END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT (“AGREEMENT”) BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. The Parties. The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer’s principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer’s principal office is located outside the Americas) (such applicable entity being referred to herein as “Juniper”), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software (“Customer”) (collectively, the “Parties”).

2. The Software. In this Agreement, “Software” means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. “Software” also includes updates, upgrades and new releases of such software. “Embedded Software” means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. License Grant. Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.

b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees, provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.

c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer’s use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer’s use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

d. For any trial copy of the Software, Customer’s right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.

e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer’s enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. Use Prohibitions. Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any ‘locked’ or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. Audit. Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.
6. Confidentiality. The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer’s internal business purposes.

7. Ownership. Juniper and Juniper’s licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. Warranty, Limitation of Liability, Disclaimer of Warranty. The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the “Warranty Statement”). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper’s or its suppliers’ or licensors’ liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. Termination. Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer’s possession or control.

10. Taxes. All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer’s payment of any withholding taxes, completing appropriate applications that would reduce the amount of withholding tax to be paid, and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer’s non-compliance or delay with its responsibilities herein. Customer’s obligations under this Section shall survive termination or expiration of this Agreement.

11. Export. Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer’s ability to export the Software without an export license.

12. Commercial Computer Software. The Software is “commercial computer software” and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT II) as applicable.

13. Interface Information. To the extent required by applicable law, and at Customer’s written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. Third Party Software. Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License (“GPL”) or the GNU Library General Public License (“LGPL”)), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at http://www.gnu.org/licenses/gpl.html, and a copy of the LGPL at http://www.gnu.org/licenses/lgpl.html.

15. Miscellaneous. This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous
agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présents confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s’y rattaché, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language).
# Table of Contents

## About this Guide

- Objectives ................................................................. xiii
- Audience ................................................................. xiv
- Conventions .............................................................. xiv
- List of Technical Publications ........................................... xv
- Requesting Technical Support ................................................ xvi
  - Self-Help Online Tools and Resources ...................................... xvii
  - Opening a Case with JTAC ................................................... xvii

## Part 1  Getting Started

### Chapter 1  Understanding J Series Services Router and SRX Series Services Gateway Configuration

- 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

- J Series Services Router and SRX Series Services Gateway Installation and Configuration Overview ................................................................. 7
- NSM Installation Overview ...................................................................... 7
- 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
- Using Templates and Configuration Groups in NSM Overview .................. 9
Part 2 Configuring J Series Services Routers and SRX Series Services Gateways

Chapter 3 Configuring User Authentication in J Series Services Routers and SRX Series Services Gateways 13

Configuring RADIUS Authentication (NSM Procedure) .........................13
Configuring TACACS+ Authentication (NSM Procedure) ......................14
Configuring Authentication Order (NSM Procedure) ..............................15
Configuring User Access (NSM Procedure) ...........................................16
   Configuring Login Classes ..............................................................16
   Configuring User Accounts ............................................................17
Configuring Template Accounts (NSM Procedure) ...............................17
   Creating a Remote Template Account ..............................................18
   Creating a Local Template Account ................................................19

Chapter 4 Configuring Chassis in J Series Services Routers and SRX Series Services Gateways 21

Configuring Aggregated Devices (NSM Procedure) ...............................21
Configuring Chassis Alarms (NSM Procedure) ......................................22
Configuring Routing Engine Redundancy (NSM Procedure) ....................23
Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors (NSM Procedure) .................................................................24

Chapter 5 Configuring USB Modem Interfaces in J Series Services Routers and SRX Series Services Gateways 27

Configuring a USB Modem Interface (NSM Procedure) ........................27
Configuring a Dialer Interface (NSM Procedure) ...................................28
Configuring Dial-in Options on a Dialer Interface (NSM Procedure) ...........29
Configuring a CHAP Access Profile on a Dialer Interface (NSM Procedure) ..................................................................................30

Chapter 6 Configuring Policy Options in J Series Services Routers and SRX Series Services Gateways 33

Configuring an AS Path in a BGP Routing Policy (NSM Procedure) ..........33
Configuring an AS Path Group in a BGP Routing Policy (NSM Procedure) ..34
Configuring a Community for use in BGP Routing Policy Conditions (NSM Procedure) .................................................................35
Configuring a BGP Export Policy Condition (NSM Procedure) ...............36
Configuring Flap Damping to Reduce the Number of BGP Update Messages (NSM Procedure) ............................................................37
Configuring a Routing Policy Statement (NSM Procedure) .....................39
Configuring Prefix List (NSM Procedure) .............................................40
### Chapter 7 Configuring Routing Options in J Series Services Routers and SRX Series Services Gateways

<table>
<thead>
<tr>
<th>Configure</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Prefixes</td>
<td>43</td>
</tr>
<tr>
<td>Multicast</td>
<td>45</td>
</tr>
<tr>
<td>Multipath</td>
<td>48</td>
</tr>
<tr>
<td>Options</td>
<td>49</td>
</tr>
<tr>
<td>Route Resolution</td>
<td>50</td>
</tr>
<tr>
<td>Routing Table Groups</td>
<td>51</td>
</tr>
<tr>
<td>Routing Tables</td>
<td>53</td>
</tr>
<tr>
<td>Source Routing</td>
<td>55</td>
</tr>
<tr>
<td>Static Routes</td>
<td>56</td>
</tr>
<tr>
<td>Generated Routes</td>
<td>57</td>
</tr>
<tr>
<td>Graceful Restart</td>
<td>58</td>
</tr>
<tr>
<td>Forwarding Table</td>
<td>59</td>
</tr>
<tr>
<td>Flow Route</td>
<td>61</td>
</tr>
<tr>
<td>Flow Sharing</td>
<td>63</td>
</tr>
<tr>
<td>Martian Addresses</td>
<td>64</td>
</tr>
<tr>
<td>Interface Routes</td>
<td>66</td>
</tr>
<tr>
<td>Instance Export</td>
<td>67</td>
</tr>
<tr>
<td>Instance Import</td>
<td>67</td>
</tr>
</tbody>
</table>

### Chapter 8 Configuring Protocols for J Series Services Routers and SRX Series Services Gateways

<table>
<thead>
<tr>
<th>Configure</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP</td>
<td>69</td>
</tr>
<tr>
<td>802.1X Authentication</td>
<td>72</td>
</tr>
<tr>
<td>802.1X Interface Settings</td>
<td>72</td>
</tr>
<tr>
<td>Static MAC Bypass</td>
<td>74</td>
</tr>
<tr>
<td>GVRP</td>
<td>74</td>
</tr>
<tr>
<td>IGMP</td>
<td>75</td>
</tr>
<tr>
<td>MSTP</td>
<td>77</td>
</tr>
<tr>
<td>OSPF</td>
<td>79</td>
</tr>
<tr>
<td>RIP</td>
<td>82</td>
</tr>
<tr>
<td>VSTP</td>
<td>84</td>
</tr>
<tr>
<td>VRRP</td>
<td>86</td>
</tr>
</tbody>
</table>

### Chapter 9 Configuring SNMP for Network Management in J Series Services Routers and SRX Series Services Gateways

<table>
<thead>
<tr>
<th>Configure</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic System Identification</td>
<td>89</td>
</tr>
<tr>
<td>SNMP Agents and Communities</td>
<td>90</td>
</tr>
<tr>
<td>SNMP Trap Groups</td>
<td>91</td>
</tr>
<tr>
<td>SNMP Views</td>
<td>92</td>
</tr>
</tbody>
</table>
Chapter 10 Configuring J Series Services Routers and SRX Series Services Gateways for DHCP

Configuring the Device as a DHCP Server (NSM Procedure) ................................................. 95
Configuring the Device as a DHCP Client (NSM Procedure) ............................................... 97

Chapter 11 Configuring Class of Service in J Series Services Routers and SRX Series Services Gateways

Configuring CoS Classifiers (NSM Procedure) ............................................................... 99
Configuring CoS Code Point Aliases (NSM Procedure) ..................................................... 102
Configuring CoS Drop Profile (NSM Procedure) .............................................................. 103
Configuring CoS Forwarding Classes (NSM Procedure) ................................................... 105
Configuring CoS Forwarding Policy (NSM Procedure) ...................................................... 106
Configuring CoS Fragmentation Maps (NSM Procedure) .................................................. 108
Configuring CoS Host Outbound Traffic (NSM Procedure) .............................................. 109
Configuring CoS Interfaces (NSM Procedure) ..................................................................... 110
Configuring CoS Rewrite Rules (NSM Procedure) ............................................................ 115
Configuring CoS Schedulers (NSM Procedure) .................................................................... 118
Configuring CoS and Applying Scheduler Maps (NSM Procedure) ...................................... 120

Chapter 12 Configuring Unified Threat Management Features in J Series Services Routers and SRX Series Services Gateways

Configuring Server-Based Antispam (NSM Procedure) ......................................................... 123
Configuring Local List Antispam (NSM Procedure) ............................................................ 124
Configuring Whitelist and Blacklist Entries ........................................................................ 124
Configuring a Custom URL Category List Custom Object ................................................... 125
Configuring Server-Based Antispam .................................................................................... 125
Configuring a UTM Policy for SNMP .................................................................................. 126
Configuring Antivirus Protection (NSM Procedure) ............................................................. 127
Configuring a MIME Pattern List Custom Object ................................................................ 127
Configuring a Filename Extension List Custom Object ......................................................... 127
Configuring a Custom URL Category List Custom Object ................................................... 128
Configuring an Antivirus Feature Profile ............................................................................ 129
Configuring a UTM Policy for Express Antivirus ................................................................. 131
Configuring Content Filtering (NSM Procedure) ................................................................. 132
Configuring a Protocol Command Custom Object .............................................................. 132
Configuring a Filename Extension List Custom Object ......................................................... 132
Configuring a MIME Pattern List Custom Object .............................................................. 133
Configuring a Content–Filtering Feature Profile ................................................................. 133
Configuring a UTM Policy for Content-Filtering ................................................................. 135
Configuring Web Filtering (NSM Procedure) ..................................................................... 135
Configuring a URL Pattern List Custom Object ................................................................. 135
Configuring a Custom URL Category List Custom Object ................................................... 136
Configuring a Web Filtering Feature Profile ....................................................................... 136
Configuring a UTM Policy for Web Filtering ...................................................................... 138
# Table of Contents

## Part 3

### Managing J Series Services Routers and SRX Series Services Gateways

#### Chapter 13

Using System Management Features in J Series Services Routers and SRX Series Services Gateways 143

- Managing J Series and SRX Series Device Software Versions Overview 143
- Viewing and Reconciling Device Inventory Overview 143
- Viewing Device Inventory in NSM (NSM Procedure) 144
- Removing a J Series or SRX Series Device from NSM Management (NSM Procedure) 145

#### Chapter 14

Topology Manager 147

- Overview of the NSM Topology Manager 147
- Requisites for a Topology Discovery Overview 147
- Understanding the NSM Topology Manager Toolbar 148

#### Chapter 15

IDP Management in J Series Services Routers and SRX Series Services Gateways 151

- Updating the NSM Attack Database (NSM Procedure) 151
- Loading the IDP Detector Engine on a J Series or SRX Series Device (NSM Procedure) 152
- Updating the Deep Inspection Attack Database on a J Series or SRX Series Device (NSM Procedure) 152

## Part 4

### Monitoring J Series Services Routers and SRX Series Services Gateways

#### Chapter 16

Real Time Monitoring of J Series Services Routers and SRX Series Services Gateways 157

- Realtime Monitor Overview 157
- Viewing Device Status 158
- Viewing Device Monitor Alarm Status (NSM Procedure) 161
- Configuring the Polling Interval for Device Alarm Status (NSM Procedure) 162

## Part 5

### Index

- Index 165
About this Guide

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
- SNMP
- DHCP
- Class of Service
- UTM

Objectives

- Objectives on page xiii
- Audience on page xiv
- Conventions on page xiv
- List of Technical Publications on page xv
- Requesting Technical Support on page xvi
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 xiv defines notice icons used in this guide.

**Table 1: Notice Icons**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📝</td>
<td>Informational note</td>
<td>Indicates important features or instructions.</td>
</tr>
<tr>
<td>🚨</td>
<td>Caution</td>
<td>Indicates a situation that might result in loss of data or hardware damage.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Warning</td>
<td>Alerts you to the risk of personal injury or death.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Laser warning</td>
<td>Alerts you to the risk of personal injury from a laser.</td>
</tr>
</tbody>
</table>

Table 2 on page xiv defines text conventions used in this guide.

