to the system log message. You can specify a string of not more than 80 uppercase characters as the system log tag.

Table 170: Configuring Rmon Fields (*continued*)

Option	Function	Your Action
Event	Specifies the attributes of the RMON event entry. An event entry generates a notification for an alarm entry when its rising or falling threshold is crossed. You can configure the type of notification that is generated.	<ol style="list-style-type: none"> 1. Expand the Rmon tree and select Event. 2. Click the New button or select a client address and click the Edit button. 3. Configure the following to create and define an RMON event entry: <ul style="list-style-type: none"> • Name—Enter a name for the event entry. • Comment—Enter a comment for the event entry. • Description—Enter a text description for the event entry. • Type—Specify the type of notification generated and where the event is to be logged when a threshold is crossed: <ul style="list-style-type: none"> • none • log—Adds the event entry to the logTable. • log-and-trap—Sends an SNMP trap and creates a log entry. • snmptrap—Sends an SNMP trap. • Community—Specify the trap group that is used when generating a trap. If that trap group has the rmon-alarm trap category configured, a trap is sent to all the targets configured for that trap group. The community string in the trap matches the name of the trap group. If nothing is configured, traps are sent to each group with the rmon-alarm category set.

- Related Documentation**
- [Configuring SNMP Trap Groups \(NSM Procedure\) on page 250](#)
 - [Example: Configuring SNMP Trap Groups](#)

Enabling SNMP Access over Routing Instances (NSM Procedure)

You can enable SNMP managers in routing instances other than the default routing instance to access SNMP information. You can use the SNMP routing instance access feature to create access lists to allow or deny SNMP clients in routing instances access to SNMP information. Specify the routing instance name to allow the SNMP client in a routing instance to access SNMP information. To deny the SNMP client in a routing instance access to SNMP information, restrict the routing instance name in the access list. If access rights are not configured, JUNOS Software does not allow SNMP managers from routing instances other than the default routing instance to access SNMP information.

To configure access lists for SNMP access over routing instances 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 **Routing Instance Access**.
6. Select the **Enable Feature** check box.
7. Enter the parameters as specified in [Table 171 on page 265](#).
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 171: Configuring Routing Instance Access Fields

Option	Function	Your Action
Comment	Specifies the comment for the routing instance access configuration.	Enter a comment.
Access List	Specifies addresses of client members in the access lists.	<ol style="list-style-type: none"> 1. Expand the Routing Instance Access tree and select Access List. 2. Click the New button or select an entry and click the Edit button. 3. Configure the following to create and define an access list entry for a routing instance: <ul style="list-style-type: none"> • Name—Enter a name for the access list entry. • Comment—Enter a comment for the access list entry. • Restrict—Select this check box to deny the specified SNMP client list access to the routing instance. If you leave the Restrict check box cleared by default, access is permitted for this particular list.

Related Documentation • [Configuring SNMP Communities \(NSM Procedure\) on page 248](#)

Configuring Tracing of SNMP Activity (NSM Procedure)

You can configure the `traceoptions` feature to track the activities of SNMP agents and record the information in log files. The logged error descriptions provide information you can use to solve problems faster. If this feature is not configured, JUNOS Software does not trace SNMP activities. The default tracing behavior is outlined below:

- Important activities are logged in files located in the `/var/log` directory. You cannot change the directory in which trace files are located. You can only customize other settings. Each log is named after the SNMP agent that generates it.
- When a trace file named *filename* reaches its maximum size, it is renamed *filename.0*, then *filename.1*, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. You can set the file size to be of any size from 10 KB through 1 gigabyte (GB). When the size of the trace file reaches the maximum value, it is renamed to the next consequential name. This process repeats until the maximum file number limit is reached. Then the oldest file is overwritten by the newest file. This way, new files are created once the size of each file exceeds the specified maximum file size value. The number of files can be from 2 through 1000.
- Log files can be accessed only by the user who configures the tracing operation.

To configure SNMP tracing activity 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 **Traceoptions**.
6. Enter the parameters as specified in [Table 172 on page 267](#).
7. 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 172: Configuring Traceoptions Fields

Option	Function	Your Action
Comment	Specifies the comment for the tracing configuration.	Enter a comment.
No Remote Trace	<p>Specify whether or not this tracing configuration is written on the remote host.</p> <p>JUNOS Software supports system-wide remote tracing, by which traces are written to files on the remote host To override the system-wide remote tracing configuration for a particular process, When the No Remote Trace check box is enabled, the process does local tracing.</p>	Select the No Remote Trace check box to force local tracing for this configuration.
File	Specifies the limits on the number and size of trace files.	<ol style="list-style-type: none"> Expand the Traceoptions tree and select File. Configure the following to create and define a tracing file entry: <ul style="list-style-type: none"> Comment—Enter a comment for the tracing file. Size—Specify the size limit for the trace file. Files—Specify the maximum trace file versions to be created. Access—Specify access permissions for the tracing file: <ul style="list-style-type: none"> None world-readable—Allows any user to read all log files. no-world-readable—Allows log files to be accessed only by the user who configures the tracing operation. Match—Specify a regular expression (regex) to be matched in the trace operation output.

Table 172: Configuring Traceoptions Fields (*continued*)

Option	Function	Your Action
Flag	Specifies which trace operations are to be logged. If this is not configured, only important activities are logged by default.	<ol style="list-style-type: none"> 1. Expand the Traceoptions tree and select Flag. 2. Click the New button or select a tracing flag and click the Edit button. 3. Configure the following to create and define a tracing flag entry: <ul style="list-style-type: none"> • Name—Specify the tracing flag to be used: <ul style="list-style-type: none"> • timer—Log internally generated events. • protocol-timeouts—Log SNMP response timeouts. • pdu—Log SNMP request and response packets. • varbind-error—Log variable binding errors. • routing-socket—Log routing socket calls. • interface-stats—Log physical and logical interface statistics. • subagent—Log subagent restarts. • general—Log general events. • nonvolatile-sets—Log nonvolatile SNMP set request handling. • all—Log all SNMP events. • Comment—Enter a comment for the tracing flag.

Related Documentation • [Configuring SNMP Communities \(NSM Procedure\) on page 248](#)

Configuring SNMP Trap Options (NSM Procedure)

You can configure the SNMP trap options feature to recognize the duplicate traps and to distinguish SNMPv1 traps based on the outgoing interface. This feature is helpful when some SNMP traps that come from the same device leave the device through a different outgoing interface, causing each such SNMP trap packet to have a different source address. You can set the source address of every SNMP trap packet sent by a device to be the same, regardless of the outgoing interface. You can also set the agent address of each SNMPv1 trap.

To configure the SNMP trap 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 **SNMP**.
5. Select **Trap Options**.
6. Select the **Enable Feature** check box.
7. Enter the parameters as specified in [Table 173 on page 269](#).
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 173: Configuring Trap Options Fields

Option	Function	Your Action
Comment	Specifies the comment for the SNMP trap option.	Enter the comment.
Agent Address	Specifies the agent address of all SNMPv1 traps generated by this device.	Choose the agent address: <ul style="list-style-type: none"> • None • outgoing-interface—Sets the agent address of each SNMPv1 trap to the address of the outgoing interface of that trap.
Logical System	On routers only, specifies the name of the logical system for this SNMP client. The logical system performs a subset of the actions of its parent physical device and have its own interfaces, policies, and routing instances.	<ol style="list-style-type: none"> 1. Expand the Trap Options tree and select Logical System. 2. Click the New button or select a routing instance and click the Edit button. 3. Configure the following to create and define a logical system entry: <ul style="list-style-type: none"> • Name—Specify the name of the logical system. • Comment—Enter a comment for the logical system. • Routing Instance—Configure the following to create and define a routing instance entry: <ul style="list-style-type: none"> Lo0—Choose one of the following as the source address for the trap packets: <ul style="list-style-type: none"> • lo0—The source address of the SNMP trap packets is set to the lowest loopback address configured on the interface lo0. • address—The source address of the SNMP trap packets is set to the address you specify. Enter a valid IPv4 address configured on one of the device interfaces.
Routing Instances	Specifies the routing instances for SNMPv1 and SNMPv2 trap targets. All targets configured in the trap group use these routing instances.	<ol style="list-style-type: none"> 1. Expand the Trap Options tree and select Routing Instances. 2. Click the New button or select a routing instance and click the Edit button. 3. Configure the following to create and define a routing instance entry: <ul style="list-style-type: none"> • Name—Specify the name of the routing instance. • Comment—Enter a comment for the routing instance.

Table 173: Configuring Trap Options Fields (*continued*)

Option	Function	Your Action
Source Address	Specifies the source address of every SNMP trap packet sent by this device. You can set a valid interface address as the source address for SNMP traps regardless of the outgoing interface. If the source address is not specified, the address of the outgoing interface is used as the source address.	<ol style="list-style-type: none"> 1. Expand the Trap options tree and select Routing Instances. 2. Expand the Routing Instances tree and select Source Address, or expand the Trap options tree and select Source Address directly. 3. Configure the following to create and define a source address entry: <ul style="list-style-type: none"> • Comment—Enter a comment for the source address. • Lo0—Choose one of the following as the source address for the trap packets: <ul style="list-style-type: none"> • lo0—The source address of the SNMP trap packets is set to the lowest loopback address configured on the interface lo0. • address—The source address of the SNMP trap packets is set to the address you specify. Enter a valid IPv4 address configured on one of the device interfaces.

Configuring SNMPv3 (NSM Procedure)

You can configure SNMP version 3 (SNMPv3) for message security and access control. You can configure the entries for the user-based security model (USM) that SNMPv3 uses for message security and the view-based access control model (VACM) that SNMPv3 uses for access control. USM specifies authentication and encryption. USM uses the concept of a user for which security parameters (levels of security, authentication, privacy protocols, and keys) are configured for both the agent and the manager. VACM specifies access-control rules.

To configure the SNMPv3 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 **SNMP**.
5. Select **V3**.
6. Enter the parameters as specified in [Table 174 on page 271](#).
7. 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 174: Configuring V3 Fields

Option	Function	Your Action
Comment	Specifies the comment for the SNMPv3 configuration.	Enter a comment.
Notify	Specifies the management targets for notifications as well as the type of notifications. Notifications can be either traps or informs.	<ol style="list-style-type: none"> Expand the V3 tree and select Notify. Click the New button or select an entry and click the Edit button. Configure the following to create and define an entry: <ul style="list-style-type: none"> Name—Specify the name for the notification. Comment—Enter the comment for the notification. Type—Choose the notification type: <ul style="list-style-type: none"> trap—Unconfirmed notifications inform—Confirmed notifications Tag—Specify a tag. Notifications are sent to all targets configured with this tag.
Notify Filter	Lists the group of MIB objects on which access is to be defined. The notify filter limits the type of traps or informs sent to the Network Security Management (NMS).	<ol style="list-style-type: none"> Expand the V3 tree and select Notify Filter. Click the New button or select an entry and click the Edit button. Configure the following to create and define an entry: <ul style="list-style-type: none"> Name—Specify the name for the notification filter. Comment—Enter the comment for the notification filter. OID—Specify an object identifier (OID) to represent a subtree of MIB objects. All MIB objects represented by this ID have the specified OID as a prefix. Specify the OID using either a sequence of dotted integers or a subtree name. <ul style="list-style-type: none"> None include—Include the subtree of MIB objects represented by the specified OID. exclude—Exclude the subtree of MIB objects represented by the specified OID.

Table 174: Configuring V3 Fields (*continued*)

Option	Function	Your Action
SNMP Community	Lists the SNMP communities authorizing the SNMPv1 or SNMPv2 clients. The access privileges associated with the configured security name define which MIB objects are available and the operations (notify, read, or write) allowed on those objects.	<ol style="list-style-type: none"> Expand the V3 tree and select SNMP Community. Configure the following to create and define an entry: <ul style="list-style-type: none"> Name—Specify the name for the SNMP community. Comment—Enter the comment for the community. Community Name—Enter the community string for the SNMPv1 or SNMPv2 community. If you do not enter a name, it is the same as the community index. Ensure that community names are unique. Security Name—Enter the name you want to use for access control. This is done to associate the community string to a security name. Context—Specify the context in which the community string is to be used. Tag—Specify the addresses of managers that are allowed to use this community string.
Target Address	Specifies the management application's address and parameters to be used in sending notifications.	<ol style="list-style-type: none"> Expand the V3 tree and select Target Address. Click the New button or select an entry and click the Edit button. Configure the following to create and define an entry: <ul style="list-style-type: none"> Name—Specify the name to be assigned to the target address. Comment—Enter a comment for the target address. Address—Enter the IPv4 or the IPv6 address of the device to receive traps or informs. <p>NOTE: Specify an address, not a hostname.</p> <ul style="list-style-type: none"> Port—Enter the UDP port number for the SNMP target. Timeout—Specify the number of seconds to wait for an inform acknowledgment. If no acknowledgment is received within the timeout period, the inform is retransmitted. The default timeout period is 15 seconds. Retry Count—Specify the maximum number of times the inform is transmitted if no acknowledgment is received. If no acknowledgment is received after the inform is transmitted the maximum number of times, the inform message is discarded. The default count is 3 times. Tag List—Specify an SNMP tag list to be used to define sets of target addresses. Address Mask—Specify an address mask to verify the source addresses for this group of target addresses. An address mask, combined with the address, defines a range of addresses. Routing Instance—Specify a routing instance for this SNMPv3 target address. Logical System—On routers only, specify the logical system group for this SNMPv3 target address. Target Parameters—Specify the message processing and security parameters to be used in sending notifications to a particular management target.

Table 174: Configuring V3 Fields (*continued*)

Option	Function	Your Action
Target Parameters	Specifies the message processing and security parameters to be used in sending notifications to a particular management target.	<ol style="list-style-type: none"> Expand the V3 tree and select Target Parameters. Click the New button or select an entry and click the Edit button. Configure the following to create and define an entry: <ul style="list-style-type: none"> Name—Specify the name to be assigned to this group of target parameters. Comment—Enter a comment for this group of target parameters. Notify Filter—Specify the notify filter to be used by this specific set of target parameters. Parameters—Configure the entries for this specific set of target parameters: <ul style="list-style-type: none"> Message Processing Model—Specify the message processing model: <ul style="list-style-type: none"> None v1—SNMPv1 message process model v2c—SNMPv2c message process model v3—SNMPv3 message process model Security Model—Specify this group's security model: <ul style="list-style-type: none"> None usm—SNMPv3 security model v1—SNMPv1 message process model v2c—SNMPv2c message process model Security Level—Specify this group's security level: <ul style="list-style-type: none"> authentication—Authentication but no encryption. none—Authentication and no encryption. privacy—Authentication and encryption. Security Name—The user name (if USM is used) or the SNMP community name (if SNMPv1 or SNMPv2c security models are used) when generating the notification.

Table 174: Configuring V3 Fields (*continued*)

Option	Function	Your Action
Usm	Specifies USM information.	<ol style="list-style-type: none"> Expand the V3 tree and select Usm. Configure the following to create and define an entry: <ul style="list-style-type: none"> Comment—Enter a comment for this USM set. Local Engine—Specify the local-engine information for USM. Assign a user associated with an SNMPv3 group. Specify the authentication type for the SNMPv3 user as MD5 or SHA. Assign the encryption algorithm: <ul style="list-style-type: none"> Advanced Encryption Standard (privayc-aes128) Triple Data Encryption Standard (privacy-3des) Data Encryption Standard (privacy-des) Configure the password used to generate the key used for encryption. Remote Engine—Enter the engine ID for the SNMP agent on the remote device where the user resides for the USM. You must do this to send inform messages to an SNMPv3 user on a remote device. The engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host. Assign a user associated with an SNMPv3 group. Assign the authentication type: <ul style="list-style-type: none"> MD5—Sets the message digest algorithm (MD5) as the authentication type. SHA—Sets the secure hash algorithm (SHA) as the authentication type. Assign the encryption algorithm: <ul style="list-style-type: none"> Advanced Encryption Standard (privayc-aes128) Triple Data Encryption Standard (privacy-3des) Data Encryption Standard (privacy-des) Configure the plain-text password used to generate the key used for encryption meeting these requirements on a device: <ul style="list-style-type: none"> The password must be at least eight characters long. The password can include alphabetic, numeric, and special characters, but not control characters.

Table 174: Configuring V3 Fields (*continued*)

Option	Function	Your Action
Vacm	Specifies the VACM information.	<ol style="list-style-type: none"> Expand the V3 tree and select Vacm. Configure the following to create and define an entry: <ul style="list-style-type: none"> Comment—Enter a comment for this VACM set. Access—Assign the security name to a group of SNMP security names that belong to the same an SNMP access policy and define the access privileges for this group. Users belonging to a particular SNMP group inherit all access privileges granted to that group. Specify a context prefix for this group or a default context prefix for all VACM entries by configuring the context security model and entering a comment for the context security model. Specify this group's security model: <ul style="list-style-type: none"> Any usm—SNMPv3 security model v1—SNMPv1 message process model v2c—SNMPv2c message process model Specify this group's security level: <ul style="list-style-type: none"> authentication—Provides authentication but no encryption. none—No authentication and no encryption. privacy—Provides authentication and encryption. Designate the level of security view access. <ul style="list-style-type: none"> Read View—Provides read access. Write View—Provides write access. Notify View—Provides notify access, in which a list of notifications is sent to each user in this group. Security To Group—Configure the group to which a specific security name belongs. Assign the security name to a group of SNMP security names that belong to the same SNMP access policy and define the access privileges for this group. Users belonging to a particular SNMP group inherit all access privileges granted to that group. Specify this group's security model: <ul style="list-style-type: none"> usm—SNMPv3 security model. v1—SNMPv1 message process model v2c—SNMPv2c message process model.

Related Documentation • [Configuring SNMP Trap Groups \(NSM Procedure\) on page 250](#)

CHAPTER 16

Configuring System for J Series Services Routers and SRX Series Services Gateways

- [Configuring Accounting \(NSM Procedure\) on page 278](#)
- [Configuring Archival \(NSM Procedure\) on page 281](#)
- [Configuring ARP \(NSM Procedure\) on page 282](#)
- [Configuring Authentication Order \(NSM Procedure\) on page 283](#)
- [Configuring Auto Configuration \(NSM Procedure\) on page 284](#)
- [Configuring a Backup Router \(NSM Procedure\) on page 285](#)
- [Configuring a Commit \(NSM Procedure\) on page 286](#)
- [Configuring Diag Port Authentication \(NSM Procedure\) on page 287](#)
- [Configuring a Domain Search \(NSM Procedure\) on page 287](#)
- [Configuring Extensions \(NSM Procedure\) on page 288](#)
- [Configuring an Inet6 Backup Router \(NSM Procedure\) on page 291](#)
- [Configuring Internet Options \(NSM Procedure\) on page 292](#)
- [Configuring Location \(NSM Procedure\) on page 294](#)
- [Configuring Login \(NSM Procedure\) on page 296](#)
- [Configuring a Name Server \(NSM Procedure\) on page 301](#)
- [Configuring PIC Console Authentication \(NSM Procedure\) on page 302](#)
- [Configuring Ports \(NSM Procedure\) on page 302](#)
- [Configuring RADIUS Options \(NSM Procedure\) on page 303](#)
- [Configuring RADIUS Server \(NSM Procedure\) on page 304](#)
- [Configuring Root Authentication \(NSM Procedure\) on page 305](#)
- [Configuring Static Host Mapping \(NSM Procedure\) on page 306](#)
- [Configuring TACACS+ Options \(NSM Procedure\) on page 307](#)
- [Configuring TACACS+ Server \(NSM Procedure\) on page 308](#)

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 278](#)
- [Configuring Events on page 280](#)
- [Configuring Traceoptions on page 280](#)

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 175 on page 279](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the destination settings.

Table 175: 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.
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.

Table 175: Destination Configuration Details (*continued*)

Option	Function	Your Action
Timeout	Specifies the request time period of the authentication server.	Set the request timeout period of the authentication server. Range: 1 - 90.
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 176 on page 281](#).
7. Click one:

- **OK**—Saves the changes.
- **Cancel**—Cancels the modifications.
- **Apply**—Applies the traceoptions settings.

Table 176: 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 281](#)
- [Configuring ARP \(NSM Procedure\) on page 282](#)
- [Configuring Auto Configuration \(NSM Procedure\) on page 284](#)

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 177 on page 282](#).
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the archival configuration settings.

Table 177: 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 278](#)
- [Configuring ARP \(NSM Procedure\) on page 282](#)
- [Configuring Auto Configuration \(NSM Procedure\) on page 284](#)

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 178 on page 283](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the ARP configuration settings.

Table 178: 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 281](#)
- [Configuring Accounting \(NSM Procedure\) on page 278](#)
- [Configuring Auto Configuration \(NSM Procedure\) on page 284](#)

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 43](#)
- [Configuring TACACS+ Authentication \(NSM Procedure\) on page 44](#)
- [Configuring User Access \(NSM Procedure\) on page 46](#)

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 179 on page 285](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the auto configuration parameters.

Table 179: 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.
Comment	Supplies a descriptive comment for the trace flag.	(Optional) Enter a comment.

Related Documentation

- [Configuring ARP \(NSM Procedure\) on page 282](#)
- [Configuring Archival \(NSM Procedure\) on page 281](#)
- [Configuring Accounting \(NSM Procedure\) on page 278](#)

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 45](#)
- [Configuring Auto Configuration \(NSM Procedure\) on page 284](#)
- [Configuring a Commit \(NSM Procedure\) on page 286](#)

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 287](#)
- [Configuring a Domain Search \(NSM Procedure\) on page 287](#)
- [Configuring a Backup Router \(NSM Procedure\) on page 285](#)

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 287](#)
- [Configuring a Backup Router \(NSM Procedure\) on page 285](#)
- [Configuring Extensions \(NSM Procedure\) on page 288](#)

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 285](#)
- [Configuring Extensions \(NSM Procedure\) on page 288](#)
- [Configuring Diag Port Authentication \(NSM Procedure\) on page 287](#)

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 289](#)
 - [Configuring Resource Limits on page 289](#)

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 180 on page 289](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the provider settings.

Table 180: 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 181 on page 290](#).
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 181: 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.
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.

Table 181: Resource Limits Configuration Details (*continued*)

Option	Function	Your Action
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 287](#)
- [Configuring Diag Port Authentication \(NSM Procedure\) on page 287](#)
- [Configuring a Commit \(NSM Procedure\) on page 286](#)

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 182 on page 291](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the Inet6 backup router settings.

Table 182: 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 292](#)
 - [Configuring Location \(NSM Procedure\) on page 294](#)
 - [Configuring Login \(NSM Procedure\) on page 296](#)

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 183 on page 292](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the internet options configuration settings.

Table 183: Internet Options Configuration Details

Option	Function	Your Action
Comment	Supplies a descriptive comment for the internet option.	(Optional) Enter a comment.
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.	Select an option. <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.	Select an option. <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.

Table 183: Internet Options Configuration Details (*continued*)

Option	Function	Your Action
None / ipip-path-mtu-discovery / no-ipip-path-mtu-discovery	Specifies that you can configure path MTU discovery for outgoing IP-IP tunnel connections.	Select an option. <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.	Select an option: <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.
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.

Table 183: Internet Options Configuration Details (*continued*)

Option	Function	Your Action
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 291](#)
- [Configuring Extensions \(NSM Procedure\) on page 288](#)
- [Configuring a Name Server \(NSM Procedure\) on page 301](#)

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 184 on page 295](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the location settings.

Table 184: 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.
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.

Table 184: Location Details (*continued*)

Option	Function	Your Action
Rack	Specifies the rack number	Enter the rack number.

Related Documentation

- [Configuring an Inet6 Backup Router \(NSM Procedure\) on page 291](#)
- [Configuring Internet Options \(NSM Procedure\) on page 292](#)
- [Configuring a Name Server \(NSM Procedure\) on page 301](#)

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 297](#)
- [Configuring Password on page 298](#)
- [Configuring Retry Options on page 299](#)
- [Configuring User on page 300](#)

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 185 on page 297](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the class settings.

Table 185: 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.
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.

Table 185: Class Configuration Details (*continued*)

Option	Function	Your Action
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 186 on page 298](#)
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the password settings.

Table 186: 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.
Maximum Length	Specifies the maximum password length size for all users.	Set the maximum password length size. Range: 20 - 128.

Table 186: Password Configuration Details (*continued*)

Option	Function	Your Action
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 187 on page 299](#)
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the retry options settings.

Table 187: 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.
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.

Table 187: Retry Options Configuration Details (*continued*)

Option	Function	Your Action
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 188 on page 300](#)
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the user settings.

Table 188: 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.
Class	Specifies the login class name.	Select a login class name from the list.

Table 188: User Configuration Details (*continued*)

Option	Function	Your Action
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 294](#)
- [Configuring Internet Options \(NSM Procedure\) on page 292](#)
- [Configuring a Name Server \(NSM Procedure\) on page 301](#)

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 296](#)
- [Configuring Location \(NSM Procedure\) on page 294](#)
- [Configuring Internet Options \(NSM Procedure\) on page 292](#)

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 301](#)
- [Configuring Login \(NSM Procedure\) on page 296](#)
- [Configuring Location \(NSM Procedure\) on page 294](#)

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 189 on page 303](#).
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 189: 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 302](#)
- [Configuring a Name Server \(NSM Procedure\) on page 301](#)
- [Configuring Login \(NSM Procedure\) on page 296](#)

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 190 on page 304](#).
7. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the radius option settings.