**Table 2: Text Conventions**

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bold typeface like this</td>
<td>Represents commands and keywords in text.</td>
<td>■ Issue the clock source command.</td>
</tr>
<tr>
<td></td>
<td>■ Represents keywords</td>
<td>■ Specify the keyword exp-msg.</td>
</tr>
<tr>
<td></td>
<td>■ Represents UI elements</td>
<td>■ Click User Objects</td>
</tr>
<tr>
<td></td>
<td>Represent text that the user must type.</td>
<td>user input</td>
</tr>
</tbody>
</table>
Table 2: Text Conventions (continued)

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>fixed-width font</td>
<td>Represents information as displayed on the terminal screen.</td>
<td>host1# show ip ospf Routing Process OSPF 2 with Router ID 5.5.0.250 Router is an area Border Router (ABR)</td>
</tr>
<tr>
<td>Key names linked</td>
<td>Indicates that you must press two or more keys simultaneously.</td>
<td>Ctrl + d</td>
</tr>
<tr>
<td>with a plus (+) sign</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Italics</td>
<td>Emphasizes words</td>
<td>The product supports two levels of access, user and privileged. clusterID, ipAddress.</td>
</tr>
<tr>
<td></td>
<td>Identifies variables</td>
<td></td>
</tr>
<tr>
<td>The angle bracket</td>
<td>Indicates navigation paths through the UI by clicking menu options and links.</td>
<td>Object Manager &gt; User Objects &gt; Local Objects</td>
</tr>
<tr>
<td>(&gt;)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

Table 3: Syntax Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Words in plain text</td>
<td>Represent keywords</td>
<td>terminal length</td>
</tr>
<tr>
<td>Words in italics</td>
<td>Represent variables</td>
<td>mask, accessListName</td>
</tr>
<tr>
<td>Words separated by the pipe (</td>
<td>) symbol</td>
<td>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.</td>
</tr>
<tr>
<td>Words enclosed in brackets ( [ ] )</td>
<td>Represent optional keywords or variables.</td>
<td>[ internal</td>
</tr>
<tr>
<td>Words enclosed in brackets followed by and asterisk ( [ ])*</td>
<td>Represent optional keywords or variables that can be entered more than once.</td>
<td>[ level1</td>
</tr>
<tr>
<td>Words enclosed in braces ( { } )</td>
<td>Represent required keywords or variables.</td>
<td>{ permit</td>
</tr>
</tbody>
</table>

List of Technical Publications

Table 4 on page xvi 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

<table>
<thead>
<tr>
<th>Guide</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network and Security Manager Installation Guide</td>
<td>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.</td>
</tr>
<tr>
<td>Network and Security Manager Administration Guide</td>
<td>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. 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.</td>
</tr>
<tr>
<td>Network and Security Manager Configuring Firewall/VPN Devices Guide</td>
<td>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.</td>
</tr>
<tr>
<td>Network and Security Manager Online Help</td>
<td>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.</td>
</tr>
<tr>
<td>JUNOS Software Interfaces and Routing Configuration Guide</td>
<td>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.</td>
</tr>
<tr>
<td>JUNOS Software Security Configuration Guide</td>
<td>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).</td>
</tr>
<tr>
<td>JUNOS Software Administration Guide</td>
<td>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 administrator user authentication and access, upgrade software, and diagnose common problems.</td>
</tr>
</tbody>
</table>

**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/customers/support/downloads/710059.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 located at 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 Topics**
- 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 Topics
- 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
- Rebooting the J Series Services Router and SRX Series services gateway
Related Topics

- 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
- Using Templates and Configuration Groups in NSM Overview on page 9

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 Topics
- NSM Installation Overview on page 8
- NSM and Device Management 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 Topics
- 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 Topics
- 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 Topics**
- 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

---

**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 Topics**
- 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 User Authentication in J Series Services Routers and SRX Series Services Gateways on page 13
- Configuring Chassis in J Series Services Routers and SRX Series Services Gateways on page 21
- Configuring USB Modem Interfaces in J Series Services Routers and SRX Series Services Gateways on page 27
- Configuring Policy Options in J Series Services Routers and SRX Series Services Gateways on page 33
- Configuring Routing Options in J Series Services Routers and SRX Series Services Gateways on page 43
- Configuring Protocols for J Series Services Routers and SRX Series Services Gateways on page 69
- Configuring SNMP for Network Management in J Series Services Routers and SRX Series Services Gateways on page 89
- Configuring J Series Services Routers and SRX Series Services Gateways for DHCP on page 95
- Configuring Class of Service in J Series Services Routers and SRX Series Services Gateways on page 99
- Configuring Unified Threat Management Features in J Series Services Routers and SRX Series Services Gateways on page 123
Configuring User Authentication in J Series Services Routers and SRX Series Services Gateways

- Configuring RADIUS Authentication (NSM Procedure) on page 13
- Configuring TACACS+ Authentication (NSM Procedure) on page 14
- Configuring Authentication Order (NSM Procedure) on page 15
- Configuring User Access (NSM Procedure) on page 16
- Configuring Template Accounts (NSM Procedure) on page 17

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 5 on page 14.
5. Click one:
   - New—Adds a new RADIUS server.
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
Table 5: RADIUS Authentication Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the IP address of the RADIUS server.</td>
<td>Enter the IP address of the RADIUS server.</td>
</tr>
<tr>
<td>Secret</td>
<td>Specifies the shared secret (password) of the RADIUS server. The secret is stored as an encrypted value in the configuration database.</td>
<td>Enter the shared secret of the RADIUS server.</td>
</tr>
<tr>
<td>Source Address</td>
<td>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.</td>
<td>Enter the loopback address of the device.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring TACACS+ Authentication (NSM Procedure) on page 14
- Configuring Authentication Order (NSM Procedure) on page 15
- Configuring User Access (NSM Procedure) on page 16

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 6 on page 14.
5. Click one:
   - New—Adds a new TACACS+ server.
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 6: TACACS+ Authentication Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the IP address of the TACACS+ server.</td>
<td>Enter the IP address of the TACACS+ server.</td>
</tr>
</tbody>
</table>
### Table 6: TACACS+ Authentication Configuration Details (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secret</td>
<td>Specifies the shared secret (password) of the TACACS+ server. The secret is stored as an encrypted value in the configuration database.</td>
<td>Enter the shared secret of the TACACS+ server.</td>
</tr>
<tr>
<td>Source Address</td>
<td>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.</td>
<td>Enter the loopback address of the device.</td>
</tr>
</tbody>
</table>

#### Related Topics
- Configuring RADIUS Authentication (NSM Procedure) on page 13
- Configuring Authentication Order (NSM Procedure) on page 15
- Configuring User Access (NSM Procedure) on page 16

### 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.
Configuring User Access (NSM Procedure)

This section includes the following topics:

- Configuring Login Classes on page 16
- Configuring User Accounts on page 17

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 7 on page 16.
5. Click one:
   - **New**—Adds a new login class.
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

### Table 7: Login Class Authentication Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a name for the login class.</td>
<td>Enter a name for the login class.</td>
</tr>
<tr>
<td>Allow Commands</td>
<td>Specifies the operational mode commands that members of a login class can use.</td>
<td>Enter the command name enclosed in quotation marks. For example, “request system reboot”.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Configures the login access privileges to be provided on the device.</td>
<td>Enter a new permission.</td>
</tr>
</tbody>
</table>
**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 8 on page 17.
5. Click one:
   - **New**—Adds a new user account.
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Identifies the user with a unique name.</td>
<td>Enter a unique name for the user.</td>
</tr>
<tr>
<td>Class</td>
<td>Specifies the user’s login class.</td>
<td>Select the class name.</td>
</tr>
</tbody>
</table>

**Login > User > Authentication**

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plain Text Password Value</td>
<td>Specifies the user’s password.</td>
<td>Enter the plain text password for the user.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Configuring RADIUS Authentication (NSM Procedure) on page 13
- Configuring TACACS+ Authentication (NSM Procedure) on page 14
- Configuring Authentication Order (NSM Procedure) on page 15

**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 18
- Creating a Local Template Account on page 19

**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 software 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 9 on page 18.
5. Click one:
   - **New**—Creates a new remote template account.
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.

**Table 9: Remote Template Account Details**

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a name for the user name. Enter the user name. For example, type <code>remote</code></td>
<td></td>
</tr>
<tr>
<td>Uid</td>
<td>Specifies the user identifier for a login account. Enter the number associated with the login account.</td>
<td></td>
</tr>
<tr>
<td>Class</td>
<td>Specifies the login class for the user. Select the login class. For example, select <code>operator</code>.</td>
<td></td>
</tr>
</tbody>
</table>
**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 10 on page 19.
5. Click one:
   - **New**—Creates a new local template account.
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

### Table 10: Local Template Account Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a name for the user name.</td>
<td>Enter the user name. For example, type <code>admin</code></td>
</tr>
<tr>
<td>Uid</td>
<td>Specifies the user identifier for a login account.</td>
<td>Enter the number associated with the login account.</td>
</tr>
<tr>
<td>Class</td>
<td>Specifies the login class for the user.</td>
<td>Select the login class. For example, select <code>superuser</code></td>
</tr>
</tbody>
</table>

**Related Topics**

- Configuring RADIUS Authentication (NSM Procedure) on page 13
- Configuring TACACS+ Authentication (NSM Procedure) on page 14
- Configuring Authentication Order (NSM Procedure) on page 15
Chapter 4
Configuring Chassis in J Series Services
Routers and SRX Series Services
Gateways

- Configuring Aggregated Devices (NSM Procedure) on page 21
- Configuring Chassis Alarms (NSM Procedure) on page 22
- Configuring Routing Engine Redundancy (NSM Procedure) on page 23
- Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors (NSM Procedure) on page 24

Configuring Aggregated Devices (NSM Procedure)

The JUNOS Software 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 11 on page 22.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
Table 11: Aggregated Devices Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure properties for Ethernet aggregated devices.</td>
<td>1. Click <strong>Ethernet</strong> next to Aggregated Devices.</td>
</tr>
<tr>
<td></td>
<td>2. Enter the number of aggregated logical devices available to the router.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 256 devices</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Lacp</strong> next to Ethernet.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>System Priority</strong> box, enter the priority for the aggregated</td>
</tr>
<tr>
<td></td>
<td>Ethernet system.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Link Protection</strong> next to Lacp.</td>
</tr>
<tr>
<td></td>
<td>6. Select the <strong>Non Revertive</strong> check box if you want to disable the</td>
</tr>
<tr>
<td></td>
<td>ability to switch to a better priority link (if one is available) once</td>
</tr>
<tr>
<td></td>
<td>a link is established as active and a collection or distribution is</td>
</tr>
<tr>
<td></td>
<td>enabled.</td>
</tr>
</tbody>
</table>

| Configure properties for sonet aggregated devices.                  | 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 Topics

- Configuring Chassis Alarms (NSM Procedure) on page 22
- Configuring Routing Engine Redundancy (NSM Procedure) on page 23
- Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors (NSM Procedure) on page 24

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 12 on page 23.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.
Table 12: Chassis Alarms Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the alarm type.</td>
<td>1. Select the interface type listed next to Alarm.</td>
</tr>
<tr>
<td></td>
<td>2. Select the alarm type for the chassis condition for each interface type.</td>
</tr>
</tbody>
</table>

Related Topics

- Configuring Aggregated Devices (NSM Procedure) on page 21
- Configuring Routing Engine Redundancy (NSM Procedure) on page 23
- Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors (NSM Procedure) on page 24

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 13 on page 23.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 13: Chassis Redundancy Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure redundancy options.</td>
<td>1. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>2. From the keepalive list, select the time before the backup router takes mastership when it detects loss of the keepalive signal.</td>
</tr>
<tr>
<td></td>
<td>Range: 2 through 10,000</td>
</tr>
<tr>
<td>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.</td>
<td>1. Click Failover next to Redundancy.</td>
</tr>
<tr>
<td></td>
<td>2. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. Select the type of failover.</td>
</tr>
</tbody>
</table>
Table 13: Chassis Redundancy Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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. | 1. Click Graceful Switchover next to Redundancy.  
2. In the Comment box, enter the comment. |

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. | 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:  
   ■ 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 Topics
- Configuring Aggregated Devices (NSM Procedure) on page 21
- Configuring Chassis Alarms (NSM Procedure) on page 22
- Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors (NSM Procedure) on page 24

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 14 on page 25.  
5. Click one:  
   ■ OK—Saves the changes.  
   ■ Cancel—Cancels the modifications.
Table 14: Chassis Routing Engine Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>On disk failure</td>
<td>From the Disk Failure Action list, select the action to instruct the router on detecting the hard disk errors on the Routing Engine.</td>
</tr>
</tbody>
</table>

Related Topics

- Configuring Aggregated Devices (NSM Procedure) on page 21
- Configuring Chassis Alarms (NSM Procedure) on page 22
- Configuring Routing Engine Redundancy (NSM Procedure) on page 23
Chapter 5

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

- Configuring a USB Modem Interface (NSM Procedure) on page 27
- Configuring a Dialer Interface (NSM Procedure) on page 28
- Configuring Dial-in Options on a Dialer Interface (NSM Procedure) on page 29
- Configuring a CHAP Access Profile on a Dialer Interface (NSM Procedure) on page 30

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 15 on page 27.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 15: USB Modem Interface Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of the new interface.</td>
<td>Enter a name for the new interface.</td>
</tr>
<tr>
<td>Dialer Options &gt; Pool</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 15: USB Modem Interface Configuration Details (continued)

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

### Related Topics
- Configuring a Dialer Interface (NSM Procedure) on page 28
- Configuring Dial-in Options on a Dialer Interface (NSM Procedure) on page 29

---

### 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 16 on page 28.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

### Table 16: Dialer Interface Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of the new interface.</td>
<td>Enter a name for the new interface.</td>
</tr>
<tr>
<td>Description</td>
<td>Differentiates between different dialer interfaces.</td>
<td>Enter a description for the new interface.</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Specifies the encapsulation.</td>
<td>Select <strong>PPP</strong> from the encapsulation list.</td>
</tr>
</tbody>
</table>
### Table 16: Dialer Interface Configuration Details (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unit</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unit</td>
<td>Specifies the logical unit.</td>
<td>Enter the unit number.</td>
</tr>
<tr>
<td><strong>Unit &gt; Dialer Options</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pool</td>
<td>Specifies the name of the dialer pool to use for USB modem connectivity.</td>
<td>Enter the name of the dialer pool.</td>
</tr>
<tr>
<td><strong>Unit &gt; Family &gt; Inet &gt; Address</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the source IP address for the dialer interface.</td>
<td>Enter the source IP address.</td>
</tr>
<tr>
<td>Destination</td>
<td>Specifies the destination IP address for the dialer interface.</td>
<td>Enter the destination IP address.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Configuring a USB Modem Interface (NSM Procedure) on page 27
- Configuring Dial-in Options on a Dialer Interface (NSM Procedure) on page 29

### 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 17 on page 29.
5. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

### Table 17: Dialer Interface for Dial-in Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unit &gt; Dialer Options &gt; Incoming Map</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Caller</td>
<td>Specifies the incoming map options for the dialer interface.</td>
<td>Select accept-all to accept all incoming calls.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select caller to accept calls from a specific caller ID.</td>
</tr>
</tbody>
</table>
Table 17: Dialer Interface for Dial-in Configuration Details (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caller</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the caller ID to be accepted on the dialer interface.</td>
<td>Enter the caller ID.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring a Dialer Interface (NSM Procedure) on page 28
- Configuring a USB Modem Interface (NSM Procedure) on page 27

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 18 on page 30.
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 19 on page 31.
7. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 18: CHAP Access Profile Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a name for the profile.</td>
<td>Enter a name for the profile.</td>
</tr>
<tr>
<td>Client</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies a name for the client.</td>
<td>Enter a name for the client.</td>
</tr>
<tr>
<td>Chap Secret</td>
<td>Specifies the CHAP secret.</td>
<td>Enter the CHAP secret.</td>
</tr>
</tbody>
</table>

**NOTE:** Enter the client name and CHAP secret for each client to be included in the CHAP profile.
### Table 19: CHAP Dialer Interface Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unit</strong></td>
<td>Unit</td>
<td>Specifies the logical unit.</td>
</tr>
<tr>
<td><strong>Unit &gt; Ppp Options &gt; Chap</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access profile</td>
<td>Specifies the profile name.</td>
<td>Enter a unique profile name containing a client list and access parameters.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Configuring a Dialer Interface (NSM Procedure) on page 28
- Configuring a USB Modem Interface (NSM Procedure) on page 27
Configuring Policy Options in J Series Services Routers and SRX Series Services Gateways

- Configuring an AS Path in a BGP Routing Policy (NSM Procedure) on page 33
- Configuring an AS Path Group in a BGP Routing Policy (NSM Procedure) on page 34
- Configuring a Community for use in BGP Routing Policy Conditions (NSM Procedure) on page 35
- Configuring a BGP Export Policy Condition (NSM Procedure) on page 36
- Configuring Flap Damping to Reduce the Number of BGP Update Messages (NSM Procedure) on page 37
- Configuring a Routing Policy Statement (NSM Procedure) on page 39
- Configuring Prefix List (NSM Procedure) on page 40

Configuring an AS Path in a BGP Routing Policy (NSM Procedure)

An autonomous system (AS) path is a path to a destination. An AS path consists of the AS numbers of all the network devices that a packet traverses if it takes the associated route to a destination. The AS numbers are assembled in a sequence, or path, that is read from right to left. For example, for a packet to reach a destination using a route with an AS path 5 4 3 2 1, the packet first traverses AS 1 and so on until it reaches AS 5, which is the last AS before its destination.

You can define a match condition based on all of or portions of the AS path. You can create a named AS path and then include it in a BGP routing policy.

To configure an AS path for a BGP routing policy in NSM:
1. In the navigation tree, select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. Click the Configuration tab.
4. In the configuration tree, expand Policy Options.
5. Select As Path.
6. Add or modify the parameters as specified in Table 20 on page 34.
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 20: AS Path Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of the AS path.</td>
<td>Enter a name.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for the AS path.</td>
<td>Enters a comment.</td>
</tr>
<tr>
<td>Path</td>
<td>Specifies the AS path (as an AS number) to be included in the routing policy.</td>
<td>Enter an AS path.</td>
</tr>
</tbody>
</table>

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 21 on page 35.
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 21: AS Path Group Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of the AS path group.</td>
<td>Enter a name.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for the AS path group.</td>
<td>Enter a comment.</td>
</tr>
</tbody>
</table>
| 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. | 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 22 on page 36.
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>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of the community.</td>
<td>Enter the name.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for the community.</td>
<td>Enter the comment.</td>
</tr>
<tr>
<td>Invert Match</td>
<td>Enables you to invert the results for the</td>
<td>Select the check-box if you want to invert the</td>
</tr>
<tr>
<td></td>
<td>community expression.</td>
<td>results. Clear the check-box if you do not want</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to invert the results.</td>
</tr>
<tr>
<td>Members</td>
<td>Specifies one or more community members.</td>
<td>1. Select Members.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the New button or select a member and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>click the Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the member community.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click OK, then click OK again.</td>
</tr>
</tbody>
</table>

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 23 on page 37.
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 23: Condition Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of the condition.</td>
<td>Enter a name.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for the condition.</td>
<td>Enter a comment.</td>
</tr>
</tbody>
</table>
| Route Active On | Enables you to specify the policy condition based on the existing routes and the corresponding route tables. | 1. Select Route Active On.  
2. Select one:  
   - 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 24 on page 38.

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 24: Damping Configuration Details**

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of the damping parameter setting</td>
<td>Enter a name.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for the damping parameter setting</td>
<td>Enter a comment.</td>
</tr>
<tr>
<td>Disable</td>
<td>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.</td>
<td>Select the check-box to disable damping. Clear the check-box to enable damping.</td>
</tr>
<tr>
<td>Half Life</td>
<td>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.</td>
<td>Enter the time limit in minutes or select it from the list.</td>
</tr>
<tr>
<td>Reuse</td>
<td>Indicates the figure-of-merit value below which a suppressed route can be used again.</td>
<td>Enter the value or select it from the list.</td>
</tr>
<tr>
<td>Suppress</td>
<td>Indicates the figure-of-merit value above which a route is suppressed for use or inclusion in advertisements.</td>
<td>Enter the value or select it from the list.</td>
</tr>
</tbody>
</table>
| Max Suppress | Indicates the maximum time in minutes that a route can be suppressed no matter how unstable it has been. | 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 25 on page 39.
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 25: Configuring Policy Statement Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of the policy statement.</td>
<td>1. Click the New button or select a policy statement and click Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select <strong>policy-statement</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the name.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for the policy statement.</td>
<td>1. Click the New button or select a policy statement and click Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select <strong>policy-statement</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the comment.</td>
</tr>
</tbody>
</table>
### Table 25: Configuring Policy Statement Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>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.</td>
<td>1. Click the New button or select a policy statement and click Edit button. 2. Expand <code>policy-statement</code> tree and select From. 3. Enter the From criteria. 4. Expand From tree and specify the match conditions.</td>
</tr>
<tr>
<td>Term</td>
<td>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.</td>
<td>1. Click the New button or select a policy statement and click Edit button. 2. Expand <code>policy-statement</code> 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.</td>
</tr>
<tr>
<td>Then</td>
<td>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.</td>
<td>1. Click the New button or select a policy statement and click Edit button. 2. Expand <code>policy-statement</code> tree and select Then. 3. Specify the parameters for Then criteria. 4. Expand Then tree and specify the actions for each match condition.</td>
</tr>
<tr>
<td>To</td>
<td>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.</td>
<td>1. Click the New button or select a policy statement and click Edit button. 2. Expand <code>policy-statement</code> tree and select To. 3. Enter the To criteria. 4. Expand To tree and specify the match conditions.</td>
</tr>
</tbody>
</table>

### 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 26 on page 41.
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>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of the prefix list.</td>
<td>1. Click the New button or select a prefix list and click Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select prefix-list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the name.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for the prefix list.</td>
<td>1. Click the New button or select a prefix list and click Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select prefix-list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the comment.</td>
</tr>
<tr>
<td>Apply Path</td>
<td>Indicates that the prefix list should include all IP prefixes pointed to</td>
<td>1. Click the New button or select a prefix list and click Edit button.</td>
</tr>
<tr>
<td></td>
<td>by a defined path.</td>
<td>2. Select prefix-list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the path.</td>
</tr>
<tr>
<td>Prefix List Item</td>
<td>Specifies the prefix list item.</td>
<td>1. Click the New button or select a prefix list and click Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Expand prefix-list tree and select Prefix List Item.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the name and comment.</td>
</tr>
</tbody>
</table>
Chapter 7

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

- Configuring Maximum Prefixes (NSM Procedure) on page 43
- Configuring Multicast (NSM Procedure) on page 45
- Configuring Multipath (NSM Procedure) on page 48
- Configuring Options (NSM Procedure) on page 49
- Configuring Route Resolution (NSM Procedure) on page 50
- Configuring Routing Table Groups (NSM Procedure) on page 51
- Configuring Routing Tables (NSM Procedure) on page 53
- Configuring Source Routing (NSM Procedure) on page 55
- Configuring Static Routes (NSM Procedure) on page 56
- Configuring Generated Routes (NSM Procedure) on page 57
- Configuring Graceful Restart (NSM Procedure) on page 58
- Configuring Forwarding Table (NSM Procedure) on page 59
- Configuring Flow Route (NSM Procedure) on page 61
- Configuring Fate Sharing (NSM Procedure) on page 63
- Configuring Martian Addresses (NSM Procedure) on page 64
- Configuring Interface Routes (NSM Procedure) on page 66
- Configuring Instance Export (NSM Procedure) on page 67
- Configuring Instance Import (NSM Procedure) on page 67

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 27 on page 44.

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>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Specifies the comment for the maximum prefix limit.</td>
<td>Enter the comment.</td>
</tr>
<tr>
<td>Limit</td>
<td>Indicates the maximum number of route prefixes. If this limit is reached, a warning is triggered and additional routes are rejected.</td>
<td>Enter limit value or select from the list.</td>
</tr>
<tr>
<td>Log Interval</td>
<td>Indicates the minimum time interval (in seconds) between log messages.</td>
<td>Enter the log interval value or select from the list.</td>
</tr>
</tbody>
</table>
| Threshold | Specifies what is to be done when the routing table reaches the maximum prefix value. The options are: | 1. Expand the Maximum Prefixes tree and select Threshold.  
   - 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.  
   - 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 28 on page 45.
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>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Specifies the comment for the multicast configuration.</td>
<td>Enter the comment.</td>
</tr>
</tbody>
</table>
| Backup Pe Group  | Enables you to configure a backup provider edge (PE) group for ingress PE device redundancy when point-to-multipoint (P2MP) label-switched paths (LSPs) are used for multicast distribution. | 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 28: Configuring Multicast Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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. | 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:  
  - 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 | Enables you to configure multicast forwarding cache properties. These properties include threshold suppression and reuse limits, and timeout values. 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. | 1. Expand the Multicast tree and select Forwarding Cache.  
2. Configure the timeout and threshold values. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Interface     | Enables you to configure the interfaces for multicast properties on which you plan to manage the maximum bandwidth. | 1. Expand the Multicast tree and select Interface.  
2. Configure the interface and the bandwidth. |
| Rpf Check Policy | 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. You can apply policies for disabling reverse-path forwarding (RPF) checks on arriving multicast packets. | 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. | 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. | 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). | 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. |
| Ssm Map       | SSM mapping translates IGMPv1 or IGMPv2 membership reports to an IGMPv3 report allowing you to support an SSM network without requiring all hosts to support IGMPv3. | 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. |
### Table 28: Configuring Multicast Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Traceoptions | Defines tracing options for the multicast group. You can also set up the file management and access control parameters. | 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 29 on page 48.
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 29: Configuring Multipath Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Specifies the comment for the multipath configuration.</td>
<td>Enter the comment.</td>
</tr>
</tbody>
</table>
Table 29: Configuring Multipath Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vpn Unequal Cost</td>
<td>Applies protocol-independent load balancing to VPN routes.</td>
<td>1. Expand the Multipath tree and select Vpn Unequal Cost.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

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 30 on page 50.
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 30: Configuring Options Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Specifies the comment for the message option.</td>
<td>Enter the comment.</td>
</tr>
<tr>
<td>Mark</td>
<td>Specifies the mark for the option.</td>
<td>Enter the mark value or select from the list.</td>
</tr>
</tbody>
</table>
| Syslog | Enables you to configure the generation of system log messages for a particular severity level and all higher levels. | 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 31 on page 51.
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 31: Route Resolution Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Specifies the comment for the route resolution.</td>
<td>Enter a comment.</td>
</tr>
</tbody>
</table>
| Rib        | Specifies the name of the routing table for which the import policies and the resolution routes are configured. | 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.                   | 1. Expand the Resolution tree and select Tracefilter.  
2. Specify the filter policies for the routing table. |
| Traceoptions| Defines tracing options for route resolution.                            | 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 software uses when importing routes. In the same way, each routing table group optionally contains one routing table that the JUNOS software 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 32 on page 52.
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 32: Rib Group Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the unique name for the routing table group.</td>
<td>1. Expand the <strong>Routing Options</strong> tree and select <strong>Rib Group</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the New button or select a routing table group and click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the name for the routing table group.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for the routing table group.</td>
<td>1. Expand the <strong>Routing Options</strong> tree and select <strong>Rib Group</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the New button or select a routing table group and click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the comment for the routing table group.</td>
</tr>
<tr>
<td>Export Rib</td>
<td>Specifies the routing table from which the JUNOS software exports routing information.</td>
<td>1. Expand the <strong>Routing Options</strong> tree and select <strong>Rib Group</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the New button or select a routing table group and click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the name of the routing table.</td>
</tr>
<tr>
<td>Import Policy</td>
<td>Enables you to apply one or more policies to routes imported into the routing table group.</td>
<td>1. Expand the <strong>rib-group</strong> tree and select <strong>Import Policy</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Set up the import policies for the routing table group.</td>
</tr>
</tbody>
</table>
### Table 32: Rib Group Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import Rib</td>
<td>Specifies the name of the routing table into which the JUNOS software 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.</td>
<td>1. Expand the rib-group tree and select Import Policy. &lt;br&gt;2. Enter the name of the routing table.</td>
</tr>
</tbody>
</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 software 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 33 on page 54.
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 33: Rib Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Name       | Specifies the unique name for the routing table.                          | 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.                           | 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.     | 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. | 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.         | 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. | 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. | 1. Expand the **Rib** tree and select **Maximum Prefixes**.  
                                                        | 2. Set up the **Maximum Prefixes** and the **Threshold**.                                                                                   |
### Table 33: Rib Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Multipath | Enables you to configure the multipath option in the routing table for load sharing between external BGP and internal BGP. | 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. | 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 34 on page 55.
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 34: Source Routing Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Specifies the comment for the source routing configuration.</td>
<td>Enter the comment.</td>
</tr>
</tbody>
</table>
Table 34: Source Routing Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ip</td>
<td>Specifies the IPv4 addressing family for source routing.</td>
<td>Select the check box.</td>
</tr>
<tr>
<td>Ipv6</td>
<td>Specifies the IPv6 addressing family for source routing.</td>
<td>Select the check box.</td>
</tr>
</tbody>
</table>