Table 190: 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 302](#)
- [Configuring PIC Console Authentication \(NSM Procedure\) on page 302](#)
- [Configuring a Name Server \(NSM Procedure\) on page 301](#)

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 191 on page 304](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the RADIUS server settings.

Table 191: 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 191: 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 302](#)
- [Configuring RADIUS Options \(NSM Procedure\) on page 303](#)
- [Configuring a Name Server \(NSM Procedure\) on page 301](#)

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 192 on page 306](#)
6. Click one:

- **OK**—Saves the changes.
- **Cancel**—Cancels the modifications.
- **Apply**—Applies the root authentication settings.

Table 192: 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 304](#)
- [Configuring RADIUS Options \(NSM Procedure\) on page 303](#)
- [Configuring a Name Server \(NSM Procedure\) on page 301](#)

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 193 on page 306](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the static host mapping settings.

Table 193: 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 193: 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 305](#)
- [Configuring RADIUS Server \(NSM Procedure\) on page 304](#)
- [Configuring RADIUS Options \(NSM Procedure\) on page 303](#)

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 194 on page 307](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the TACACS+ options settings.

Table 194: 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 194: 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 305](#)
- [Configuring RADIUS Server \(NSM Procedure\) on page 304](#)
- [Configuring Static Host Mapping \(NSM Procedure\) on page 306](#)

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 195 on page 308](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
 - **Apply**—Applies the TACACS+ server settings.

Table 195: 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 195: 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 307](#)
 - [Configuring RADIUS Server \(NSM Procedure\) on page 304](#)
 - [Configuring Static Host Mapping \(NSM Procedure\) on page 306](#)

Configuring J Series Services Routers and SRX Series Services Gateways for DHCP

- [Configuring the Device as a DHCP Server \(NSM Procedure\) on page 311](#)
- [Configuring the Device as a DHCP Client \(NSM Procedure\) on page 313](#)

Configuring the Device as a DHCP Server (NSM Procedure)

The Dynamic Host Configuration Protocol (DHCP) server provides a framework for passing configuration information to client hosts (such as PCs) on a TCP/IP network. A router or interface that acts as a DHCP server can allocate network IP addresses and deliver configuration settings to client hosts without user intervention. DHCP access service minimizes the overhead required to add clients to the network by providing a centralized, server-based setup. You do not have to manually create and maintain IP address assignments for clients.

To configure the device as a DHCP server for a subnet and a single client:

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 DHCP server.
3. Click the **Configuration** tab. In the configuration tree, select **System > Services > Dhcp**.
4. Add or modify DHCP settings as specified in [Table 196 on page 311](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 196: DHCP Server Configuration Details

Option	Function	Your Action
Maximum Lease Time	Specifies the maximum length of time in seconds for which a client can request and hold a lease on a DHCP server.	Select the maximum lease time.

Table 196: DHCP Server Configuration Details (*continued*)

Option	Function	Your Action
Default Lease Time	Specifies the length of time in seconds that a client holds the lease for an IP address assigned by a DHCP server. This setting is used if a lease time is not requested by the client.	Select the default lease time.
Domain Name	Specifies the name of the domain in which clients search for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified.	Enter the domain name.
Boot File	Specifies the boot file advertised to DHCP clients. After the client receives an IP address and the boot file location from the DHCP server, the client uses the boot image stored in the boot file to complete DHCP setup.	Enter the location of the boot file on the boot server. The filename can include a path name.
Boot Server	Specifies the name of the boot server advertised to DHCP clients. The client uses a boot file located on the boot server to complete DHCP setup.	Enter the address of a boot server. You must specify an IPv4 address, not a hostname.
Server Identifier	Specifies the server identifier. This is an optional setting that can be used to identify a DHCP server in a DHCP message.	Enter the IPv4 address of the server. This address must be accessible by all clients served within a specified range of addresses (based on an address pool or static binding).
Dhcp > Pool		
Name	Specifies the logical subnet address or netmask.	Enter the IP address pool range.
Low	Specifies lowest IP address in the pool that is available for dynamic address assignment.	Enter the IP address.
High	Specifies highest IP address in the pool that is available for dynamic address assignment.	Enter the IP address.
Dhcp > Domain Search		

Table 196: DHCP Server Configuration Details (*continued*)

Option	Function	Your Action
Name	Specifies the domain search suffixes to be used by the clients.	Enter the list of domain names to search. The list can contain up to 6 domain names, with a total of up to 256 characters.
Dhcp > Name Server		
Name	Defines a Domain Name System (DNS) name server.	Enter the address of the name server. To configure multiple name servers, include multiple address options.
Dhcp > Option		
Name	Specifies the ID number that indexes the option and must be unique across a DHCP server.	Select the ID number.
Flag	Specifies the option type.	Select the option type.
Dhcp > Static Binding		
Name	Specifies the MAC address of the client. This is a hardware address that uniquely identifies a client on the network.	Enter the MAC address of the client.
Dhcp > Static Binding > Fixed Address		
Name	Specifies the fixed IP address assigned to the client. Typically a client has one address assigned, but you can assign more.	Enter the fixed IP address.

Related Documentation

- [Configuring the Device as a DHCP Client \(NSM Procedure\) on page 313](#)

Configuring the Device as a DHCP Client (NSM Procedure)

A device can act as a DHCP client, receiving its TCP/IP settings and the IP address for any physical interface in any security zone from an external DHCP server. The device can also act as a DHCP server, providing TCP/IP settings and IP addresses to clients in any zone.

To configure the device as a DHCP client:

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 DHCP client.

3. Click the **Configuration** tab. In the configuration tree, select **Interfaces**.
4. Select the interface on which you want to configure DHCP client information, and select **Unit > Family > Inet > Dhcp**.
5. Click **Enable** next to Dhcp, and add or modify DHCP settings as specified in [Table 197 on page 314](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 197: DHCP Client Configuration Details

Option	Function	Your Action
Lease Time	Specifies the DHCP lease time in seconds.	Enter the DHCP lease time in seconds.
Retransmission Attempt	Specifies the number of attempts allowed to retransmit a DHCP packet.	Enter the number of attempts allowed to retransmit a DHCP packet.
Retransmission Interval	Specifies the interval allowed between retransmission attempts in seconds.	Enter the interval allowed between retransmission attempts in seconds.
Server Address	Specifies the IPv4 address of the preferred DHCP server.	Enter the IPv4 address of the preferred DHCP server.
Vendor Id	Specifies the vendor class ID for the DHCP client.	Enter the vendor class ID.
Dhcp > Client Identifier		
Ascii	Specifies the DHCP client identifier as either an ASCII or hexadecimal value.	Select the DHCP client identifier, and type the ASCII or hexadecimal value.

**Related
Documentation**

- [Configuring the Device as a DHCP Server \(NSM Procedure\) on page 311](#)

CHAPTER 18

Configuring Class of Service in J Series Services Routers and SRX Series Services Gateways

- [Configuring CoS Classifiers \(NSM Procedure\) on page 316](#)
- [Configuring CoS Code Point Aliases \(NSM Procedure\) on page 318](#)
- [Configuring CoS Drop Profile \(NSM Procedure\) on page 319](#)
- [Configuring CoS Forwarding Classes \(NSM Procedure\) on page 321](#)
- [Configuring CoS Forwarding Policy \(NSM Procedure\) on page 323](#)
- [Configuring CoS Fragmentation Maps \(NSM Procedure\) on page 324](#)
- [Configuring CoS Host Outbound Traffic \(NSM Procedure\) on page 325](#)
- [Configuring CoS Interfaces \(NSM Procedure\) on page 326](#)
- [Configuring CoS Rewrite Rules \(NSM Procedure\) on page 332](#)
- [Configuring CoS Schedulers \(NSM Procedure\) on page 335](#)
- [Configuring CoS and Applying Scheduler Maps \(NSM Procedure\) on page 336](#)
- [Configuring CoS Traffic Control Profiles \(NSM Procedure\) on page 338](#)

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 198 on page 316](#).
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 198: 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 198: 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 318](#)
- [Configuring CoS Drop Profile \(NSM Procedure\) on page 319](#)
- [Configuring CoS Forwarding Classes \(NSM Procedure\) on page 321](#)
- [Configuring CoS Interfaces \(NSM Procedure\) on page 326](#)
- [Configuring CoS Rewrite Rules \(NSM Procedure\) on page 332](#)
- [Configuring CoS Schedulers \(NSM Procedure\) on page 335](#)
- [Configuring CoS and Applying Scheduler Maps \(NSM Procedure\) on page 336](#)

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 199 on page 319](#)
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 199: 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, myl. 5. In the Bits box, type the code point—for example, 110001. 6. Click OK.

Related Documentation

- [Configuring CoS Classifiers \(NSM Procedure\) on page 316](#)
- [Configuring CoS Drop Profile \(NSM Procedure\) on page 319](#)
- [Configuring CoS Forwarding Classes \(NSM Procedure\) on page 321](#)
- [Configuring CoS Interfaces \(NSM Procedure\) on page 326](#)
- [Configuring CoS Rewrite Rules \(NSM Procedure\) on page 332](#)
- [Configuring CoS Schedulers \(NSM Procedure\) on page 335](#)
- [Configuring CoS and Applying Scheduler Maps \(NSM Procedure\) on page 336](#)

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 200 on page 320](#).
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 200: 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 200: 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 316](#)
- [Configuring CoS Code Point Aliases \(NSM Procedure\) on page 318](#)
- [Configuring CoS Forwarding Classes \(NSM Procedure\) on page 321](#)
- [Configuring CoS Interfaces \(NSM Procedure\) on page 326](#)
- [Configuring CoS Rewrite Rules \(NSM Procedure\) on page 332](#)
- [Configuring CoS Schedulers \(NSM Procedure\) on page 335](#)
- [Configuring CoS and Applying Scheduler Maps \(NSM Procedure\) on page 336](#)

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 201 on page 322](#).
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 201: 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 316](#)
- [Configuring CoS Code Point Aliases \(NSM Procedure\) on page 318](#)
- [Configuring CoS Drop Profile \(NSM Procedure\) on page 319](#)
- [Configuring CoS Interfaces \(NSM Procedure\) on page 326](#)
- [Configuring CoS Rewrite Rules \(NSM Procedure\) on page 332](#)
- [Configuring CoS Schedulers \(NSM Procedure\) on page 335](#)
- [Configuring CoS and Applying Scheduler Maps \(NSM Procedure\) on page 336](#)

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 202 on page 323](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 202: 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 202: 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 316](#)
 - [Configuring CoS Routing Instances \(NSM Procedure\)](#)
 - [Configuring Tracing Operations \(NSM Procedure\)](#)

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 203 on page 325](#).
6. Click one:

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

Table 203: 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 323](#)
- [Configuring CoS Schedulers \(NSM Procedure\) on page 335](#)
- [Configuring CoS Traffic Control Profiles \(NSM Procedure\) on page 338](#)

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 204 on page 326](#).
6. Click one:

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

Table 204: 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 321](#)
- [Configuring CoS Fragmentation Maps \(NSM Procedure\) on page 324](#)
- [Configuring CoS Traffic Control Profiles \(NSM Procedure\) on page 338](#)
- [Configuring CoS Interfaces \(NSM Procedure\) on page 326](#)

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 205 on page 327](#).
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 205: 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 205: 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 205: 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 205: 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 205: 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 316](#)
- [Configuring CoS Code Point Aliases \(NSM Procedure\) on page 318](#)
- [Configuring CoS Drop Profile \(NSM Procedure\) on page 319](#)
- [Configuring CoS Forwarding Classes \(NSM Procedure\) on page 321](#)
- [Configuring CoS Rewrite Rules \(NSM Procedure\) on page 332](#)
- [Configuring CoS Schedulers \(NSM Procedure\) on page 335](#)

- [Configuring CoS and Applying Scheduler Maps \(NSM Procedure\) on page 336](#)

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 206 on page 332](#).
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 206: 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 206: 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 206: 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 316](#)
- [Configuring CoS Code Point Aliases \(NSM Procedure\) on page 318](#)
- [Configuring CoS Drop Profile \(NSM Procedure\) on page 319](#)
- [Configuring CoS Forwarding Classes \(NSM Procedure\) on page 321](#)
- [Configuring CoS Interfaces \(NSM Procedure\) on page 326](#)
- [Configuring CoS Schedulers \(NSM Procedure\) on page 335](#)
- [Configuring CoS and Applying Scheduler Maps \(NSM Procedure\) on page 336](#)

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 207 on page 335](#).
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 207: 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.

Table 207: Configuring Schedulers (*continued*)

Task	Action
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	<ul style="list-style-type: none"> • Configuring CoS Classifiers (NSM Procedure) on page 316 • Configuring CoS Code Point Aliases (NSM Procedure) on page 318 • Configuring CoS Drop Profile (NSM Procedure) on page 319 • Configuring CoS Forwarding Classes (NSM Procedure) on page 321 • Configuring CoS Interfaces (NSM Procedure) on page 326 • Configuring CoS Rewrite Rules (NSM Procedure) on page 332 • Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 336

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 208 on page 337](#).
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 208: 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.
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.