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 35 on page 57.
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 35: Static Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Specifies the comment for the static route.</td>
<td>Enter the comment.</td>
</tr>
<tr>
<td>Rib Group</td>
<td>Specifies the routing table group name for which the static route is configured.</td>
<td>Enter the name.</td>
</tr>
</tbody>
</table>
| 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. | 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. | 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 36 on page 58.
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 36: Generated Routes Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Specifies the comment for the generated route.</td>
<td>Enter a comment.</td>
</tr>
<tr>
<td>Defaults</td>
<td>Enables you to specify globally generated route options. These are treated as global defaults and apply to all the generated routes you configure.</td>
<td>1. Expand the Generate tree and select Defaults.&lt;br&gt;2. Configure the default route options.</td>
</tr>
<tr>
<td>Route</td>
<td>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.</td>
<td>1. Expand the Generate tree and select Route.&lt;br&gt;2. Configure the individual route options.</td>
</tr>
</tbody>
</table>

### 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 37 on page 59.
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 37: Graceful Restart Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Specifies the comment for the graceful restart.</td>
<td>Enter a comment.</td>
</tr>
<tr>
<td>Disable</td>
<td>Specifies whether graceful restart is enabled for the device.</td>
<td>□ Select the check box to disable graceful restart.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>□ Clear the check box to enable graceful restart.</td>
</tr>
<tr>
<td>Restart Duration</td>
<td>Specifies the duration of the grace period for the device to restart.</td>
<td>Enter a value for the duration or select a value from the list.</td>
</tr>
</tbody>
</table>

### 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 38 on page 60.

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 38: Forwarding Table Fields**

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Specifies the comment for the forwarding table.</td>
<td>Enter a comment.</td>
</tr>
<tr>
<td>None</td>
<td>Specifies that no next-hop parameter is to be added to the forwarding table.</td>
<td>Select the option button.</td>
</tr>
<tr>
<td>indirect-next-hop</td>
<td>Specifies that the forwarding table supports indirectly connected next hops.</td>
<td>Select the option button to enable indirect-next-hop.</td>
</tr>
<tr>
<td>no-indirect-next-hop</td>
<td>Specifies that the forwarding table does not support indirectly connected next hops.</td>
<td>Select the option button to enable no-indirect-next-hop.</td>
</tr>
<tr>
<td>Unicast Reverse Path</td>
<td>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.</td>
<td>Select the path from the drop-down list.</td>
</tr>
</tbody>
</table>
| Export            | Enables you to apply one or more policies to routes being exported from the routing table into the forwarding table. | 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 39 on page 61.
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 39: Flow Route Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Specifies the comment for the flow route.</td>
<td>Enter a comment.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Route</th>
<th>Specifies the name of the flow route.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td></td>
</tr>
</tbody>
</table>

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.
### Table 39: Flow Route Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| **Comment**       | Specifies the comment for the flow route.                                 | 1. Expand the Flow tree and select Route.  
2. Click the New button or select a flow route and click the Edit button.  
3. Enter the comment for the flow route.                                      |
| **Match**         | Specifies the conditions that the packet must match for the packet to be included in flow route. Match conditions are:  
- Destination Port  
- DSCP  
- Fragment  
- Icmp Code  
- Icmp Type  
- Packet Length  
- Port  
- Protocol  
- Source Port  
- Tcp Flag | 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. | 1. Expand the Route tree and select Then.  
2. Configure the then conditions for the packet.                               |
| **Validation**    | 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. | 1. Expand the Flow tree and select Validation.  
2. Enter the comment for the validation procedure.                             |
| **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. | 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. | 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 40 on page 63.
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 40: Fate Sharing Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Specifies the comment for the fate sharing</td>
<td>Enter a comment.</td>
</tr>
<tr>
<td>Group</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 40: Fate Sharing Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Name   | Specifies the name of the fate sharing group. | 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. | 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. | 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. | 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 41 on page 65.
7. Click one:
### Table 41: Configuring Martian Address Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Address | Specifies the martian address or the destination prefix of a series of martian addresses that are to be allowed or disallowed. | 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. | 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. | 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 | Specifies match criteria for the route’s mask length with the martian address. The criteria are:  
- Exact  
- Longer  
- Or longer  
- Upto  
- Through  
- Prefix Length Range | 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. |

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

You can associate a routing table group with the device’s interfaces and specify routing tables into which interface routes are imported. To define the routing tables into which interface routes are imported, you create a routing table group and associate it with the device’s interfaces.

To configure interface routes in NSM:

1. In the navigation tree, select Device Manager > Devices.
2. In the Devices list, double click the device to select it.
3. Click the Configuration tab.
4. In the configuration tree, expand Routing Options.
5. Select Interface Routes.
6. Add or modify the parameters as specified in Table 42 on page 66.
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 42: Interface Routes Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Specifies the comment for the interface route.</td>
<td>Enter a comment.</td>
</tr>
<tr>
<td>Family</td>
<td>Specifies the address family as IPv4 or IPv6.</td>
<td>1. Expand the Interface Routes tree and select Family.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the New button or select a family name and click the Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the family name and comment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Set up the export policy and import policy.</td>
</tr>
</tbody>
</table>
Table 42: Interface Routes Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Rib Group | Specifies the routing table groups to which interface routes are imported. | 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.
Configuring Protocols for J Series Services Routers and SRX Series Services Gateways

- Configuring BGP (NSM Procedure) on page 69
- Configuring 802.1X Authentication (NSM Procedure) on page 72
- Configuring GVRP (NSM Procedure) on page 74
- Configuring IGMP (NSM Procedure) on page 75
- Configuring MSTP (NSM Procedure) on page 77
- Configuring OSPF (NSM Procedure) on page 79
- Configuring RIP (NSM Procedure) on page 82
- Configuring VSTP (NSM Procedure) on page 84
- Configuring VRRP (NSM Procedure) on page 86

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 43 on page 70.
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 43: BGP Configuration Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>The general parameters to be set up for applying BGP.</td>
<td>1. Expand the Protocol tree.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select BGP and select General tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the general parameters like comment, description, local address, hold time, etc.</td>
</tr>
<tr>
<td>Path Selection</td>
<td>Enables you to specify the path selection criteria.</td>
<td>1. Expand the Protocol tree.</td>
</tr>
<tr>
<td>Traceoptions</td>
<td>Defines trace options for IGMP snooping.</td>
<td>2. Select BGP and select Traceoptions tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Set up the file and flag parameters.</td>
</tr>
<tr>
<td>Metric Out</td>
<td>Enables you to specify the metric value to add to the routes transmitted to the neighbor.</td>
<td>1. Expand the Protocol tree.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select BGP and select Metric Out tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Set up the metric value and minimum IGP.</td>
</tr>
<tr>
<td>Multihop</td>
<td>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.</td>
<td>1. Expand the Protocol tree.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select BGP and select Multihop tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Set up the comment, TtI and specify whether the next hop has to be changed.</td>
</tr>
<tr>
<td>Field</td>
<td>Function</td>
<td>Your Action</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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. | 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 routing table from BGP. | 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. | 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. | 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 routing table from BGP. | 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 | 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. |
| Graceful Restart | Enables you to specify the graceful restart parameters. | 1. Expand the Protocol tree.  
2. Select BGP and select Graceful Restart tab.  
3. Specify the graceful restart parameters. |
### Table 43: BGP Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Bfd Liveness Detection | Enables you to configure bidirectional forwarding detection (BFD) timers. | 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.                                       | 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 72
2. Configuring Static MAC Bypass on page 74

### 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.
3. Select Authenticator > Interface.
4. Click the Add icon.
5. Add/modify member settings for the interface as specified in Table 44 on page 73.
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 44: 802/1X Authentication for an Interface

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Profile Name</td>
<td>Specifies the name for the profile.</td>
<td>Enter the name</td>
</tr>
<tr>
<td>Interface</td>
<td>Specifies the interface for which 802.1X authentication is being configured.</td>
<td>Select Interface. Click the Add icon.</td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the interface name.</td>
<td>Enter the interface name.</td>
</tr>
<tr>
<td>Disable</td>
<td>Disables 802.1X authentication on the interface.</td>
<td>Select to disable authentication.</td>
</tr>
<tr>
<td>Supplicant</td>
<td>Specifies the mode to be adopted for supplicants:</td>
<td>Select the required mode.</td>
</tr>
<tr>
<td></td>
<td>■ Single — allows only one host for authentication.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Multiple — allows multiple hosts for authentication. Each host is checked before being admitted to the network.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Single authentication for multiple hosts — Allows multiple hosts but only the first is authenticated.</td>
<td></td>
</tr>
<tr>
<td>Retries</td>
<td>Maximum number of retries</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td>Quiet Period</td>
<td>Specifies the port waiting time after an authentication failure.</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td>Transmit Period</td>
<td>Specifies the retransmit interval.</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td>Supplicant Timeout</td>
<td>Port timeout value for the response from the supplicant.</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td>Server Timeout</td>
<td>Port timeout value for the response from the RADIUS server.</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td>Maximum Requests</td>
<td>Specifies the maximum number of authentication requests to be made to the server.</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td>Guest Vlan</td>
<td>Specifies the guest VLAN to move the interface to in case of an authentication failure.</td>
<td>Enter the VLAN name.</td>
</tr>
<tr>
<td>Reauthentication</td>
<td>Specifies enabling reauthentication on the selected interface.</td>
<td>Select Reauthentication.</td>
</tr>
<tr>
<td></td>
<td>Select one:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ reauthentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ no-reauthentication</td>
<td></td>
</tr>
</tbody>
</table>
**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 45 on page 75.
**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>
<thead>
<tr>
<th>Table 45: GVRP Configuration Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option</strong></td>
</tr>
<tr>
<td>Disable</td>
</tr>
<tr>
<td>Join Timer</td>
</tr>
<tr>
<td>Leave Times</td>
</tr>
<tr>
<td>Leaveall Times</td>
</tr>
</tbody>
</table>

---

**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 46 on page 76.
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 46: IGMP Configuration Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for IGMP.</td>
<td>Enter a comment.</td>
</tr>
<tr>
<td>Query Interval</td>
<td>Defines how often the device sends general host-query messages.</td>
<td>Select the query interval.</td>
</tr>
<tr>
<td>Query Response Interval</td>
<td>Defines how long the query router/switch waits to receive a response to a host-query message from a host.</td>
<td>Enter the query response interval.</td>
</tr>
<tr>
<td>Query Last Member Interval</td>
<td>Defines how often the device sends group-specific query messages.</td>
<td>Enter the query last member interval.</td>
</tr>
<tr>
<td>Robust Count</td>
<td>Defines the number of intervals the device waits before removing a multicast group from the multicast forwarding table.</td>
<td>Select the robust count.</td>
</tr>
<tr>
<td>Accounting</td>
<td>Specifies whether accounting is enabled for IGMP.</td>
<td>Select to enable accounting.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Specifies the interface and the multicast group that has to be associated with IGMP.</td>
<td>1. Expand the IGMP tree and select Interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the New button or select an interface and click Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Select Disable to disable IGMP on the interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Select the version.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Specify the Ssm Map.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. You can enable Immediate Leave and Promiscuous Mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7. You can enable accounting on the interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8. Select the option Interface &gt; Static to configure the multicast group to be associated with the interface.</td>
</tr>
</tbody>
</table>
### 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 47 on page 77.