Table 208: Assigning Forwarding Classes to Output Queues (*continued*)

Task	Action
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 316](#)
- [Configuring CoS Code Point Aliases \(NSM Procedure\) on page 318](#)
- [Configuring CoS Drop Profile \(NSM Procedure\) on page 319](#)
- [Configuring CoS Forwarding Classes \(NSM Procedure\) on page 321](#)
- [Configuring CoS Interfaces \(NSM Procedure\) on page 326](#)
- [Configuring CoS Rewrite Rules \(NSM Procedure\) on page 332](#)
- [Configuring CoS Schedulers \(NSM Procedure\) on page 335](#)

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 209 on page 339](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 209: 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 319](#)
- [Configuring CoS Host Outbound Traffic \(NSM Procedure\) on page 325](#)
- [Configuring CoS Routing Instances \(NSM Procedure\)](#)
- [Configuring CoS Translation Table \(NSM Procedure\)](#)

Configuring Event Options in J Series Services Routers and SRX Series Services Gateways

- [Configuring Event Script \(NSM Procedure\) on page 341](#)
- [Generating Internal Events \(NSM Procedure\) on page 342](#)
- [Configuring Event Policy \(NSM Procedure\) on page 343](#)
- [Configuring Event Policy Tracing Operations \(NSM Procedure\) on page 346](#)

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 210 on page 341](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 210: 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.

Table 210: Event Script Configuration Details (*continued*)

Task	Your Action
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 \(NSM Procedure\)](#)
- [Generating Internal Events \(NSM Procedure\) on page 342](#)
- [Configuring Event Policy \(NSM Procedure\) on page 343](#)
- [Configuring Event Policy Tracing Operations \(NSM Procedure\) on page 346](#)

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 211 on page 343](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 211: 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 \(NSM Procedure\)](#)
- [Configuring Event Script \(NSM Procedure\) on page 341](#)
- [Configuring Event Policy \(NSM Procedure\) on page 343](#)
- [Configuring Event Policy Tracing Operations \(NSM Procedure\) on page 346](#)

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 212 on page 344](#).
6. Click one:

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

Table 212: 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 212: 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)
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 212: 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 \(NSM Procedure\)](#)
- [Configuring Event Script \(NSM Procedure\) on page 341](#)
- [Generating Internal Events \(NSM Procedure\) on page 342](#)
- [Configuring Event Policy Tracing Operations \(NSM Procedure\) on page 346](#)

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 213 on page 347](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 213: 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 \(NSM Procedure\)](#)
- [Configuring Event Script \(NSM Procedure\) on page 341](#)
- [Generating Internal Events \(NSM Procedure\) on page 342](#)
- [Configuring Event Policy \(NSM Procedure\) on page 343](#)

CHAPTER 20

Configuring Firewall in J Series Services Routers and SRX Series Services Gateways

- [Configuring the Firewall Filter for Any Family Type \(NSM Procedure\) on page 349](#)
- [Configuring the Firewall Filter for Bridge Family Type \(NSM Procedure\) on page 351](#)
- [Configuring the Firewall Filter for Ccc Family Type \(NSM Procedure\) on page 353](#)
- [Configuring Filters for inet Family Type \(NSM Procedure\) on page 355](#)

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 214 on page 350](#).
5. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 214: 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 351](#)

- [Configuring the Firewall Filter for Ccc Family Type \(NSM Procedure\) on page 353](#)
- [Configuring Filters for inet Family Type \(NSM Procedure\) on page 355](#)

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 215 on page 351](#).
5. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 215: 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 215: 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. 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. 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 349](#)
- [Configuring the Firewall Filter for Ccc Family Type \(NSM Procedure\) on page 353](#)

- [Configuring Filters for inet Family Type \(NSM Procedure\) on page 355](#)
- [Configuring Filters for inet6 Family Type \(NSM Procedure\)](#)
- [Configuring the Firewall Filter for MPLS Family Type \(NSM Procedure\)](#)

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 216 on page 353](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 216: 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 216: 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 Ip property, Loss Priority, and User Vlan-Ip 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 351](#)
- [Configuring the Firewall Filter for MPLS Family Type \(NSM Procedure\)](#)
- [Configuring the Firewall Filter for VPLS Family Type \(NSM Procedure\)](#)

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 355](#)
- [Configuring Prefix-specific Actions \(NSM Procedure\) on page 357](#)
- [Configuring Service Filters \(NSM Procedure\) on page 358](#)
- [Configuring Simple Filters \(NSM Procedure\) on page 359](#)

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 217 on page 355](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 217: 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 217: 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 217: 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 218 on page 358](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 218: 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 219 on page 358](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 219: 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 219: 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 220 on page 360](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 220: 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 Application Layer Gateways in J Series Services Routers and SRX Series Services Gateways

- [Configuring H.323 ALG \(NSM Procedure\) on page 361](#)
- [Configuring SIP ALG \(NSM Procedure\) on page 363](#)
- [Configuring SCCP ALG \(NSM Procedure\) on page 366](#)
- [Configuring MGCP ALG \(NSM Procedure\) on page 368](#)
- [Enabling or Disabling ALGs \(NSM Procedure\) on page 371](#)

Configuring H.323 ALG (NSM Procedure)

The H.323 standard is a legacy VoIP protocol defined by the ITU-T. H.323 consists of a suite of protocols (such as H.225.0 and H.245) that are used for call signaling and call control for VoIP.

To configure H.323 ALG:

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 H.323 ALG.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Alg > H323**.
4. Add or modify settings as specified in [Table 221 on page 361](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 221: H.323 ALG Configuration Details

Option	Function	Your Action
Endpoint Registration Timeout	Controls how long entries remain in the NAT table.	Enter a value between 10 and 50,000 seconds.

Table 221: H.323 ALG Configuration Details (*continued*)

Option	Function	Your Action
Media Source Port Any	Allows media traffic from any port number. By default, this feature is disabled. When disabled, the device allows a temporary opening, or pinhole, in the firewall as needed for media traffic.	Select this option to enable traffic from any port number.
Threshold	Limits the rate per second at which RAS requests to the gatekeeper are processed. Messages exceeding the threshold are dropped. This feature is disabled by default.	Enter the value for the message flood gatekeeper threshold.
Permit NAT Applied	<p>Specifies how unidentified H.323 messages are handled by the device. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown H.323 (unsupported) messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped.</p> <p>This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing.</p>	Select this option to permit unidentified H.323 messages. By default, unknown (unsupported) messages are dropped.

Table 221: H.323 ALG Configuration Details (*continued*)

Option	Function	Your Action
Permit Routed	Specifies that unknown messages be allowed to pass if the session is in Route mode. (Sessions in Transparent mode are treated as Route mode.)	Select this option.

Related Documentation

- [Configuring SIP ALG \(NSM Procedure\) on page 363](#)
- [Configuring SCCP ALG \(NSM Procedure\) on page 366](#)
- [Configuring MGCP ALG \(NSM Procedure\) on page 368](#)
- [Enabling or Disabling ALGs \(NSM Procedure\) on page 371](#)

Configuring SIP ALG (NSM Procedure)

SIP is an IETF-standard protocol for initiating, modifying, and terminating multimedia sessions over the Internet. Such sessions might include conferencing, telephony, or multimedia, with features such as instant messaging and application-level mobility in network environments.

To configure SIP ALG:

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 SIP ALG.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Alg > Sip**.
4. Add or modify settings as specified in [Table 222 on page 363](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 222: SIP ALG Configuration Details

Option	Function	Your Action
C Timeout	Specifies the INVITE transaction timeout at the proxy, in minutes. Because the SIP ALG is in the middle, instead of using the INVITE transaction timer value B (which is $(64 * T1) = 32$ seconds), the SIP ALG gets its timer value from the proxy.	Select a value between 3 and 10 minutes. The default is 3.

Table 222: SIP ALG Configuration Details (*continued*)

Option	Function	Your Action
Inactive Media Timeout	Specifies the maximum length of time (in seconds) a call can remain active without any media (RTP or RTCP) traffic within a group. Each time an RTP or RTCP packet occurs within a call, this timeout resets. When the period of inactivity exceeds this setting, the temporary openings (pinholes) in the firewall SIP ALG opened for media are closed. Note that upon timeout, while resources for media (sessions and pinholes) are removed, the call is not terminated.	Select a value between 10 and 2,550 seconds. The default is 120 seconds.
Maximum Call Duration	Sets the absolute maximum length of a call. When a call exceeds this parameter setting, the SIP ALG tears down the call and releases the media sessions.	Select a value between 3 and 7,200 minutes. The default is 720 minutes.
T1 Interval	Specifies the roundtrip time estimate (in seconds) of a transaction between endpoints. Because many SIP timers scale with the T1-Interval (as described in RFC 3261), when you change the value of the T1-Interval timer, those SIP timers also are adjusted.	Select a value between 500 and 5,000 milliseconds. The default is 500 milliseconds.
T4 Interval	Specifies the maximum time a message remains in the network. Because many SIP timers scale with the T4-Interval (as described in RFC 3261), when you change the value of the T4-Interval timer, those SIP timers also are adjusted.	Select a value between 5 and 10 seconds. The default is 5 seconds.
Disable	Enables or disables translation of the host IP address in the call-ID header. Translation is enabled by default.	Select this option to enable translation of host IP address in the call-ID header. By default, translation is enabled.

Table 222: SIP ALG Configuration Details (*continued*)

Option	Function	Your Action
Retain Hold Resource	Specifies whether the device frees media resources for a SIP ALG, even when a media stream is placed on hold.	Select this option to enable the device to retain media stream resources when the media stream is on hold. By default, media stream resources are released when the media stream is held.
Timeout	Specifies the amount of time (in seconds) to make an attack table entry for each INVITE, which is listed in the application screen.	Enter a value between 1 and 3,600 seconds.
Destination Ip	Protects servers against INVITE attacks. Configure the SIP application screen to protect the server at some or all destination IP addresses against INVITE attacks. You can include up to 16 destination IP addresses of servers to be protected.	Select None , destination-ip , or all . If you select destination-ip, enter or select an IP address.

Table 222: SIP ALG Configuration Details (*continued*)

Option	Function	Your Action
Permit NAT Applied	<p>Specifies how unidentified SIP messages are handled by the device. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown SIP (unsupported) messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped.</p> <p>This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing.</p>	Select this option to permit unidentified SIP messages. By default, unknown (unsupported) messages are dropped.
Permit Routed	Specifies that unknown messages be allowed to pass if the session is in Route mode. (Sessions in Transparent mode are treated as Route mode.)	Select this option.

Related Documentation

- [Configuring SCCP ALG \(NSM Procedure\) on page 366](#)
- [Configuring H.323 ALG \(NSM Procedure\) on page 361](#)
- [Configuring MGCP ALG \(NSM Procedure\) on page 368](#)
- [Enabling or Disabling ALGs \(NSM Procedure\) on page 371](#)

Configuring SCCP ALG (NSM Procedure)

SCCP is a protocol for call signaling. Skinny is based on a call-agent-based call-control architecture. The control protocol uses binary-coded frames encoded on TCP frames

sent to well-known TCP port number destinations to set up and tear down RTP media sessions.

To configure SCCP ALG:

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 SCCP ALG.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Alg > Sccp**.
4. Add or modify settings as specified in [Table 223 on page 367](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 223: SCCP ALG Configuration Details

Option	Function	Your Action
Inactive Media Timeout	Indicates the maximum length of time (in seconds) a call can remain active without any media (RTP or RTCP) traffic within a group. Each time an RTP or RTCP packet occurs within a call, this timeout resets. When the period of inactivity exceeds this setting, the SCCP ALG the gates opened for media are closed.	Select a value between 10 and 600 seconds.
Threshold	Protects SCCP ALG clients from flood attacks by limiting the number of calls they attempt to process.	Select a value for call flood threshold from 2 to 1,000.

Table 223: SCCP ALG Configuration Details (*continued*)

Option	Function	Your Action
Permit NAT Applied	<p>Specifies how unidentified SCCP messages are handled by the device. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown SCCP (unsupported) messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped.</p> <p>This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing.</p>	Select this option to permit unidentified SCCP messages. By default, unknown (unsupported) messages are dropped.
Permit Routed	Specifies that unknown messages be allowed to pass if the session is in Route mode. (Sessions in Transparent mode are treated as Route mode.)	Select this option.

Related Documentation

- [Configuring SIP ALG \(NSM Procedure\) on page 363](#)
- [Configuring H.323 ALG \(NSM Procedure\) on page 361](#)
- [Configuring MGCP ALG \(NSM Procedure\) on page 368](#)
- [Enabling or Disabling ALGs \(NSM Procedure\) on page 371](#)

Configuring MGCP ALG (NSM Procedure)

MGCP is a text-based Application Layer Protocol used for call setup and call control between the media gateway and the media gateway controller (MGC).

To configure MGCP ALG:

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 MGCP ALG.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Alg > Mgcp**.
4. Add or modify settings as specified in [Table 224 on page 369](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 224: MGCP ALG Configuration Details

Option	Function	Your Action
Inactive Media Timeout	Specifies the maximum length of time (in seconds) a call can remain active without any media (RTP or RTCP) traffic within a group. Each time an RTP or RTCP packet occurs within a call, this timeout resets. When the period of inactivity exceeds this setting, the temporary openings (pinholes) in the firewall MGCP ALG opened for media are closed. Note that upon timeout, while resources for media (sessions and pinholes) are removed, the call is not terminated.	Select a value between 10 and 2,550 seconds. The default is 120 seconds.
Transaction Timeout	Specifies a timeout value for MGCP transactions. A transaction is a signaling message, for example, a NTFY from the gateway to the call agent or a 200 OK from the call agent to the gateway. The Juniper Networks device tracks these transactions, and clears them when they time out.	Enter a value from 3 to 50 seconds.

Table 224: MGCP ALG Configuration Details (*continued*)

Option	Function	Your Action
Maximum Call Duration	Sets the absolute maximum length of a call. When a call exceeds this parameter setting, the MGCP ALG tears down the call and releases the media sessions.	Select a value between 3 and 7,200 minutes. The default is 720 minutes.
Connection Flood Threshold	Limits the number of new connection requests allowed per media gateway per second.	Enter a value from 2 to 10,000.
Message Flood Threshold	Limits the rate per second at which message requests to the media gateway are processed. Messages exceeding the threshold are dropped by the MGCP ALG.	Enter a value from 2 to 50,000 seconds per media gateway. By default, this feature is disabled.
Permit NAT Applied	<p>Specifies how unidentified MGCP messages are handled by the Juniper Networks device. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown MGCP (unsupported) messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped.</p> <p>This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing.</p>	Select this option to permit unidentified MGCP messages. By default, unknown (unsupported) messages are dropped.

Table 224: MGCP ALG Configuration Details (*continued*)

Option	Function	Your Action
Permit Routed	Specifies that unknown messages be allowed to pass if the session is in Route mode. (Sessions in Transparent mode are treated as Route mode.)	Select this option.

Related Documentation

- [Configuring SCCP ALG \(NSM Procedure\) on page 366](#)
- [Configuring SIP ALG \(NSM Procedure\) on page 363](#)
- [Configuring H.323 ALG \(NSM Procedure\) on page 361](#)
- [Enabling or Disabling ALGs \(NSM Procedure\) on page 371](#)

Enabling or Disabling ALGs (NSM Procedure)

All ALGs are enabled by default.

To enable or disable ALGs:

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 enable or disable ALGs.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Alg**.
4. Select the check box next to an ALG as specified in [Table 225 on page 371](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 225: ALG Configuration Options

Option	Function	Your Action
Multimedia Application Protocols		
RTSP	Provides an ALG for the Real-Time Streaming Protocol.	Select the Disable check box to disable the RTSP ALG.
Basic Internet Protocols		
DNS	Provides an ALG for the Domain Name System. The DNS ALG monitors DNS query and reply packets and closes session if the	Select the Disable check box to disable the DNS ALG.

Table 225: ALG Configuration Options (*continued*)

Option	Function	Your Action
	DNS flag indicates the packet is a reply message.	
FTP	Provides an ALG for the File Transfer Protocol. The FTP ALG monitors PORT, PASV and 227 commands. It performs NAT of IP/port in the message and gate opening on the device as necessary. The FTP ALG supports FTP put and FTP get command blocking. When FTP_NO_PUT or FTP_NO_GET is set in the policy, the FTP ALG sends back a blocking command and closes the associated opened gate when either the FTP STOR or FTP RETR command is observed.	Select the Disable check box to disable the FTP ALG.
TFTP	Provides an ALG for the Trivial File Transfer Protocol. The TFTP ALG processes a TFTP packet that initiates the request and opens a gate to allow return packets from the reverse direction to the port that sends the request.	Select the Disable check box to disable the TFTP ALG.
TALK	Provides an ALG for the TALK Protocol. The TALK protocol uses UDP port 517 and port 518 for control channel connections. The talk program consists of a server and a client. The server handles client notifications and helps to establish talk sessions. There are two types of talk servers: ntalk and talkd. The TALK ALG processes packets of both ntalk and talkd formats. It also performs NAT and gate opening as necessary.	Select the Disable check box to disable the TALK ALG.

Table 225: ALG Configuration Options (*continued*)

Option	Function	Your Action
RSH	Provides an ALG for the Remote Shell. The RSH ALG handles TCP packets destined for port 514 and process the RSH port command. The RSH ALG performs NAT on the port in the port command and opens gates as necessary.	Select the Disable check box to disable the RSH ALG.
PPTP	Provides an ALG for the Point-to-Point Tunneling Protocol. The PPTP is a Layer 2 protocol that tunnels PPP data across TCP/IP networks. The PPTP client is freely available on Windows systems and is widely deployed for building VPNs.	Select the Disable check box to disable the PPTP ALG.
Database and Network Support Protocols		
SQL	Provides an ALG for the Structured Query Language. The SQLNET ALG processes an SQL TNS response frame from the server side. It parses the packet and looks for (HOST=ipaddress), (PORT=port) pattern, and performs NAT and gate opening on the client side for the TCP data channel.	Select the Disable check box to disable the SQL ALG.

**Related
Documentation**

- [Configuring H.323 ALG \(NSM Procedure\) on page 361](#)
- [Configuring SIP ALG \(NSM Procedure\) on page 363](#)
- [Configuring SCCP ALG \(NSM Procedure\) on page 366](#)
- [Configuring MGCP ALG \(NSM Procedure\) on page 368](#)

Configuring Unified Threat Management Features in J Series Services Routers and SRX Series Services Gateways

- [Configuring Server-Based Antispam \(NSM Procedure\) on page 375](#)
- [Configuring Local List Antispam \(NSM Procedure\) on page 376](#)
- [Configuring Antivirus Protection \(NSM Procedure\) on page 379](#)
- [Configuring Content Filtering \(NSM Procedure\) on page 384](#)
- [Configuring Web Filtering \(NSM Procedure\) on page 387](#)

Configuring Server-Based Antispam (NSM Procedure)

Antispam filtering allows you to use both a third-party server-based spam block list (SBL) and to optionally create your own local whitelists (benign) and blacklists (malicious) for filtering against e-mail messages. The antispam feature is not meant to replace your antispam server, but to complement it.

To configure server-based antispam:

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 server-based antispam.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Utm > Feature Profile > Anti Spam**.
4. Select **Symantec Sbl** and enable the feature.
5. Expand **Symantec Sbl** and select **Profile**.
6. Add or modify antispam profile settings as specified in [Table 226 on page 376](#).
7. Click one:
 - **New**—Adds a new profile.
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 226: Server-Based Antispam Profile Settings

Option	Function	Your Action
Name	Specifies a name for the antispam profile.	Enter a unique name for the antispam profile.
sbl-default-server	Specifies whether the Symantec SBL server is used.	Select sbl-default-server if you are using the default server. Otherwise, select None .
Spam Action	Specifies the action to be taken by the device when spam is detected.	Select one of the following: tag-subject (of e-mail), block (e-mail), tag-header (of e-mail).
Custom Tag String	Specifies the string used for identifying a message as spam.	Enter a custom string for identifying a message as spam. By default, the device uses ***SPAM*** .

Related Documentation

- [Configuring Local List Antispam \(NSM Procedure\) on page 376](#)
- [Configuring Antivirus Protection \(NSM Procedure\) on page 379](#)
- [Configuring Content Filtering \(NSM Procedure\) on page 384](#)

Configuring Local List Antispam (NSM Procedure)

This section includes the following topics:

- [Configuring Whitelist and Blacklist Entries on page 376](#)
- [Configuring a Custom URL Category List Custom Object on page 377](#)
- [Configuring Server-Based Antispam on page 377](#)
- [Configuring a UTM Policy for SNMP on page 378](#)

Configuring Whitelist and Blacklist Entries

To configure local whitelist and blacklist custom objects:

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 whitelist and blacklist custom objects.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Utm > Custom Objects**.
4. Select **Url Pattern** and click **New**.
5. Enter a unique **name** for the list.
6. Select **Value** and add a new entry.
7. Enter a **value** for the URL pattern for whitelist or blacklist antispam filtering.



NOTE: For URL pattern wildcard support, the wildcard rule is as follows: `*\.[]\?*` and you must precede all wildcard URLs with `http://`. You can only use an asterisk (*) if it is at the beginning of the URL and is followed by a dot (.). You can only use a question mark (?) at the end of the URL.

The following wildcard syntax is supported: `http://*juniper.net`, `http://www.juniper.ne?`, `http://www.juniper.n??`. The following wildcard syntax is not supported: `*juniper.net`, `www.juniper.ne?`, `http://*juniper.net`, `http://*`.

8. Click **OK** to save the changes.

Configuring a Custom URL Category List Custom Object

To configure a custom URL category list custom object:

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 URL category list custom objects.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Utm > Custom Objects**.
4. Select **Custom Url Category** and click **New**.
5. Enter a unique name for the list.
6. Select **Value** and add a new entry.
7. Enter the name of the URL pattern list you created for bypassing scanning.
8. Click **OK** to save the changes.

Configuring Server-Based Antispam

Antispam filtering allows you to use both a third-party server-based spam block list (SBL) and to optionally create your own local whitelists (benign) and blacklists (malicious) for filtering against e-mail messages. The antispam feature is not meant to replace your antispam server, but to complement it.

To configure server-based antispam:

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 server-based antispam.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Utm > Feature Profile > Anti Spam**.
4. Select **Symantec Sbl** and enable the feature.
5. Expand **Symantec Sbl** and select **Profile**.

6. Add or modify antispam profile settings as specified in [Table 227 on page 378](#).
7. Click one:
 - **New**—Adds a new profile.
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 227: Server-Based Antispam Profile Settings

Option	Function	Your Action
Name	Specifies a name for the antispam profile.	Enter a unique name for the antispam profile.
sbl-default-server	Specifies whether the Symantec SBL server is used.	Select sbl-default-server if you are using the default server. Otherwise, select None .
Spam Action	Specifies the action to be taken by the device when spam is detected.	Select one of the following: tag-subject (of e-mail), block (e-mail), tag-header (of e-mail).
Custom Tag String	Specifies the string used for identifying a message as spam.	Enter a custom string for identifying a message as spam. By default, the device uses ***SPAM*** .

Configuring a UTM Policy for SNMP

To configure a UTM policy 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 a UTM policy for SNMP.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Utm > Utm Policy**.
4. Click **New** to add a new UTM policy entry.
5. Enter a unique name for the UTM policy.
6. Select **Antispam** and enter the name of the antispam profile.
7. Click **OK** to save the changes.

Once you have configured a UTM policy for SNMP, attach the UTM policy to a security policy that you create.

Related Documentation

- [Configuring Antivirus Protection \(NSM Procedure\) on page 379](#)
- [Configuring Content Filtering \(NSM Procedure\) on page 384](#)
- [Configuring Web Filtering \(NSM Procedure\) on page 387](#)

Configuring Antivirus Protection (NSM Procedure)

This section includes the following topics:

- [Configuring a MIME Pattern List Custom Object on page 379](#)
- [Configuring a Filename Extension List Custom Object on page 379](#)
- [Configuring a URL Pattern List Custom Object on page 380](#)
- [Configuring a Custom URL Category List Custom Object on page 380](#)
- [Configuring an Antivirus Feature Profile on page 381](#)
- [Configuring a UTM Policy for Express Antivirus on page 383](#)

Configuring a MIME Pattern List Custom Object

To configure a MIME pattern list custom object:

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 MIME pattern list custom object.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Utm > Custom Objects**.
4. Select **Mime Pattern** and click **New**.
5. Enter a unique name for the list.
6. Select **Value** and add a new entry.
7. Enter a value for the MIME pattern.
8. Click **OK** to save the changes.

Configuring a Filename Extension List Custom Object

To configure a filename extension list custom object:

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 filename extension list.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Utm > Custom Objects**.
4. Select **Filename Extension** and click **New**.
5. Enter a unique name for the extension list.
6. Select **Value** and add a new entry.
7. Enter the extensions in the **Value** box.
8. Click **OK** to save the changes.

Configuring a URL Pattern List Custom Object

To configure a URL pattern list custom object:

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 URL pattern list custom objects.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Utm > Custom Objects**.
4. Select **Url Pattern** and click **New**.
5. Enter a unique name for the list.
6. Select **Value** and add a new entry.
7. In Value, enter the URLs or IP addresses you want added to the list for bypassing scanning.