**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 47: MSTP Configuration Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable</td>
<td>Specifies whether MSTP must be disabled on the port.</td>
<td>Click to select the option.</td>
</tr>
<tr>
<td>Configuration Name</td>
<td>Specifies the configuration name.</td>
<td>Type a name.</td>
</tr>
<tr>
<td>Revision Level</td>
<td>Specifies the configuration revision level.</td>
<td>Select a value.</td>
</tr>
<tr>
<td>Max Hops</td>
<td>Specifies the number of hops in a region before the BPDUs are discarded.</td>
<td>Select a value.</td>
</tr>
</tbody>
</table>
### Table 47: MSTP Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Age</td>
<td>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.</td>
<td>Select a value.</td>
</tr>
<tr>
<td>Hello time</td>
<td>Specifies the hello time for all MST instances.</td>
<td>Select a value.</td>
</tr>
<tr>
<td>Forward Delay</td>
<td>Specifies the number of seconds a port waits before changing from its spanning-tree learning and listening states to the forwarding state.</td>
<td>Select a value.</td>
</tr>
<tr>
<td>Bridge Priority</td>
<td>Specifies the bridge priority.</td>
<td>Enter a value.</td>
</tr>
<tr>
<td>Bpdu Block on Edge</td>
<td>Specifies whether Bpdu blocks must be processed.</td>
<td>Select to enable the feature.</td>
</tr>
</tbody>
</table>
| Interface            | Specifies MSTP settings for the interface.                               | 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:  
|                      |                                                                          | ■ Block  
|                      |                                                                          | ■ Alarm  
| Msti                 | Specifies MST instances settings for an interface or VLAN.               | 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 48 on page 79.
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 48: OSPF Configuration Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 48: OSPF Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Specifies the comment for OSPF.</td>
<td>1. Enter the comment.</td>
</tr>
<tr>
<td>Disable</td>
<td>Specifies whether to disable the OSPF configuration.</td>
<td>1. Specify whether to enable or disable OSPF.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ To enable OSPF, clear the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ To disable OSPF, select the check box.</td>
</tr>
<tr>
<td>Prefix Export Limit</td>
<td>Configure a limit to the number of prefixes to be exported.</td>
<td>1. Enter the prefix export limit or select from the list.</td>
</tr>
<tr>
<td>Rib Group</td>
<td>Specifies the routing table group.</td>
<td>1. Select rib group from the list.</td>
</tr>
<tr>
<td>Route Type Community</td>
<td>Specifies an extended community value to encode the OSPF route type.</td>
<td>1. Select route type community from the list.</td>
</tr>
<tr>
<td>Domain VPN Tag</td>
<td>Virtual private network (VPN) tag for OSPFv2 external routes generated by the provider edge (PE) router.</td>
<td>1. Enter the domain VPN tag or select from the list.</td>
</tr>
<tr>
<td>Preference</td>
<td>Specifies the route preference for OSPF internal routes.</td>
<td>1. Enter the preference or select from the list.</td>
</tr>
<tr>
<td>External Preference</td>
<td>Specifies the external route preference.</td>
<td>1. Enter the external route preference or select from the list.</td>
</tr>
<tr>
<td>Reference Bandwidth</td>
<td>Specifies the reference bandwidth used in calculating the default interface cost.</td>
<td>1. Enter the reference bandwidth.</td>
</tr>
<tr>
<td>No RFC 1583</td>
<td>Disable compatibility with RFC 1583. Disabling compatibility with RFC 1583 can prevent routing loops.</td>
<td>1. Specify whether to configure RFC 1583.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ To enable compatibility with RFC 1583, clear the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ To disable compatibility with RFC 1583, select the check box.</td>
</tr>
<tr>
<td>No NSSA ABR</td>
<td>Disable compatibility with NSSA ABR.</td>
<td>1. Specify whether NSSA ABR has to be configured.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ To enable NSSA ABR, clear the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ To disable NSSA ABR, select the check box.</td>
</tr>
<tr>
<td>Area</td>
<td>Enables you to set up the area details for OSPF.</td>
<td></td>
</tr>
</tbody>
</table>
Table 48: OSPF Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain ID</td>
<td>Enables you to configure domain ID for the OSPF.</td>
<td>1. Expand the OSPF tree and select Domain ID.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Specify the domain ID.</td>
</tr>
<tr>
<td>Export</td>
<td>Enables you to specify the export policies to be configured on the peer.</td>
<td>1. Expand the OSPF tree and select Export.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Specify the export policies.</td>
</tr>
<tr>
<td>Graceful Restart</td>
<td>Enables you to specify the graceful restart parameters for OSPF.</td>
<td>1. Expand the OSPF tree and select Graceful Restart.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Set up the graceful restart parameters.</td>
</tr>
<tr>
<td>Import</td>
<td>Enables you to specify the import policies to be configured on the peer.</td>
<td>1. Expand the OSPF tree and select Import.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Specify the import policies.</td>
</tr>
<tr>
<td>Overload</td>
<td>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.</td>
<td>1. Expand the OSPF tree and select Overload.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Specify the comment and timeout.</td>
</tr>
<tr>
<td>Sham Link</td>
<td>Enables you to configure the local endpoint of a sham link.</td>
<td>1. Expand the OSPF tree and select Sham Link.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enable the feature and specify the comment and local address.</td>
</tr>
<tr>
<td>SPF Options</td>
<td>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.</td>
<td>1. Expand the OSPF tree and select SPF Options.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Specify the comment, delay, holddown and rapid runs.</td>
</tr>
</tbody>
</table>
Table 48: OSPF Configuration Fields *(continued)*

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traceoptions</td>
<td>Enables you to configure OSPF protocol level tracing options.</td>
<td>1. Expand the OSPF tree and select Traceoptions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Expand the Traceoptions tree and set up the file and flag parameters.</td>
</tr>
</tbody>
</table>

**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 49 on page 83.
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 49: RIP Configuration Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Specifies the comment for RIP.</td>
<td>1. Enter the comment.</td>
</tr>
<tr>
<td>Metric In</td>
<td>Specifies the metric to add to incoming routes when advertising into RIP routes that were learned from other protocols.</td>
<td>1. Specify the metric to add incoming routes.</td>
</tr>
<tr>
<td>Message Size</td>
<td>Specifies the number of route entries to be included in every RIP update message.</td>
<td>1. Enter the message size or select from the list.</td>
</tr>
<tr>
<td>Hold Down</td>
<td>Time period the expired route is retained in the routing table before being removed.</td>
<td>1. Enter the hold down value or select from the list.</td>
</tr>
<tr>
<td>Route Timeout</td>
<td>Specifies the route timeout interval for RIP.</td>
<td>1. Enter the route timeout or select from the list.</td>
</tr>
<tr>
<td>Update Interval</td>
<td>Enables you to configure an update time interval to periodically send out routes learned by RIP to neighbors.</td>
<td>1. Enter the update interval or select from the list.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>The type of authentication for RIP route queries received on an interface.</td>
<td>1. Select authentication type from the list.</td>
</tr>
<tr>
<td>Authentication Key</td>
<td>Authentication key for RIP route queries received on an interface.</td>
<td>1. Enter the authentication key.</td>
</tr>
<tr>
<td>Graceful Restart</td>
<td>Enables you to specify the graceful restart parameters for RIP.</td>
<td>1. Expand the RIP tree and select Graceful Restart.</td>
</tr>
<tr>
<td>Group</td>
<td>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.</td>
<td>1. Expand the RIP tree and select Group.</td>
</tr>
<tr>
<td>Import</td>
<td>Enables you to specify the import policies to be configured on the peer.</td>
<td>1. Expand the RIP tree and select Import.</td>
</tr>
<tr>
<td>Receive</td>
<td>Enables you to configure RIP receive options.</td>
<td>1. Expand the RIP tree and select Receive.</td>
</tr>
</tbody>
</table>

---

**Configuring RIP (NSM Procedure)**
### Table 49: RIP Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIB Group</td>
<td>The routing table group.</td>
<td>1. Expand the RIP tree and select Rib Group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Specify the comment and ribgroup name.</td>
</tr>
<tr>
<td>Send</td>
<td>Enables you to configure RIP send options.</td>
<td>1. Expand the RIP tree and select Send.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Specify the send options.</td>
</tr>
<tr>
<td>Traceoptions</td>
<td>Enables you to configure RIP protocol level tracing options.</td>
<td>1. Expand the RIP tree and select Traceoptions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Expand the Traceoptions tree and set up the file and flag parameters.</td>
</tr>
</tbody>
</table>

### 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 &gt; 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 50 on page 85.
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 50: VSTP Configuration Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSTP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies comment for OSPF.</td>
<td>1. Expand the Protocol tree and select VSTP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the comment.</td>
</tr>
<tr>
<td>Disable</td>
<td>Specifies whether to disable the VSTP configuration.</td>
<td>1. Expand the Protocol tree and select VSTP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Specify whether to disable VSTP.</td>
</tr>
<tr>
<td>Bridge Priority</td>
<td>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.</td>
<td>1. Expand the Protocol tree and select VSTP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the bridge priority.</td>
</tr>
<tr>
<td>Max Age</td>
<td>Specifies the maximum age of received protocol BPDUs.</td>
<td>1. Expand the Protocol tree and select VSTP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the max age or select from the list.</td>
</tr>
<tr>
<td>Hello Time</td>
<td>The time interval at which the root bridge transmits configuration BPDUs.</td>
<td>1. Expand the Protocol tree and select VSTP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the hello time or select from the list.</td>
</tr>
<tr>
<td>Forward Delay</td>
<td>Specifies how long a bridge interface remains in the listening and learning states before transitioning to the forwarding state.</td>
<td>1. Expand the Protocol tree and select VSTP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the forward delay time or select from the list.</td>
</tr>
<tr>
<td>Interface</td>
<td>Specifies the interface to be associated with VSTP.</td>
<td>1. Expand the Protocol tree.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select VSTP and expand the tree.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Select Interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Set up the priority, cost, mode, edge and specify whether the interface has to be disabled.</td>
</tr>
<tr>
<td>Traceoptions</td>
<td>Enables you to configure VSTP level tracing options.</td>
<td>1. Expand the Protocol tree.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select VSTP and expand the tree.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Select Traceoptions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Set up the file and flag parameters.</td>
</tr>
</tbody>
</table>
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 51 on page 86.
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 51: VRRP Configuration Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRRP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies comment for VRRP.</td>
<td>1. Expand the Protocol tree and select VRRP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the comment.</td>
</tr>
</tbody>
</table>
### Table 51: VRRP Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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. | 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.                     | 1. Expand the Protocol tree.  
2. Select VRRP and expand the tree.  
3. Select Traceoptions.  
4. Set up the file and flag parameters. |
Chapter 9
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 89
- Configuring SNMP Agents and Communities (NSM Procedure) on page 90
- Configuring SNMP Trap Groups (NSM Procedure) on page 91
- Configuring SNMP Views (NSM Procedure) on page 92

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 52 on page 89.
5. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

Table 52: Basic System Identification Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Name</td>
<td>Specifies a system name for the device.</td>
<td>Enter the system name as a free-form text string.</td>
</tr>
<tr>
<td>Description</td>
<td>Provides a description for the system.</td>
<td>Enter a description for the system. For example, type J4350 with 4 PIMs.</td>
</tr>
<tr>
<td>Location</td>
<td>Specifies the system location information.</td>
<td>Enter the system location information (such as a lab name and a rack name).</td>
</tr>
</tbody>
</table>
Table 52: Basic System Identification Details (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact</td>
<td>Specifies the contact information for the system.</td>
<td>Enter the system contact information (such as a name and a phone number).</td>
</tr>
<tr>
<td>Snmp &gt; Engine Id</td>
<td>Use Mac Address</td>
<td>Select this option.</td>
</tr>
</tbody>
</table>

Snmp > Community

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a name for the community.</td>
<td>Enter a name for the community.</td>
</tr>
<tr>
<td>View</td>
<td>Specifies the view associated with the community.</td>
<td>Enter the view name.</td>
</tr>
<tr>
<td>Authorization</td>
<td>Specifies the access granted to the community.</td>
<td>Select an access to be granted for the community. For example, type read-write.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring SNMP Agents and Communities (NSM Procedure) on page 90
- Configuring SNMP Trap Groups (NSM Procedure) on page 91
- Configuring SNMP Views (NSM Procedure) on page 92

Configuring SNMP Agents and Communities (NSM Procedure)

To configure SNMP agents and communities:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab and then double-click the device for which you want to configure SNMP agents and communities.
3. Click the Configuration tab. In the configuration tree, select Snmp > Community.
4. Add or modify community and client information as specified in Table 53 on page 90.
5. Click one:
   - New—Creates a new community.
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 53: SNMP Agents and Community Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a name for the community.</td>
<td>Enter a name for the community.</td>
</tr>
<tr>
<td>View</td>
<td>Specifies the view associated with the community.</td>
<td>Enter the view name.</td>
</tr>
<tr>
<td>Authorization</td>
<td>Specifies the access granted to the community.</td>
<td>Select an access to be granted for the community. For example, type read-write.</td>
</tr>
</tbody>
</table>
Table 53: SNMP Agents and Community Configuration Details (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies community access to a client at a particular IP address.</td>
<td>Enter the IP address.</td>
</tr>
<tr>
<td>Restrict</td>
<td>Restricts client access to the specified IP address.</td>
<td>Select this option to restrict client access for the specified IP address.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring Basic System Identification for SNMP (NSM Procedure) on page 89
- Configuring SNMP Trap Groups (NSM Procedure) on page 91
- Configuring SNMP Views (NSM Procedure) on page 92

Configuring SNMP Trap Groups (NSM Procedure)

To configure trap 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 SNMP trap groups.
3. Click the Configuration tab. In the configuration tree, select Snmp > Trap Group.
4. Add or modify SNMP trap group as specified in Table 54 on page 91.
5. Click one:
   - New—Creates a new SNMP trap group.
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 54: SNMP Trap Group Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a name for the trap group.</td>
<td>Enter a name for the trap group.</td>
</tr>
<tr>
<td>Version</td>
<td>Specifies the version number of SNMP traps.</td>
<td>Select the version number for the SNMP trap.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Specifies the SNMP trap port number.</td>
<td>Enter the trap port number.</td>
</tr>
<tr>
<td>Routing Instance</td>
<td>Specifies a routing instance for trap targets.</td>
<td>Enter the name of the routing instance.</td>
</tr>
</tbody>
</table>

Snmp > Trap Group > Categories
Table 54: SNMP Trap Group Configuration Details (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Define the types of traps that will be sent to the targets of the named trap group.</td>
<td>Select the trap type.</td>
</tr>
</tbody>
</table>

Snmp > Trap Group > Targets

| Name                 | Specifies the IPv4 or IPv6 address of the system to receive traps.       | Enter the IPv4 or IPv6 address of the system, but not a hostname. |

Related Topics

- Configuring Basic System Identification for SNMP (NSM Procedure) on page 89
- Configuring SNMP Agents and Communities (NSM Procedure) on page 90
- Configuring SNMP Views (NSM Procedure) on page 92