NOTE: For URL pattern wildcard support, the wildcard rule is as follows: `*\.[]\?*` and you must precede all wildcard URLs with `http://`. You can only use an asterisk (*) if it is at the beginning of the URL and is followed by a dot (.). You can only use a question mark (?) at the end of the URL.

The following wildcard syntax is supported: `http://*juniper.net`, `http://www.juniper.ne?`, `http://www.juniper.n??`. The following wildcard syntax is not supported: `*juniper.net`, `www.juniper.ne?`, `http://*juniper.net`, `http://*`.

8. Click **OK** to save the changes.

Configuring a Custom URL Category List Custom Object

To configure a custom URL category list custom object:

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 URL category list custom objects.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Utm > Custom Objects**.
4. Select **Custom Url Category** and click **New**.
5. Enter a unique name for the list.
6. Select **Value** and add a new entry.
7. Enter the name of the URL pattern list you created for bypassing scanning.
8. Click **OK** to save the changes.

Configuring an Antivirus Feature Profile

When configuring antivirus protection, you must first create the antivirus custom objects you are using. Those custom objects may include the MIME pattern list, MIME exception list, and the filename extension list. Once you have created your custom objects, you can configure full antivirus protection, including intelligent prescreening, and content size limits.

To configure an antivirus feature 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 an antivirus feature profile.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Utm > Feature Profile > Antivirus > Kaspersky Lab Engine**.
4. Add or modify antivirus profile settings as specified in [Table 228 on page 381](#).
5. Click one:
 - **New**—Adds a new profile.
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 228: Antivirus Feature Profile Settings

Option	Function	Your Action
Pattern Update		
Url	Specifies the URL for the pattern database.	If the URL is not already entered, enter the URL for the pattern database. Note that the URL is <code>http://update.juniper-updates.net/AV/SRX210</code> and you should not change it.
Interval	Specifies the time interval for automatically updating the pattern database.	Enter the time interval for automatically updating the pattern database. The default interval is 60 minutes.
No Autoupdate	Specifies whether automatic updates are disabled.	Select this option if you want to disable automatic updates and update the pattern database manually.
Pattern Update > Email Notify		
Admin Email	Specifies the e-mail addresses of the administrators.	Enter the e-mail addresses of the administrators who should receive e-mail notifications when updates are made to the pattern file.

Table 228: Antivirus Feature Profile Settings (*continued*)

Option	Function	Your Action
Custom Message	Specifies the text that will appear in the custom message.	Enter the text to appear in the body of the notification e-mail.
Custom Message Subject	Specifies the custom message subject.	Enter the text to appear in the subject line of the notification e-mail.
Profile		
Name	Specifies the name of the Kaspersky lab engine profile.	Enter a unique name for the Kaspersky lab engine profile.
Profile > Fallback Options		
Enable Feature	Enables fallback options.	Select this option to enable fallback options.
The available fallback options are as follows:	Specifies the fallback options.	Select log-and-permit or block from the list.
<ul style="list-style-type: none"> • Default • Corrupt File • Password File • Decompress Layer • Content Size • Engine Not Ready • Timeout • Out of Resources • Too Many Requests 		
Profile > Notification Options		
Enable Feature	Enables notification options.	Select this option to enable notification options.
The notification options that can be configured are the following:	Specifies the notification actions for fallback block, fallback nonblock, and virus detection.	<ul style="list-style-type: none"> • Custom Message—Enter the text to appear in the body of the notification e-mail. • Custom Message Subject—Enter the text to appear in the subject line of the notification e-mail. • notify-mail-sender—Select this option to notify the sender of the mail. • Type—Select protocol-only or message from the Type list.
Profile > Scan Options		

Table 228: Antivirus Feature Profile Settings (*continued*)

Option	Function	Your Action
Enable Feature	Enables scan options.	Select this option to enable scan options.
intelligent-prescreening	Enables intelligent prescreening.	Select this option to enable intelligent prescreening.
Content Size Limit	Specifies the content size parameters. The content size check occurs before the scan request is sent. The content size refers to accumulated TCP payload size.	Enter content size parameters.
Timeout	Specifies the scanning timeout parameters.	Enter the scanning timeout parameters.
Profile > Trickling		
Enable Feature	Enables trickling feature.	Select this option to enable trickling feature.
Timeout	Specifies the trickling timeout parameters.	Enter the trickling timeout parameters.
Antivirus > Mime Whitelist		
Enable Feature	Enables this feature.	Select this option to enable this feature.
List	Specifies the name of the URL whitelist.	Enter the name of the URL whitelist custom object you created.

Configuring a UTM Policy for Express Antivirus

To configure a UTM policy for express antivirus:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device that you want to configure.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Utm > Utm Policy**.
4. Click **New** to add a new UTM policy entry.

5. Enter a unique name for the UTM policy.
6. Select **Antivirus** and enter the name of the antivirus profile.
7. In the Http, Imap, Pop3, or Smtplib profile boxes, enter the name of the profile you created earlier.
8. For Ftp, select the upload and download profiles.
9. Click **OK** to save the changes.

Once you have configured a UTM policy for express antivirus, attach the UTM policy to a security policy that you create.

**Related
Documentation**

- [Configuring Local List Antispam \(NSM Procedure\) on page 376](#)
- [Configuring Content Filtering \(NSM Procedure\) on page 384](#)
- [Configuring Web Filtering \(NSM Procedure\) on page 387](#)

Configuring Content Filtering (NSM Procedure)

This section includes the following topics:

- [Configuring a Protocol Command Custom Object on page 384](#)
- [Configuring a Filename Extension List Custom Object on page 385](#)
- [Configuring a MIME Pattern List Custom Object on page 385](#)
- [Configuring a Content-Filtering Feature Profile on page 385](#)
- [Configuring a UTM Policy for Content-Filtering on page 387](#)

Configuring a Protocol Command Custom Object

To configure a protocol command custom object:

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 protocol command custom object.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Utm > Custom Objects**.
4. Select **Protocol Command** and click **New**.
5. Enter a unique name for the protocol command custom object.
6. Select **Value** and add a new entry.
7. Enter the commands for the protocol in Value.
8. Click **OK** to save the changes.

Configuring a Filename Extension List Custom Object

To configure a filename extension list custom object:

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 filename extension list.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Utm > Custom Objects**.
4. Select **Filename Extension** and click **New**.
5. Enter a unique name for the extension list.
6. Select **Value** and add a new entry.
7. Enter the extensions in the **Value** box.
8. Click **OK** to save the changes.

Configuring a MIME Pattern List Custom Object

To configure a MIME pattern list custom object:

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 MIME pattern list custom object.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Utm > Custom Objects**.
4. Select **Mime Pattern** and click **New**.
5. Enter a unique name for the list.
6. Select **Value** and add a new entry.
7. Enter a value for the MIME pattern.
8. Click **OK** to save the changes.

Configuring a Content–Filtering Feature Profile

To configure a content-filtering feature 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 a content-filtering feature profile.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Utm > Feature Profile > Content Filing > Profile**.
4. Add or modify content-filtering profile settings as specified in [Table 229 on page 386](#).
5. Click one:

- **New**—Adds a new profile.
- **OK**—Saves the changes.
- **Cancel**—Cancels the modifications.

Table 229: Content—Filtering Feature Profile Settings

Option	Function	Your Action
Profile		
Name	Specifies the name of the content-filtering profile.	Enter a unique name for this profile.
Permit Command	The permit protocol command list is intended to act as an exception list for the block protocol command list.	Enter the protocol command custom object you created for permitting commands from the list.
Block Command	Specifies the block command.	Enter the protocol command custom object you created for blocking commands from the list.
Block Extension	Specifies the extensions that are blocked.	Enter the file extension list custom object you created for blocking extensions from the list.
Profile > Block Content Type		
The content types that can be blocked are the following:	Specifies the content types that can be blocked.	Select one or more of the content types to be blocked.
<ul style="list-style-type: none"> • Activex • Java Applet • Exe • Zip • Http Cookie 		
Profile > Block Mime		
Enable Feature	Enables configuration of block MIME features.	Select this option to configure block MIME features.
List	Specifies the MIME list custom object.	Enter the MIME list custom object you created for blocking MIME patterns.
Exception	Specifies the exception MIME list custom object.	Enter the exception MIME list custom object you created for MIME patterns that will not be blocked.
Profile > Notification Options		
Enable Feature	Enables notification options.	Select this option to enable notification options.

Table 229: Content–Filtering Feature Profile Settings (*continued*)

Option	Function	Your Action
Type	Specifies the notification type.	Select message as the type of notification that is sent when a fallback option of block is triggered.
notify-mail-sender	Specifies that notification will be sent to the sender.	Select this option to notify the sender of the mail.
Custom Message	Specifies the notification actions for fallback block, fallback nonblock, and virus detection.	Enter the text to appear in the body of the notification e-mail.

Configuring a UTM Policy for Content-Filtering

To configure a UTM policy for content filtering:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device that you want to configure.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Utm > Utm Policy**.
4. Click **New** to add a new UTM policy entry.
5. Enter a unique name for the UTM policy.
6. Select **Content Filtering** and enter the name of the profile you had created.
7. In the Http, Imap, Pop3, or Smtplib profile boxes, enter the name of the profile you created earlier.
8. For Ftp, select the upload and download profiles.
9. Click **OK** to save the changes.

Once you have configured a UTM policy for content filtering, attach the UTM policy to a security policy that you create.

Related Documentation

- [Configuring Local List Antispam \(NSM Procedure\) on page 376](#)
- [Configuring Antivirus Protection \(NSM Procedure\) on page 379](#)
- [Configuring Web Filtering \(NSM Procedure\) on page 387](#)

Configuring Web Filtering (NSM Procedure)

This section includes the following topics:

- [Configuring a URL Pattern List Custom Object on page 388](#)
- [Configuring a Custom URL Category List Custom Object on page 388](#)

- [Configuring a Web Filtering Feature Profile on page 389](#)
- [Configuring a UTM Policy for Web Filtering on page 391](#)

Configuring a URL Pattern List Custom Object

To configure a URL pattern list custom object:

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 URL pattern list custom objects.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Utm > Custom Objects**.
4. Select **Url Pattern** and click **New**.
5. Enter a unique name for the list.
6. Select **Value** and add a new entry.
7. In Value, enter the URLs or IP addresses that you want to be added to the list for bypassing scanning.



NOTE: For URL pattern wildcard support, the wildcard rule is as follows: `*\.[]\?*` and you must precede all wildcard URLs with `http://`. You can only use an asterisk (*) if it is at the beginning of the URL and is followed by a dot (.). You can only use a question mark (?) at the end of the URL.

The following wildcard syntax is supported: `http://*juniper.net`, `http://www.juniper.ne?`, `http://www.juniper.n??`. The following wildcard syntax is not supported: `*juniper.net`, `www.juniper.ne?`, `http://*juniper.net`, `http://*`.

8. Click **OK** to save the changes.

Configuring a Custom URL Category List Custom Object

To configure a custom URL category list custom object:

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 whitelist and blacklist custom objects.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Utm > Custom Objects**.
4. Select **Custom Url Category** and click **New**.
5. Enter a unique name for the list.
6. Select **Value** and add a new entry.

7. Enter the name of the URL pattern list you created for bypassing scanning.
8. Click **OK** to save the changes.

Configuring a Web Filtering Feature Profile

To configure a Web filtering feature 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 a Web filtering feature profile.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Utm > Feature Profile > Web Filtering**.
4. Add or modify Web filtering feature profile settings as specified in [Table 230 on page 389](#).
5. Click one:
 - **New**—Adds a new profile.
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 230: Web Filtering Feature Profile Settings

Option	Function	Your Action
Url Whitelist	Specifies the URL whitelist.	Enter the name of the custom URL list you created. This is the first filtering category that both integrated and redirect Web filtering use. If there is no match, the URL is sent to the SurfControl server.
Url Blacklist	Specifies the URL blacklist.	Enter the name of the custom URL list you created. This is the first filtering category that both integrated and redirect Web filtering use. If there is no match, the URL is sent to the SurfControl server.
Type	Specifies the type of Web filtering.	Select surf-control-integrated from the list.
Surf Control Integrated > Cache		
Enable Feature	Enables cache options.	Select this option to enable cache options.
Timeout	Specifies the timeout limit for cache entries.	Enter a timeout limit in minutes for expiring cache entries. (The default is 24 hours and the maximum allowed life span.)
Size	Specifies the size limit for the cache.	Enter a size limit for the cache in kilobytes. (The default is 500 KB.)

Table 230: Web Filtering Feature Profile Settings (*continued*)

Option	Function	Your Action
Surf Control Integrated > Server		
Enable Feature	Enables server options.	Select this option to enable server options.
Host	Specifies the Surf Control server address.	Enter the Surf Control server name or IP address.
Port	Specifies the port number for communicating with the Surf Control server.	Enter the port number for communicating with the Surf Control server. (Default ports are 80, 8080, and 8081.)
Surf Control Integrated > Profile		
Name	Specifies a name for the Web-filtering profile.	Enter a unique name for this profile.
Default	Specifies the default action for this profile for requests that experience errors.	Select log-and-permit , permit , or block from the list.
Custom Block Message	Specifies the custom message.	Enter a custom message to be sent when HTTP requests are blocked.
Timeout	Specifies the timeout limit.	Enter a value in seconds. Once this limit is reached, fail mode settings are applied. The default setting is 10 seconds.
Surf Control Integrated > Profile > Fallback Settings		
Enable Feature	Enables fallback options.	Select this option to enable fallback options.
The available fallback options are as follows:	Specifies the fallback options.	Select log-and-permit or block from the list.
<ul style="list-style-type: none"> • Default • Server Connectivity • Timeout • Too Many Requests 		
Surf Control Integrated > Profile > Category		
Name	Specifies the name of the category.	Enter the name of the custom URL category list custom object you created.
Action	Specifies the action to be taken.	Select log-and-permit , permit , or block from the list.

Configuring a UTM Policy for Web Filtering

To configure a UTM policy for Web filtering:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device that you want to configure.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Utm > Utm Policy**.
4. Click **New** to add a new UTM policy entry.
5. Enter a unique name for the UTM policy.
6. Select **Web Filtering** and enter the name of Web filtering profile you created earlier in Http Profile.
7. In the Http profile box, enter the name of the profile you created earlier.
8. Click **OK** to save the changes.

Once you have configured a UTM policy for Web filtering, attach the UTM policy to a security policy that you create.

Related Documentation

- [Configuring Local List Antispam \(NSM Procedure\) on page 376](#)
- [Configuring Content Filtering \(NSM Procedure\) on page 384](#)
- [Configuring Antivirus Protection \(NSM Procedure\) on page 379](#)

Configuring Network Address Translation in J Series Services Routers and SRX Series Services Gateways

- [Configuring Source NAT Objects on JUNOS OS \(NSM Procedure\) on page 393](#)

Configuring Source NAT Objects on JUNOS OS (NSM Procedure)

Network and Security Manager (NSM) allows you to configure Network Address Translation (NAT) objects running on JUNOS devices using the NAT rulebase.

To configure source NAT objects on JUNOS OS:

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 NAT running on JUNOS OS.
3. Click the **Configuration** tab. In the configuration tree, select **Security > Nat > Source > Pool**.
4. Add or modify settings as specified in [Table 231 on page 393](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 231: JUNOS Source NAT Configuration Details

Option	Function	Your Action
Pool		
Name	Specifies the name of the new pool.	1. Click the New button.
Comment	Specifies the comment for the new pool. This is optional.	2. Enter a name and comment. 3. Click OK .
Pool > Address		

Table 231: JUNOS Source NAT Configuration Details (*continued*)

Option	Function	Your Action
IP Address	Specifies the starting range of the IP address.	1. Click the New button.
Ipaddr	Specifies the ending range of the IP address.	2. Enter the comment and the starting range of the IP address. 3. Click the End of Range tab. 4. Enter the comment and the ending range of the IP address. 5. Click OK .
Pool > Host Address Base		
Ipaddr	Specifies the host IP address.	1. Enter a comment. 2. Enter the IP address of the host. 3. Click OK .
Pool > Overflow Pool > Pool Name		
None	Specifies that no pool name is selected.	1. Enter a comment.
pool-name	Specifies the pool name.	2. Select one of the following options: <ul style="list-style-type: none"> • None • pool-name • interface
interface	Specifies the interface name for the pool.	3. If you select pool-name , enter a pool name. 4. Click OK .
Pool > Port Translation		
No Translation	Specifies that no port is selected.	1. Enter a comment. 2. For No Translation, select the No Translation check box. 3. Click OK .
Translation	Specifies the lower and higher ranges of the port.	1. Enter the comment and the lower range. 2. Click the To tab. 3. Enter the comment and the higher range. 4. Click OK .
Pool > Routing Instance		
Ri Name	Specifies the routing instance name.	1. Enter a comment. 2. Select the routing instance name from the drop-down list. 3. Click OK .

- Related Documentation**
- [NSM and Device Management Overview on page 3](#)
 - [Communication Between NSM and a Device Overview on page 3](#)

CHAPTER 24

Configuring Bridge Domains in J Series Services Routers and SRX Series Services Gateways

- [Configuring Bridge Domains Properties \(NSM Procedure\) on page 397](#)

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 397](#)
- [Configuring Multicast Monitoring Options \(NSM Procedure\) on page 398](#)
- [Configuring VLAN ID \(NSM Procedure\) on page 401](#)

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 232 on page 398](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 232: 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 233 on page 399](#).
6. Click one:
 - **OK**—saves the changes
 - **Cancel**—cancels the modifications

Table 233: 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 233: 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 234 on page 401](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 234: 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.

Configuring Forwarding Options in J Series Services Routers and SRX Series Services Gateways

- [Configuring Accounting Options \(NSM Procedure\) on page 403](#)
- [Specifying Address Family for Filters \(NSM Procedure\) on page 405](#)
- [Configuring Load Balancing Using Hash Key \(NSM Procedure\) on page 406](#)
- [Configuring Helpers \(NSM Procedure\) on page 407](#)
- [Configuring Per-Flow and Per-Prefix Load Balancing \(NSM Procedure\) on page 416](#)
- [Configuring Port Mirroring \(NSM Procedure\) on page 417](#)

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 235 on page 404](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 235: 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.
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).

Table 235: Accounting Options Configuration Details (*continued*)

Task	Your Action
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)
- [Specifying Address Family for Filters \(NSM Procedure\) on page 405](#)
- [Configuring Load Balancing Using Hash Key \(NSM Procedure\) on page 406](#)

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 236 on page 405](#).
5. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 236: 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 236: 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)
- [Configuring Per-Flow and Per-Prefix Load Balancing \(NSM Procedure\) on page 416](#)
- [Configuring Port Mirroring \(NSM Procedure\) on page 417](#)

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 237 on page 407](#).
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 237: 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 403](#)
- [Configuring Helpers \(NSM Procedure\) on page 407](#)
- [Configuring Per-Flow and Per-Prefix Load Balancing \(NSM Procedure\) on page 416](#)

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 408](#)
- [Enabling DNS Request Packet Forwarding on page 411](#)
- [Configuring a Port for a DHCP or BOOTP Relay Agent on page 413](#)
- [Configuring Tracing Operations for BOOTP, DNS, and TFTP Packet Forwarding on page 415](#)

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 238 on page 408](#).
5. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 238: 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 238: 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 238: 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 238: 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 239 on page 413](#).
5. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 239: 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 240 on page 414](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 240: 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 241 on page 415](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 241: 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 242 on page 416](#).
5. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 242: 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 417](#)
- [Configuring Helpers \(NSM Procedure\) on page 407](#)
- [Configuring Load Balancing Using Hash Key \(NSM Procedure\) on page 406](#)

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 243 on page 418](#).
5. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 243: 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 243 on page 418. 5. To configure input packet properties for port mirroring, refer Table 243 on page 418.

Table 243: 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 416](#)
- [Configuring Load Balancing Using Hash Key \(NSM Procedure\) on page 406](#)
- [Specifying Address Family for Filters \(NSM Procedure\) on page 405](#)

CHAPTER 26

Configuring Interfaces in J Series Services Routers and SRX Series Services Gateways

- [Configuring Interfaces on the Routing Platform \(NSM Procedure\) on page 421](#)
- [Configuring Interface set on the Routing Platform \(NSM Procedure\) on page 449](#)

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 421](#)
- [Damping Interface Transitions \(NSM Procedure\) on page 423](#)
- [Configuring Receive Bucket Properties on Interfaces \(NSM Procedure\) on page 424](#)
- [Configuring Tracing Operations of an Individual Router Interface \(NSM Procedure\) on page 424](#)
- [Configuring Transmit Leaky Bucket Properties \(NSM Procedure\) on page 425](#)
- [Configuring Logical Interface Properties \(NSM Procedure\) on page 426](#)
- [Configuring Protocol Family Information for the Logical Interface \(NSM Procedure\) on page 429](#)
- [Configuring the Traffic Shaping Profile \(NSM Procedure\) on page 447](#)

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 244 on page 422](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 244: 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 245 on page 423](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 245: 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 246 on page 424](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 246: 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 247 on page 425](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 247: 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 248 on page 426](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 248: 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 426](#)
- [Configuring an IP Demux Underlying Interface \(NSM Procedure\) on page 427](#)
- [Configuring the Logical Demux Source Family Type on the IP Demux Underlying Interface \(NSM Procedure\) on page 428](#)
- [Configuring Epd Threshold for the Logical Interface \(NSM Procedure\) on page 428](#)

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 249 on page 427](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 249: 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 250 on page 428](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 250: 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 251 on page 428](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 251: 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 252 on page 429](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 252: 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 430](#)
2. [Configuring Protocol Family \(Inet\) Information for the Logical Interface \(NSM Procedure\) on page 431](#)
3. [Configuring Protocol Family \(Inet6\) Information for the Logical Interface \(NSM Procedure\) on page 437](#)
4. [Configuring Protocol Family \(ISO\) Information for the Logical Interface \(NSM Procedure\) on page 444](#)
5. [Configuring Protocol Family \(MPLS\) Information for the Logical Interface \(NSM Procedure\) on page 445](#)
6. [Configuring Protocol Family \(TCC\) Information for the Logical Interface \(NSM Procedure\) on page 447](#)

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 253 on page 430](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 253: 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 253: 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 254 on page 432](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 254: 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 254: 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 254: Inet 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 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. Select 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 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 254: 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 254: 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 254: 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 255 on page 438](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 255: 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 255: 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 255: 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 255: 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 255: Inet6 Family Configuration Details (*continued*)

Task	Your Action
Specify the bandwidth threshold for VRRP.	<ol style="list-style-type: none"> Click Bandwidth Threshold next to interface. Click Add new entry next to Bandwidth Threshold. 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 Click Route next to Track. In the Route_address box, enter the address. In the Routing Instances box, enter the routing instance in which the route is to be tracked. 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. Click Virtual Address next to vrrp-group. 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"> 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"> 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"> Click Input next to Filter. 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"> Click Add new entry next to input-list. In the New input-list window, enter the filter names. Up to 16 filters can be included in a filter input list.

Table 255: 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 255: 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 256 on page 445](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 256: 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 257 on page 446](#).
6. Click one:
 - OK—Saves the changes.
 - Cancel—Cancels the modifications.

Table 257: 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 258 on page 447](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 258: 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 259 on page 448](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 259: 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 260 on page 449](#).
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 260: 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 421](#)
- [Configuring Trace Options on the Routing Platform \(NSM Procedure\)](#)

Configuring Multicast Snooping Options in J Series Services Routers and SRX Series Services Gateways

- [Configuring Multicast Monitoring Options \(NSM Procedure\) on page 451](#)

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 261 on page 452](#).
5. Click one:
 - OK—To save the changes.
 - Cancel—To cancel the modifications.

Table 261: 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 261: 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 421](#)

PART 3

Managing J Series Services Routers and SRX Series Services Gateways

- [Using System Management Features in J Series Services Routers and SRX Series Services Gateways on page 457](#)
- [Topology Manager on page 461](#)
- [IDP Management in J Series Services Routers and SRX Series Services Gateways on page 465](#)

CHAPTER 28

Using System Management Features in J Series Services Routers and SRX Series Services Gateways

- [Managing J Series and SRX Series Device Software Versions Overview on page 457](#)
- [Viewing and Reconciling Device Inventory Overview on page 457](#)
- [Viewing Device Inventory in NSM \(NSM Procedure\) on page 458](#)
- [Removing a J Series or SRX Series Device from NSM Management \(NSM Procedure\) on page 459](#)

Managing J Series and SRX Series Device Software Versions Overview

You can use Network and Security Manager (NSM) to upgrade or adjust the software on managed J Series and SRX Series devices running JUNOS Release 9.3 or later.

When a software upgrade is applied to a J Series or SRX 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 J Series and SRX Series devices with dual Routing Engines.

For steps on updating the device software version, see “Upgrading the Device Software” in the *Network and Security Manager Administration Guide*.

Related Documentation

- [Viewing Device Inventory in NSM \(NSM Procedure\) on page 458](#)
- [Viewing and Reconciling Device Inventory Overview on page 457](#)

Viewing and Reconciling Device Inventory Overview

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 J Series and SRX 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 J-Web 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**

- [Viewing Device Inventory in NSM \(NSM Procedure\) on page 458](#)

Viewing Device Inventory in NSM (NSM Procedure)

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.

To view the device inventory in NSM:

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 appears.
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.
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.

**Related
Documentation**

- [Viewing and Reconciling Device Inventory Overview on page 457](#)

Removing a J Series or SRX Series Device from NSM Management (NSM Procedure)

Deleting a device removes all device configuration information from the management system, but might be the best solution if you need to perform extensive troubleshooting or reconfigure the device locally.