Configuring SNMP Views (NSM Procedure)

To configure SNMP views:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab and then double-click the device for which you want to configure SNMP views.
3. Click the Configuration tab. In the configuration tree, select Snmp > View.
4. Add or modify SNMP views as specified in Table 55 on page 92.
5. Click one:
   - New—Creates a new view.
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 55: SNMP View Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a name for the view.</td>
<td>Enter a name for the view.</td>
</tr>
</tbody>
</table>

Snmp > View > Oid

| Name                 | Specifies the MIB for the view.                                          | Enter the OID of the MIB in either dotted integer or subtree name format. |
| Include or Exclude   | Specifies whether the view includes or excludes the MIB.                 | Select this option. |

Related Topics

- Configuring Basic System Identification for SNMP (NSM Procedure) on page 89
Chapter 9: Configuring SNMP for Network Management in J Series Services Routers and SRX Series Services Gateways

- Configuring SNMP Agents and Communities (NSM Procedure) on page 90
- Configuring SNMP Trap Groups (NSM Procedure) on page 91
Chapter 10
Configuring J Series Services Routers and SRX Series Services Gateways for DHCP

- Configuring the Device as a DHCP Server (NSM Procedure) on page 95
- Configuring the Device as a DHCP Client (NSM Procedure) on page 97

**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 56 on page 95.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Lease Time</td>
<td>Specifies the maximum length of time in seconds for which a client can request and hold a lease on a DHCP server.</td>
<td>Select the maximum lease time.</td>
</tr>
<tr>
<td>Option</td>
<td>Function</td>
<td>Your Action</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Default Lease Time</td>
<td>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.</td>
<td>Select the default lease time.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>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.</td>
<td>Enter the domain name.</td>
</tr>
<tr>
<td>Boot File</td>
<td>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.</td>
<td>Enter the location of the boot file on the boot server. The filename can include a path name.</td>
</tr>
<tr>
<td>Boot Server</td>
<td>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.</td>
<td>Enter the address of a boot server. You must specify an IPv4 address, not a hostname.</td>
</tr>
<tr>
<td>Server Identifier</td>
<td>Specifies the server identifier. This is an optional setting that can be used to identify a DHCP server in a DHCP message.</td>
<td>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).</td>
</tr>
</tbody>
</table>

**Dhcp > Pool**

<table>
<thead>
<tr>
<th>Name</th>
<th>Specifies the logical subnet address or netmask.</th>
<th>Enter the IP address pool range.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Specifies lowest IP address in the pool that is available for dynamic address assignment.</td>
<td>Enter the IP address.</td>
</tr>
<tr>
<td>High</td>
<td>Specifies highest IP address in the pool that is available for dynamic address assignment.</td>
<td>Enter the IP address.</td>
</tr>
</tbody>
</table>

**Dhcp > Domain Search**

<table>
<thead>
<tr>
<th>Name</th>
<th>Specifies the domain search suffixes to be used by the clients.</th>
<th>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.</th>
</tr>
</thead>
</table>
### Table 56: DHCP Server Configuration Details *(continued)*

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dhcp &gt; Name Server</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Defines a Domain Name System (DNS) name server.</td>
<td>Enter the address of the name server. To configure multiple name servers, include multiple address options.</td>
</tr>
<tr>
<td><strong>Dhcp &gt; Option</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the ID number that indexes the option and must be unique across a DHCP server.</td>
<td>Select the ID number.</td>
</tr>
<tr>
<td>Flag</td>
<td>Specifies the option type.</td>
<td>Select the option type.</td>
</tr>
<tr>
<td><strong>Dhcp &gt; Static Binding</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the MAC address of the client. This is a hardware address that uniquely identifies a client on the network.</td>
<td>Enter the MAC address of the client.</td>
</tr>
<tr>
<td><strong>Dhcp &gt; Static Binding &gt; Fixed Address</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the fixed IP address assigned to the client. Typically a client has one address assigned, but you can assign more.</td>
<td>Enter the fixed IP address.</td>
</tr>
</tbody>
</table>

**Related Topics**: Configuring the Device as a DHCP Client (NSM Procedure) on page 97

---

**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 57 on page 98.

6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

### Table 57: DHCP Client Configuration Details

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

**Related Topics**
- Configuring the Device as a DHCP Server (NSM Procedure) on page 95
Chapter 11
Configuring Class of Service in J Series Services Routers and SRX Series Services Gateways

- Configuring CoS Classifiers (NSM Procedure) on page 99
- Configuring CoS Code Point Aliases (NSM Procedure) on page 102
- Configuring CoS Drop Profile (NSM Procedure) on page 103
- Configuring CoS Forwarding Classes (NSM Procedure) on page 105
- Configuring CoS Forwarding Policy (NSM Procedure) on page 106
- Configuring CoS Fragmentation Maps (NSM Procedure) on page 108
- Configuring CoS Host Outbound Traffic (NSM Procedure) on page 109
- Configuring CoS Interfaces (NSM Procedure) on page 110
- Configuring CoS Rewrite Rules (NSM Procedure) on page 115
- Configuring CoS Schedulers (NSM Procedure) on page 118
- Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 120

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 software 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 58 on page 100.
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 58: Configuring and Applying Behavior Aggregate Classifiers**

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure behavior aggregate classifiers for DiffServ CoS.</td>
<td>1. Click <strong>Add new entry</strong> next to Dscp. 2. In the Name box, type the name of the behavior aggregate classifier—for example, <em>ba-classifier</em>. 3. In the Import box, type the name of the default DSCP map.</td>
</tr>
<tr>
<td>Configure a best-effort forwarding class classifier.</td>
<td>1. Click <strong>Add new entry</strong> next to Forwarding class. 2. In the Class name box, type the name of the previously configured best-effort forwarding class—for example, <em>be-class</em>. 3. Click <strong>Add new entry</strong> next to Loss priority. 4. From the Loss val list, select <em>high</em>. 5. Click <strong>Add new entry</strong> next to Code points. 6. In the Value box, type the value of the high-priority code point for best-effort traffic—for example, <em>00001</em>. 7. Click <strong>OK</strong> three times.</td>
</tr>
</tbody>
</table>
### Table 58: Configuring and Applying Behavior Aggregate Classifiers (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure an expedited forwarding class classifier</td>
<td>1. Click <strong>Add new entry</strong> next to Forwarding class.</td>
</tr>
<tr>
<td></td>
<td>2. In the Class name box, type the name of the previously configured expedited forwarding—for example, <strong>class-ef-class</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add new entry</strong> next to Loss priority.</td>
</tr>
<tr>
<td></td>
<td>4. From the Loss val list, select <strong>high</strong>.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Add new entry</strong> next to Code points.</td>
</tr>
<tr>
<td></td>
<td>6. In the Value box, type the value of the high-priority code point for expedited forwarding traffic—for example, <strong>101111</strong>.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>OK</strong> three times.</td>
</tr>
</tbody>
</table>

| Configure an assured forwarding class classifier | 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 | 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 Topics**
- Configuring CoS Code Point Aliases (NSM Procedure) on page 102
- Configuring CoS Drop Profile (NSM Procedure) on page 103
- Configuring CoS Forwarding Classes (NSM Procedure) on page 105
- Configuring CoS Interfaces (NSM Procedure) on page 110
- Configuring CoS Rewrite Rules (NSM Procedure) on page 115
- Configuring CoS Schedulers (NSM Procedure) on page 118
- Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 120
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 59 on page 102
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 59: Configuring Code Point Aliases

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
</table>
| Assign an alias to the dscp code point. | 1. In the Configuration tree, expand Code Point Aliases.  
2. Select Dscp.  
3. Click the Add New icon.  
4. In the Name box, type the alias that you want to assign to the code point—for example, my1.  
5. In the Bits box, type the code point—for example, 110001.  
6. Click OK. |

Related Topics
- Configuring CoS Classifiers (NSM Procedure) on page 99
- Configuring CoS Drop Profile (NSM Procedure) on page 103
- Configuring CoS Forwarding Classes (NSM Procedure) on page 105
- Configuring CoS Interfaces (NSM Procedure) on page 110
- Configuring CoS Rewrite Rules (NSM Procedure) on page 115
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 60 on page 103.
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>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drop Profile</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 60: Drop Profile Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the drop profile name.</td>
<td>1. Click the <strong>New</strong> button or <strong>Edit</strong> button in the Drop Profile interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the drop profile name in the Name box.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for the drop profile.</td>
<td>1. Click the <strong>New</strong> button or <strong>Edit</strong> button in the Drop Profile interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the comment for the drop profile in the Comment box.</td>
</tr>
</tbody>
</table>

### Fill Level

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the fill level for the drop profile.</td>
<td>1. On Drop Profile interface click the <strong>New</strong> button or select a profile and click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Expand the Drop Profile tree and select Fill Level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click the <strong>New</strong> button or select a fill level and click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Select a value from Name list.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for the fill level</td>
<td>1. On the Drop Profile interface click the <strong>New</strong> button or select a profile and click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Expand the Drop Profile tree and select Fill Level .</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click the <strong>New</strong> button or select a fill level and click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Enter a comment in the Comment box.</td>
</tr>
</tbody>
</table>

### Related Topics
- Configuring CoS Classifiers (NSM Procedure) on page 99
- Configuring CoS Code Point Aliases (NSM Procedure) on page 102
- Configuring CoS Forwarding Classes (NSM Procedure) on page 105
- Configuring CoS Interfaces (NSM Procedure) on page 110
- Configuring CoS Rewrite Rules (NSM Procedure) on page 115
- Configuring CoS Schedulers (NSM Procedure) on page 118
- Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 120
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 61 on page 105.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

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

### Table 61: Assigning Forwarding Classes to Output Queues

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign best-effort traffic to queue 0.</td>
<td>1. Select Queue and click Add new entry.</td>
</tr>
<tr>
<td></td>
<td>2. In the Queue num box, type 0.</td>
</tr>
<tr>
<td></td>
<td>3. In the Class name box, type the previously configured name of the best-effort class—for example, be-class.</td>
</tr>
<tr>
<td></td>
<td>4. Click OK.</td>
</tr>
</tbody>
</table>
Table 61: Assigning Forwarding Classes to Output Queues (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
</table>
| Assign expedited forwarding traffic to queue 1. | 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. | 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 Topics
- Configuring CoS Classifiers (NSM Procedure) on page 99
- Configuring CoS Code Point Aliases (NSM Procedure) on page 102
- Configuring CoS Drop Profile (NSM Procedure) on page 103
- Configuring CoS Interfaces (NSM Procedure) on page 110
- Configuring CoS Rewrite Rules (NSM Procedure) on page 115
- Configuring CoS Schedulers (NSM Procedure) on page 118
- Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 120

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 62 on page 107.
6. Click one:
- OK—Saves the changes.
- Cancel—Cancels the modifications.

Table 62: Forwarding Policy Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify the name of forwarding class and override the incoming packet classification. | 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. |

Specify the map for CoS forwarding routes.  
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 Topics**
- Configuring CoS Classifiers (NSM Procedure) on page 99
- 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 63 on page 108.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defines fragmentation properties for individual forwarding classes.</td>
<td>1. Click Add new entry next to Fragmentation Maps.</td>
</tr>
<tr>
<td></td>
<td>2. In the Name box, enter the name of the fragmentation map.</td>
</tr>
<tr>
<td></td>
<td>3. Click Forwarding Class next to fragmentation-maps.</td>
</tr>
<tr>
<td></td>
<td>4. Click Add new entry next to Forwarding Class.</td>
</tr>
<tr>
<td></td>
<td>5. In the Name box, enter the name of the forwarding class.</td>
</tr>
<tr>
<td></td>
<td>6. From the Multilink Class, select the multilink class to be assigned to the forwarding class. Range: 0 through 7</td>
</tr>
<tr>
<td></td>
<td>7. From the Drop Timeout list, select the sequencing timeout interval for each forwarding class of a multiclass MLPPP. Range: 0 through 2000</td>
</tr>
</tbody>
</table>
Table 63: Fragmentation Maps Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Set the fragmentation threshold for an individual forwarding class for only AS PIC link services IQ interfaces (lsq). | 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 Topics
- Configuring CoS Forwarding Policy (NSM Procedure) on page 106
- Configuring CoS Schedulers (NSM Procedure) on page 118
- Configuring CoS Traffic Control Profiles (NSM Procedure)

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 64 on page 109.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 64: Host Outbound Traffic Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forwarding Class</td>
<td>Defines a forwarding class name.</td>
<td>In the Forwarding Class box, enter the name for the forwarding class.</td>
</tr>
</tbody>
</table>
Table 64: Host Outbound Traffic Configuration Details (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dscp Code Point</td>
<td>Sets the value of the DSCP code point in the ToS field of the packet generated by the Routing Engine (host).</td>
<td>From the Dscp Code Point list, select the DSCP code point value.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring CoS Forwarding Classes (NSM Procedure) on page 105
- Configuring CoS Fragmentation Maps (NSM Procedure) on page 108
- Configuring CoS Traffic Control Profiles (NSM Procedure)
- Configuring CoS Interfaces (NSM Procedure) on page 110

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 65 on page 110.
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 65: Interfaces Configuration Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 65: Interfaces Configuration Fields *(continued)*

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the interface name.</td>
<td>1. Expand the <strong>Interfaces</strong> tree and select <strong>Interface</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in <strong>Interface</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the interface name in the <strong>Name</strong> box.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for the interface.</td>
<td>1. Expand the <strong>Interfaces</strong> tree and select <strong>Interface</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in <strong>Interface</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the comment for the interface in the <strong>Comment</strong> box.</td>
</tr>
<tr>
<td>Scheduler Map</td>
<td>Specifies the scheduler configuration mapped to the forwarding class.</td>
<td>1. Expand the <strong>Interfaces</strong> tree and select <strong>Interface</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in <strong>Interface</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Select the scheduler map from the list.</td>
</tr>
<tr>
<td>Scheduler Map Chassis</td>
<td>Specifies the scheduler configuration mapped to the forwarding class for the particular chassis in the chassis queue.</td>
<td>1. Expand the <strong>Interfaces</strong> tree and select <strong>Interface</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in <strong>Interface</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Select the scheduler map chassis from the list.</td>
</tr>
<tr>
<td>Input Traffic Control Profile</td>
<td>Applies an input traffic scheduling and shaping profile to the logical interface.</td>
<td>1. Click the <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in <strong>Interface</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Expand the <strong>Interface</strong> tree and select <strong>Input Traffic Control Profile</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the comment and the <strong>profile name</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click <strong>Ok</strong>.</td>
</tr>
</tbody>
</table>
### Table 65: Interfaces Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input Traffic Control Profile Remaining</td>
<td>Applies an input traffic scheduling and shaping profile for remaining traffic to the logical interface.</td>
<td>1. Click the New button or select an interface and click the Edit button in Interface. &lt;br&gt;2. Expand the Interface tree and select Input Traffic Control Profile Remaining &lt;br&gt;3. Specify a comment and a profile name. &lt;br&gt;4. Click Ok.</td>
</tr>
<tr>
<td>Output Traffic Control Profile</td>
<td>Applies an output traffic scheduling and shaping profile to the logical interface.</td>
<td>1. Click the New button or select an interface and click the Edit button in Interface. &lt;br&gt;2. Expand the Interface tree and select Output Traffic Control Profile. &lt;br&gt;3. Specify a comment and a profile name. &lt;br&gt;4. Click Ok.</td>
</tr>
<tr>
<td>Output Traffic Control Profile Remaining</td>
<td>Applies an output traffic scheduling and shaping profile for remaining traffic to the logical interface.</td>
<td>1. Click the New button or select an interface and click the Edit button in Interface. &lt;br&gt;2. Expand the Interface tree and select Output Traffic Control Profile Remaining. &lt;br&gt;3. Specify a comment and a profile name. &lt;br&gt;4. Click Ok.</td>
</tr>
<tr>
<td>Shaping Rate</td>
<td>Shapes the output of the physical interface, so that the interface transmits less traffic than it is physically capable of carrying.</td>
<td>1. Click the New button or select an interface and click the Edit button in Interface. &lt;br&gt;2. Expand Interface tree and select Shaping Rate. &lt;br&gt;3. Specify the comment and the rate. &lt;br&gt;4. Click Ok.</td>
</tr>
</tbody>
</table>
Table 65: Interfaces Configuration Fields *(continued)*

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit</td>
<td>Sets the units that need to be allocated to the specific forwarding class and scheduling map.</td>
<td>1. Click the <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in Interface. &lt;br&gt;2. Expand <strong>Interface</strong> tree and select <strong>Unit</strong>. &lt;br&gt;3. Specify the Unit, Classifiers, Output Traffic Control Profile and Shaping Rate. &lt;br&gt;4. Click <strong>Ok</strong>.</td>
</tr>
<tr>
<td>Interface Set</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the interface set name.</td>
<td>1. Expand the <strong>Interfaces</strong> tree and select <strong>Interface Set</strong>. &lt;br&gt;2. Click the <strong>New</strong> button or select an interface set and click the <strong>Edit</strong> button. &lt;br&gt;3. Select the name from the list.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for the interface.</td>
<td>1. Expand the <strong>Interfaces</strong> tree and select <strong>Interface Set</strong>. &lt;br&gt;2. Click the <strong>New</strong> button or select an interface set and click the <strong>Edit</strong> button. &lt;br&gt;3. Enter the comment.</td>
</tr>
<tr>
<td>Internal Node</td>
<td>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.</td>
<td>1. Expand the <strong>Interfaces</strong> tree and select <strong>Interface Set</strong>. &lt;br&gt;2. Click the <strong>New</strong> button or select an interface set and click the <strong>Edit</strong> button. &lt;br&gt;3. Set the internal node.</td>
</tr>
<tr>
<td>Excess Bandwidth Share</td>
<td>Sets the excess bandwidth sharing value.</td>
<td>1. Expand the <strong>Interfaces</strong> tree and select <strong>Interface Set</strong>. &lt;br&gt;2. Click the <strong>New</strong> button or select an interface set and click the <strong>Edit</strong> button. &lt;br&gt;3. Expand interface—set tree and select <strong>Excess Bandwidth Share</strong>. &lt;br&gt;4. Specify the comment and proportion. &lt;br&gt;5. Click <strong>Ok</strong>.</td>
</tr>
</tbody>
</table>
### Table 65: Interfaces Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Input Excess Bandwidth Share   | Sets the excess input bandwidth sharing value.                           | 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. | 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**.                                                                 |
| Input Traffic Control Profile Remaining | Applies an input traffic scheduling and shaping profile for remaining traffic to the logical interface. | 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. | 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**.                                                                 |
### Table 65: Interfaces Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output Traffic Control Profile Remaining</td>
<td>Applies an output traffic scheduling and shaping profile for remaining traffic to the logical interface.</td>
<td>1. Expand the <strong>Interfaces</strong> tree and select <strong>Interface Set</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the <strong>New</strong> button or select an interface set and click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Expand interface—set tree and select <strong>Output Traffic Control Profile Remaining</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Specify the comment and profile name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Click <strong>Ok</strong>.</td>
</tr>
</tbody>
</table>

#### Related Topics
- Configuring CoS Classifiers (NSM Procedure) on page 99
- Configuring CoS Code Point Aliases (NSM Procedure) on page 102
- Configuring CoS Drop Profile (NSM Procedure) on page 103
- Configuring CoS Forwarding Classes (NSM Procedure) on page 105
- Configuring CoS Rewrite Rules (NSM Procedure) on page 115
- Configuring CoS Schedulers (NSM Procedure) on page 118
- Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 120

## 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 66 on page 116.

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 66: Configuring and Applying Rewrite Rules

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure rewrite rules for DiffServ CoS.</td>
<td>1. Click <strong>Configure</strong> next to Rewrite Rules.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Dscp.</td>
</tr>
<tr>
<td></td>
<td>3. In the Name box, type the name of the rewrite rules—for example, <strong>rewrite-dscps</strong>.</td>
</tr>
<tr>
<td>Configure best-effort forwarding class rewrite rules.</td>
<td>1. Click <strong>Add new entry</strong> next to Forwarding class.</td>
</tr>
<tr>
<td></td>
<td>2. In the Queue num box, type <strong>1</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. In the Class name box, type the name of the previously configured best-effort forwarding class—for example, <strong>be-class</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Add new entry</strong> next to Loss priority.</td>
</tr>
<tr>
<td></td>
<td>5. From the Loss val list, select <strong>low</strong>.</td>
</tr>
<tr>
<td></td>
<td>6. In the Code point box, type the value of the low-priority code point for best-effort traffic—for example, <strong>000000</strong>.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td>8. Click <strong>Add new entry</strong> next to Loss priority.</td>
</tr>
<tr>
<td></td>
<td>9. From the Loss val list, select <strong>high</strong>.</td>
</tr>
<tr>
<td></td>
<td>10. In the Code point box, type the value of the high-priority code point for best-effort traffic—for example, <strong>000001</strong>.</td>
</tr>
<tr>
<td></td>
<td>11. Click <strong>OK</strong> twice.</td>
</tr>
</tbody>
</table>
Table 66: Configuring and Applying Rewrite Rules (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
</table>
| Configure expedited forwarding class rewrite rules. | 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. |
| Configure assured forwarding class rewrite rules. | 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. |
Table 66: Configuring and Applying Rewrite Rules (continued)

Apply rewrite rules to an interface.

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 Topics**

- Configuring CoS Classifiers (NSM Procedure) on page 99
- Configuring CoS Code Point Aliases (NSM Procedure) on page 102
- Configuring CoS Drop Profile (NSM Procedure) on page 103
- Configuring CoS Forwarding Classes (NSM Procedure) on page 105
- Configuring CoS Interfaces (NSM Procedure) on page 110
- Configuring CoS Schedulers (NSM Procedure) on page 118
- Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 120

---

**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 67 on page 119.
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 67: Configuring Schedulers

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the buffer size.</td>
<td>1. Click the <strong>Add New</strong> icon.</td>
</tr>
<tr>
<td></td>
<td>2. Expand <strong>Buffer Size</strong></td>
</tr>
<tr>
<td></td>
<td>3. Select <strong>Percent</strong></td>
</tr>
<tr>
<td></td>
<td>4. Under Percent, select the appropriate option:</td>
</tr>
<tr>
<td></td>
<td>■ To specify no buffer size, select <strong>None</strong>.</td>
</tr>
<tr>
<td></td>
<td>■ To specify buffer size as a percentage of the total buffer, select <strong>percent</strong> and type an integer from 1 through 100.</td>
</tr>
<tr>
<td></td>
<td>■ To specify buffer size as the remaining available buffer, select <strong>remainder</strong>.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>OK</strong></td>
</tr>
</tbody>
</table>

Configure drop profile map. 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. 1. Click the **Add New** icon. 2. Expand **Transmit Rate**. 3. Select **Rate**. 4. Under Rate, select the appropriate option:  ■ 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 Topics**  ■ Configuring CoS Classifiers (NSM Procedure) on page 99  ■ Configuring CoS Code Point Aliases (NSM Procedure) on page 102  ■ Configuring CoS Drop Profile (NSM Procedure) on page 103
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 68 on page 120.
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>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
</table>
| Configure a scheduler map for DiffServ CoS. | 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. | 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**. |
Table 68: Assigning Forwarding Classes to Output Queues (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
</table>
| Configure an expedited forwarding class and scheduler. | 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. | 1. Select **Forwarding Class** and click **Add new entry**.  
2. In the Name box, type the name of the previously configured assured forwarding class—for example, **af-class**.  
3. Select the previously configured assured forwarding scheduler—for example, **af-scheduler**.  
4. Click **OK**. |
| Apply the scheduler map to an interface. | 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 Topics**
- Configuring CoS Classifiers (NSM Procedure) on page 99
- Configuring CoS Code Point Aliases (NSM Procedure) on page 102
- Configuring CoS Drop Profile (NSM Procedure) on page 103
- Configuring CoS Forwarding Classes (NSM Procedure) on page 105
- Configuring CoS Interfaces (NSM Procedure) on page 110
- Configuring CoS Rewrite Rules (NSM Procedure) on page 115
- Configuring CoS Schedulers (NSM Procedure) on page 118
Chapter 12
Configuring Unified Threat Management Features in J Series Services Routers and SRX Series Services Gateways

- Configuring Server-Based Antispam (NSM Procedure) on page 123
- Configuring Local List Antispam (NSM Procedure) on page 124
- Configuring Antivirus Protection (NSM Procedure) on page 127
- Configuring Content Filtering (NSM Procedure) on page 132
- Configuring Web Filtering (NSM Procedure) on page 135

**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 69 on page 124.
7. Click one:
   - **New**—Adds a new profile.
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.
### Table 69: Server-Based Antispam Profile Settings

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

**Related Topics**
- Configuring Local List Antispam (NSM Procedure) on page 124
- Configuring Antivirus Protection (NSM Procedure) on page 127
- Configuring Content Filtering (NSM Procedure) on page 132

### Configuring Local List Antispam (NSM Procedure)

This section includes the following topics:
- Configuring Whitelist and Blacklist Entries on page 124
- Configuring a Custom URL Category List Custom Object on page 125
- Configuring Server-Based Antispam on page 125
- Configuring a UTM Policy for SNMP on page 126

### 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.


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 70 on page 126.
7. Click one:
   - **New**—Adds a new profile.
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.