To remove a J Series or SRX Series device from NSM management:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab and then select the device that you want to remove from NSM management.
3. Right-click and select **Delete**, or click the **Delete** button. The Delete dialog box appears. If the device is referenced in a firewall rule, this dialog box displays the rules that reference it. You can click the links that appear to display the security policies to view or edit those references.
4. Remove the device by clicking **Next**. The Delete dialog box displays the progress of the deletion.
5. After NSM finishes, click **Finish** to close the dialog box.

Related Documentation

- [Adding J Series Services Routers or SRX Series Services Gateways in NSM Overview on page 8](#)

CHAPTER 29

Topology Manager

- [Overview of the NSM Topology Manager on page 461](#)
- [Requisites for a Topology Discovery Overview on page 461](#)
- [Understanding the NSM Topology Manager Toolbar on page 462](#)

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 Overview on page 461](#)
- [Understanding the NSM Topology Manager Toolbar on page 462](#)

Requisites for a Topology Discovery Overview

To use the Topology Manager, first add one or more devices 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 either seed devices and/or preferred subnets to initiate topology discovery. You also need:

- The management IP address of the device that acts as the seed IP address.
- SNMP credentials:
 - For SNMPv1 and SNMPv2c: Community string.
 - For SNMPv3: Username, security level, authentication type, privacy type, privacy password, and authentication password.

- 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 461](#)
- [Understanding the NSM Topology Manager Toolbar on page 462](#)

Understanding 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:** Use this tool to print a network topology map as an image file and the devices and links tables as text files from different views.
- **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 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 461](#)
 - [Requisites for a Topology Discovery Overview on page 461](#)

IDP Management in J Series Services Routers and SRX Series Services Gateways

- [Updating the NSM Attack Database \(NSM Procedure\) on page 465](#)
- [Loading the IDP Detector Engine on a J Series or SRX Series Device \(NSM Procedure\) on page 466](#)
- [Updating the Deep Inspection Attack Database on a J Series or SRX Series Device \(NSM Procedure\) on page 466](#)

Updating the NSM Attack Database (NSM Procedure)

You must update the attack object database before you can use IDP functionality. To update the IDP and deep inspection (DI) databases and the IDP detector engine, download new attack objects from the attack object database server to the NSM GUI server.

To update the IDP and DI attack object databases on the NSM GUI server:

1. From the Tools menu in the NSM UI, click **View/Update NSM Attack Database**. The Attack Update Manager wizard appears.
2. Click **Next** to proceed. The current attack database version in NSM and the latest attack database version appear.
3. Click **Finish** to start downloading the latest attack database version from the server. The progress and status of the attack update process appear in the Job Information page.
4. Click one:
 - **Cancel Job**—Cancels the IDP detector engine loading process.
 - **Refresh**—Refreshes the status of the update process.
 - **Notify Later**—Notifies the completion of the update process.
 - **Close**—Closes the Job Information page.

After you have updated the attack object database on the NSM GUI server, you can use that database to update the attack object database on your managed devices.

- Related Documentation**
- [Loading the IDP Detector Engine on a J Series or SRX Series Device \(NSM Procedure\) on page 466](#)
 - [Updating the Deep Inspection Attack Database on a J Series or SRX Series Device \(NSM Procedure\) on page 466](#)

Loading the IDP Detector Engine on a J Series or SRX Series Device (NSM Procedure)

IDP attack objects are loaded onto IDP-capable devices with the IDP rulebase.

To load a new detector engine onto a J Series or SRX Series device:

1. From the Devices menu in the NSM UI, select **IDP Detector Engine > Load IDP Detector Engine for JUNOS**. The Load JUNOS IDP Detector Engine wizard appears.
2. Click **Next** to proceed. The available IDP detector engine versions are displayed.
3. Select the JUNOS device to be updated and click **Finish**. The progress and status of the IDP detector engine update process appears in the Job Information page.
4. Click one:
 - **Cancel Job**—Cancels the IDP detector engine loading process.
 - **Refresh**—Refreshes the status of the update process.
 - **Notify Later**—Notifies the completion of the update process.
 - **Close**—Closes the Job Information page.

- Related Documentation**
- [Updating the NSM Attack Database \(NSM Procedure\) on page 465](#)
 - [Updating the Deep Inspection Attack Database on a J Series or SRX Series Device \(NSM Procedure\) on page 466](#)

Updating the Deep Inspection Attack Database on a J Series or SRX Series Device (NSM Procedure)

To update the deep inspection attack database on a J Series or SRX Series device:

1. From the Devices menu in the NSM UI, select **Update Device Attack Database**. The Change Device Signature Package wizard appears.
2. Click **Next** to proceed. The available deep inspection signature database versions appear.
3. Select the JUNOS device to be updated and click **Finish**. The progress and status of the attack object database update process appears in the Job Information page.
4. Click one:
 - **Cancel Job**—Cancels the attack object database update process.
 - **Refresh**—Refreshes the status of the update process.

- **Notify Later**—Notifies the completion of the update process.
- **Close**—Closes the Job Information page.

**Related
Documentation**

- [Updating the NSM Attack Database \(NSM Procedure\) on page 465](#)
- [Loading the IDP Detector Engine on a J Series or SRX Series Device \(NSM Procedure\) on page 466](#)

PART 4

Monitoring J Series Services Routers and SRX Series Services Gateways

- Real Time Monitoring of J Series Services Routers and SRX Series Services Gateways on page 471

CHAPTER 31

Real Time Monitoring of J Series Services Routers and SRX Series Services Gateways

- [Realtime Monitor Overview on page 471](#)
- [Viewing Device Status on page 471](#)
- [Viewing Device Monitor Alarm Status \(NSM Procedure\) on page 474](#)
- [Configuring the Polling Interval for Device Alarm Status \(NSM Procedure\) on page 475](#)

Realtime Monitor Overview

The Realtime Monitor module in NSM includes views that you can use to monitor real-time status and statistics about all the managed security devices, VPN tunnels, NSRP clusters, IDP sensors, and IDP clusters in your network. You can also use the Realtime Monitor to identify problems, track security events, 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, and then color-coding each event to organize problems.

Related Documentation • [Viewing Device Status on page 471](#)

Viewing Device Status

[Table 262 on page 472](#) lists and describes device information that you can view through the Device Monitor.

Table 262: 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 from 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 262: 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). 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 on 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 262: 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 on the device. • Out Of Sync—The inventory information in the NSM database is not synchronized with the information on 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**
- [Viewing Device Monitor Alarm Status \(NSM Procedure\) on page 474](#)
 - [Configuring the Polling Interval for Device Alarm Status \(NSM Procedure\) on page 475](#)

Viewing Device Monitor Alarm Status (NSM Procedure)

Alarms refresh automatically through periodic polling.

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. Retrieve the current alarm status in the device by clicking the **Refresh** button.

The poll time is derived from the device server time.

- Related Documentation**
- [Viewing Device Status on page 471](#)
 - [Configuring the Polling Interval for Device Alarm Status \(NSM Procedure\) on page 475](#)

Configuring the Polling Interval for Device Alarm Status (NSM Procedure)

The default polling interval is 900 seconds (15 minutes). To configure polling intervals for alarm Status:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to set the polling interval.
3. Click the **Info** tab, and select **Device Admin**.
4. 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.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

- Related Documentation**
- [Viewing Device Status on page 471](#)
 - [Viewing Device Monitor Alarm Status \(NSM Procedure\) on page 474](#)

PART 5

Index

- [Index on page 479](#)

Index

Symbols

802.1x authentication.....110

A

access profile, configuring.....31
accounting options
 class usage profile, configuring.....33
 filter profile, configuring.....35
 interface profile, configuring.....36
 log file, configuring.....34
 MIB profile, configuring.....38
 policy decision statistics profile,
 configuring.....37
 routing engine profile, configuring.....39
accounting options, configuring.....33
address family, specifying.....405
aggregated devices, configuring.....53
application, application set
 configuring.....41

B

BGP
 configuring.....107
bridge domain
 logical interfaces, configuring.....397
 multicast monitoring options,
 configuring.....398
 VLAN ID, configuring.....401
bridge domains properties
 configuring.....397

C

chassis alarms, configuring.....54
chassis FPC, configuring.....55
classifiers
 CoS.....316
client lists
 configuring.....253
code point aliases.....318

commit delay timer
 configuring.....259
 See also nonvolatile
communities
 configuring.....248
CoS classifiers.....316
CoS code point aliases.....318
CoS drop profiles.....319
CoS forwarding classes.....321
CoS forwarding policy, configuring.....323
CoS fragmentation maps, configuring.....324
CoS host outbound traffic, configuring.....325
CoS interfaces.....326
CoS rewrite rules.....332
CoS scheduler maps.....336
CoS schedulers.....335
CoS traffic control profiles, configuring.....338
customer support.....xviii
 contacting JTAC.....xviii

D

drop profiles.....319

E

event policy tracing, configuring.....346
event policy, configuring.....343
event script, configuring.....341

F

fate sharing
 configuring.....101
firewall filter
 any family type, configuring.....349
 bridge family type, configuring.....351
 Ccc family type, configuring.....353
 inet family type, configuring.....355
flow
 configuring.....99
forwarding
 accounting options, configuring.....403
forwarding classes.....321
forwarding table
 configuring.....97

G

generated routes
 configuring.....95
graceful restart
 configuring.....96

GVRP.....	112
-----------	-----

H

health monitoring	
configuring.....	256
helpers	
DNS packet forwarding, enabling.....	411
port, configuring.....	413
router/interface, configuring.....	408
tracing operations, configuring.....	415
helpers, configuring.....	407

I

IGMP	
configuring.....	113
inet family type	
firewall filter, configuring.....	355
prefix-specific actions, configuring.....	357
service filters, configuring.....	358
simple filters, configuring.....	359
instance export	
configuring.....	105
instance import	
configuring.....	105
interface	
configuring.....	258
interface routes	
configuring.....	104
interface set, configuring.....	449
interfaces	
logical interface properties, configuring.....	426
properties, configuring.....	421
receive bucket properties, configuring.....	424
tracing operations, configuring.....	424
traffic shaping profile, configuring.....	447
transitions, damping.....	423
transmit leaky bucket, configuring.....	425
interfaces, configuring.....	421

L

LDAP server, configuring.....	22
load balancing	
per-flow/per-prefix, configuring.....	416
load balancing, configuring.....	406
local engine ID	
configuring.....	255
logical interface	
demux source family type, configuring.....	428
epd threshold, configuring.....	428

IP demux, configuring.....	427
unit properties, configuring.....	426
logical interfaces	
Ccc family information, configuring.....	430
inet family information, configuring.....	431
inet6 family information, configuring.....	437
ISO family information, configuring.....	444
MPLS family information, configuring.....	445
protocol family information, configuring.....	429
TCC family information, configuring.....	447

M

martian addresses	
configuring.....	102
maximum prefixes	
configuring.....	81
MSTP.....	154
multicast	
configuring.....	83
multipath	
configuring.....	86

O

Options	
configuring.....	87
OSPF.....	156

P

port mirroring	
configuring.....	417
protocols	
802.1x.....	110
BGP.....	107
GVRP.....	112
IGMP.....	113
OSPF.....	156
RIP.....	160
VRRP.....	175
VSTP.....	173
Protocols	
MSTP.....	154

R

resolution	
configuring.....	88
rewrite rules.....	332
rib	
configuring.....	91

rib groups		
configuring.....	89	
RIP.....	160	
rmon		
configuring.....	260	
routing engine		
reboot or halt, configuring.....	66	
routing engine redundancy, configuring.....	65	
routing instance access		
configuring.....	264	
routing options		
fate sharing.....	101	
flow.....	99	
forwarding table.....	97	
generated routes.....	95	
graceful restart.....	96	
instance export.....	105	
instance import.....	105	
interface routes.....	104	
martian addresses.....	102	
maximum prefixes.....	81	
multicast.....	83	
multipath.....	86	
Options.....	87	
resolution.....	88	
rib.....	91	
rib groups.....	89	
source routing.....	93	
Static Routes.....	94	
S		
scheduler maps.....	336	
schedulers.....	335	
SNMP		
client lists.....	253	
commit delay timer.....	259	
<i>See also</i> nonvolatile		
communities.....	248	
health monitoring.....	256	
interface.....	258	
local engine ID.....	255	
rmon.....	260	
routing instance access.....	264	
traceoptions.....	266	
trap groups.....	250	
trap options.....	268	
v3.....	270	
views.....	252	
source routing		
configuring.....	93	
Static Routes		
configuring.....	94	
support, technical <i>See</i> technical support		
T		
T640 router, configuring.....	60	
technical support		
contacting JTAC.....	xviii	
traceoptions		
configuring.....	266	
trap groups		
configuring.....	250	
trap options		
configuring.....	268	
V		
v3		
configuring.....	270	
views		
configuring.....	252	
VRRP.....	175	
VSTP.....	173	