### Table 70: Server-Based Antispam Profile Settings

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

### 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 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 Topics**
- Configuring Antivirus Protection (NSM Procedure) on page 127
- Configuring Content Filtering (NSM Procedure) on page 132
- Configuring Web Filtering (NSM Procedure) on page 135
Configuring Antivirus Protection (NSM Procedure)

This section includes the following topics:

- Configuring a MIME Pattern List Custom Object on page 127
- Configuring a Filename Extension List Custom Object on page 127
- Configuring a URL Pattern List Custom Object on page 128
- Configuring a Custom URL Category List Custom Object on page 128
- Configuring an Antivirus Feature Profile on page 129
- Configuring a UTM Policy for Express Antivirus on page 131

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 71 on page 129.
5. Click one:
   - New—Adds a new profile.
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 71: Antivirus Feature Profile Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern Update</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Url</td>
<td>Specifies the URL for the pattern database.</td>
<td>If the URL is not already entered, enter the URL for the pattern database. Note that the URL is <a href="http://update.juniper-updates.net/AV/SRX210">http://update.juniper-updates.net/AV/SRX210</a> and you should not change it.</td>
</tr>
<tr>
<td>Interval</td>
<td>Specifies the time interval for automatically updating the pattern database.</td>
<td>Enter the time interval for automatically updating the pattern database. The default interval is 60 minutes.</td>
</tr>
<tr>
<td>No Autoupdate</td>
<td>Specifies whether automatic updates are disabled.</td>
<td>Select this option if you want to disable automatic updates and update the pattern database manually.</td>
</tr>
<tr>
<td>Pattern Update &gt; Email Notify</td>
<td>Specifies the e-mail addresses of the administrators.</td>
<td>Enter the e-mail addresses of the administrators who should receive e-mail notifications when updates are made to the pattern file.</td>
</tr>
</tbody>
</table>
### Table 71: Antivirus Feature Profile Settings (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Message</td>
<td>Specifies the text that will appear in the custom message.</td>
<td>Enter the text to appear in the body of the notification e-mail.</td>
</tr>
<tr>
<td>Custom Message Subject</td>
<td>Specifies the custom message subject.</td>
<td>Enter the text to appear in the subject line of the notification e-mail.</td>
</tr>
<tr>
<td><strong>Profile</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the name of the Kaspersky lab engine profile.</td>
<td>Enter a unique name for the Kaspersky lab engine profile.</td>
</tr>
<tr>
<td><strong>Profile &gt; Fallback Options</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Feature</td>
<td>Enables fallback options.</td>
<td>Select this option to enable fallback options.</td>
</tr>
<tr>
<td>The available fallback options are as follows:</td>
<td>Specifies the fallback options.</td>
<td>Select log-and-permit or block from the list.</td>
</tr>
<tr>
<td>■ Default</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Corrupt File</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Password File</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Decompress Layer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Content Size</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Engine Not Ready</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Timeout</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Out of Resources</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Too Many Requests</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Profile &gt; Notification Options</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Feature</td>
<td>Enables notification options.</td>
<td>Select this option to enable notification options.</td>
</tr>
<tr>
<td>The notification options that can be configured are the following:</td>
<td>Specifies the notification actions for fallback block, fallback nonblock, and virus detection.</td>
<td>■ Custom Message—Enter the text to appear in the body of the notification e-mail.</td>
</tr>
<tr>
<td>■ Fallback Block</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Fallback Non Block</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Virus Detection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Custom Message Subject—Enter the text to appear in the subject line of the notification e-mail.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ notify-mail-sender—Select this option to notify the sender of the mail.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Type—Select <strong>protocol-only</strong> or <strong>message</strong> from the Type list.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Profile &gt; Scan Options</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Feature</td>
<td>Enables scan options.</td>
<td>Select this option to enable scan options.</td>
</tr>
<tr>
<td>intelligent-prescreening</td>
<td>Enables intelligent prescreening.</td>
<td>Select this option to enable intelligent prescreening.</td>
</tr>
</tbody>
</table>

---

130  Configuring an Antivirus Feature Profile
### Table 71: Antivirus Feature Profile Settings (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Size Limit</td>
<td>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.</td>
<td>Enter content size parameters.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Specifies the scanning timeout parameters.</td>
<td>Enter the scanning timeout parameters.</td>
</tr>
<tr>
<td><strong>Profile &gt; Trickling</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Feature</td>
<td>Enables trickling feature.</td>
<td>Select this option to enable trickling feature.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Specifies the trickling timeout parameters.</td>
<td>Enter the trickling timeout parameters.</td>
</tr>
<tr>
<td><strong>Antivirus &gt; Mime Whitelist</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Feature</td>
<td>Enables this feature.</td>
<td>Select this option to enable this feature.</td>
</tr>
<tr>
<td>List</td>
<td>Specifies the name of the URL whitelist.</td>
<td>Enter the name of the URL whitelist custom object you created.</td>
</tr>
</tbody>
</table>

### 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 Smtp 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 Topics
- Configuring Local List Antispam (NSM Procedure) on page 124
- Configuring Content Filtering (NSM Procedure) on page 132
- Configuring Web Filtering (NSM Procedure) on page 135

Configuring Content Filtering (NSM Procedure)

This section includes the following topics:
- Configuring a Protocol Command Custom Object on page 132
- Configuring a Filename Extension List Custom Object on page 132
- Configuring a MIME Pattern List Custom Object on page 133
- Configuring a Content–Filtering Feature Profile on page 133
- Configuring a UTM Policy for Content-Filtering on page 135

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.
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 Filtering** > **Profile**.
4. Add or modify content-filtering profile settings as specified in Table 72 on page 133.
5. Click one:
   - **New**—Adds a new profile.
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

**Table 72: Content-Filtering Feature Profile Settings**

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of the content-filtering profile.</td>
<td>Enter a unique name for this profile.</td>
</tr>
</tbody>
</table>
### Table 72: Content-Filtering Feature Profile Settings (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit Command</td>
<td>The permit protocol command list is intended to act as an exception list for the block protocol command list.</td>
<td>Enter the protocol command custom object you created for permitting commands from the list.</td>
</tr>
<tr>
<td>Block Command</td>
<td>Specifies the block command.</td>
<td>Enter the protocol command custom object you created for blocking commands from the list.</td>
</tr>
<tr>
<td>Block Extension</td>
<td>Specifies the extensions that are blocked.</td>
<td>Enter the file extension list custom object you created for blocking extensions from the list.</td>
</tr>
</tbody>
</table>

#### Profile > Block Content Type

The content types that can be blocked are the following:
- 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.
- **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 Smtp 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 Topics**
- Configuring Local List Antispam (NSM Procedure) on page 124
- Configuring Antivirus Protection (NSM Procedure) on page 127
- Configuring Web Filtering (NSM Procedure) on page 135

**Configuring Web Filtering (NSM Procedure)**

This section includes the following topics:
- Configuring a URL Pattern List Custom Object on page 135
- Configuring a Custom URL Category List Custom Object on page 136
- Configuring a Web Filtering Feature Profile on page 136
- Configuring a UTM Policy for Web Filtering on page 138

**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.


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 73 on page 137.
5. Click one:
- **New**—Adds a new profile.
- **OK**—Saves the changes.
- **Cancel**—Cancels the modifications.

**Table 73: Web Filtering Feature Profile Settings**

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Url Whitelist</strong></td>
<td>Specifies the URL whitelist.</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Url Blacklist</strong></td>
<td>Specifies the URL blacklist.</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Specifies the type of Web filtering.</td>
<td>Select <code>surf-control-integrated</code> from the list.</td>
</tr>
<tr>
<td><strong>Surf Control Integrated &gt; Cache</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Feature</td>
<td>Enables cache options.</td>
<td>Select this option to enable cache options.</td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
<td>Specifies the timeout limit for cache entries.</td>
<td>Enter a timeout limit in minutes for expiring cache entries. (The default is 24 hours and the maximum allowed life span.)</td>
</tr>
<tr>
<td><strong>Size</strong></td>
<td>Specifies the size limit for the cache.</td>
<td>Enter a size limit for the cache in kilobytes. (The default is 500 KB.)</td>
</tr>
<tr>
<td><strong>Surf Control Integrated &gt; Server</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Feature</td>
<td>Enables server options.</td>
<td>Select this option to enable server options.</td>
</tr>
<tr>
<td><strong>Host</strong></td>
<td>Specifies the Surf Control server address.</td>
<td>Enter the Surf Control server name or IP address.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Specifies the port number for communicating with the Surf Control server.</td>
<td>Enter the port number for communicating with the Surf Control server. (Default ports are 80, 8080, and 8081.)</td>
</tr>
<tr>
<td><strong>Surf Control Integrated &gt; Profile</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Specifies a name for the Web-filtering profile.</td>
<td>Enter a unique name for this profile.</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>Specifies the default action for this profile for requests that experience errors.</td>
<td>Select <code>log-and-permit</code>, <code>permit</code>, or <code>block</code> from the list.</td>
</tr>
<tr>
<td><strong>Custom Block Message</strong></td>
<td>Specifies the custom message.</td>
<td>Enter a custom message to be sent when HTTP requests are blocked.</td>
</tr>
</tbody>
</table>
### Table 73: Web Filtering Feature Profile Settings (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout</td>
<td>Specifies the timeout limit.</td>
<td>Enter a value in seconds. Once this limit is reached, fail mode settings are applied. The default setting is 10 seconds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Surf Control Integrated &gt; Profile &gt; Fallback Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Feature</td>
</tr>
</tbody>
</table>

| The available fallback options are as follows:       |
| Default                                               |
| Server Connectivity                                   |
| Timeout                                               |
| Too Many Requests                                     |

<table>
<thead>
<tr>
<th>Surf Control Integrated &gt; Profile &gt; Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Action</td>
</tr>
</tbody>
</table>

---

**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 Topics**  ■ Configuring Local List Antispam (NSM Procedure) on page 124
Chapter 12: Configuring Unified Threat Management Features in J Series Services Routers and SRX Series Services Gateways

- Configuring Content Filtering (NSM Procedure) on page 132
- Configuring Antivirus Protection (NSM Procedure) on page 127
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 143
- Topology Manager on page 147
- IDP Management in J Series Services Routers and SRX Series Services Gateways on page 151
Chapter 13
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 143
- Viewing and Reconciling Device Inventory Overview on page 143
- Viewing Device Inventory in NSM (NSM Procedure) on page 144
- Removing a J Series or SRX Series Device from NSM Management (NSM Procedure) on page 145

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 Topics
- Viewing Device Inventory in NSM (NSM Procedure) on page 144
- Viewing and Reconciling Device Inventory Overview on page 143

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 Topics**

- Viewing Device Inventory in NSM (NSM Procedure) on page 144

---

**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.
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 Topics

- Viewing and Reconciling Device Inventory Overview on page 143
- Adding J Series Services Routers or SRX Series Services Gateways in NSM Overview on page 8
Chapter 14

Topology Manager

- Overview of the NSM Topology Manager on page 147
- Requisites for a Topology Discovery Overview on page 147
- Understanding the NSM Topology Manager Toolbar on page 148

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 Topics
- Requisites for a Topology Discovery Overview on page 147
- Understanding the NSM Topology Manager Toolbar on page 148

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 Topics**

- Overview of the NSM Topology Manager on page 147
- Understanding the NSM Topology Manager Toolbar on page 148

### 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 Topics**

- Overview of the NSM Topology Manager on page 147
Requisites for a Topology Discovery Overview on page 147
Chapter 15
IDP Management in J Series Services Routers and SRX Series Services Gateways

- Updating the NSM Attack Database (NSM Procedure) on page 151
- Loading the IDP Detector Engine on a J Series or SRX Series Device (NSM Procedure) on page 152
- Updating the Deep Inspection Attack Database on a J Series or SRX Series Device (NSM Procedure) on page 152

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.
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 Topics
- Updating the NSM Attack Database (NSM Procedure) on page 151
- Updating the Deep Inspection Attack Database on a J Series or SRX Series Device (NSM Procedure) on page 152

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 Topics**
- Updating the NSM Attack Database (NSM Procedure) on page 151
- Loading the IDP Detector Engine on a J Series or SRX Series Device (NSM Procedure) on page 152
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 157
Chapter 16
Real Time Monitoring of J Series Services Routers and SRX Series Services Gateways

- Realtime Monitor Overview on page 157
- Viewing Device Status on page 158
- Viewing Device Monitor Alarm Status (NSM Procedure) on page 161
- Configuring the Polling Interval for Device Alarm Status (NSM Procedure) on page 162

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 Topics
- Realtime Monitor Overview on page 157
- Viewing Device Status on page 158
Table 74 on page 158 lists and describes device information that you can view through the Device Monitor.

### Table 74: Device Status Information

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name assigned to the device in NSM.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain in NSM in which the device is managed.</td>
</tr>
<tr>
<td>Platform</td>
<td>Model number of the device.</td>
</tr>
<tr>
<td>OS Version</td>
<td>Operating system firmware version running on the device.</td>
</tr>
</tbody>
</table>
Table 74: Device Status Information (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Status</td>
<td>Current configuration status of the device in NSM:</td>
</tr>
<tr>
<td>■ None</td>
<td>No state has been set (does not show in Device Monitor).</td>
</tr>
<tr>
<td>■ Modeled</td>
<td>The device exists in NSM, but a connection to the device has not yet been established.</td>
</tr>
<tr>
<td>■ RMA</td>
<td>Equivalent to bringing the device into the Modeled state. RMA results from an administrator selection in the UI when a device goes down.</td>
</tr>
<tr>
<td>■ Waiting for 1st connect</td>
<td>NSM is waiting for the device to connect.</td>
</tr>
<tr>
<td>■ Import Needed</td>
<td>You must import the configuration of the device into NSM.</td>
</tr>
<tr>
<td>■ OS Version Adjustment Needed</td>
<td>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.</td>
</tr>
<tr>
<td>■ Platform Mismatch</td>
<td>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.</td>
</tr>
<tr>
<td>■ Device Firmware Mismatch</td>
<td>The OS version selected when adding a DMI device does not match the OS version running on the device itself.</td>
</tr>
<tr>
<td>■ Device Type Mismatch</td>
<td>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.</td>
</tr>
<tr>
<td>■ Detected duplicate serial number</td>
<td>The device has the same sequence number as another managed device. A device in this state cannot connect to NSM.</td>
</tr>
<tr>
<td>■ Update Needed</td>
<td>An update to this device is required.</td>
</tr>
<tr>
<td>■ Managed</td>
<td>The device is currently being managed by NSM.</td>
</tr>
<tr>
<td>■ Managed, In Sync</td>
<td>The physical device configuration is synced with the modeled configuration in NSM.</td>
</tr>
</tbody>
</table>
Table 74: Device Status Information (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Status (continued)</td>
<td>■ 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).&lt;br&gt;■ 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).&lt;br&gt;■ 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.&lt;br&gt;■ 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.</td>
</tr>
<tr>
<td>Connection Status</td>
<td>Connection status of the device in NSM:&lt;br&gt;■ Up—Device is currently connected to NSM.&lt;br&gt;■ Down—Device is not currently connected to NSM but has connected in the past.&lt;br&gt;■ Never Connected—Device has never connected to NSM.&lt;br&gt;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 devDaemon.deviceHeartbeatTimeout parameter in the Device Server configuration file. Refer to the Network and Security Manager Installation Guide for more information on editing configuration files. <strong>NOTE:</strong> 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.</td>
</tr>
<tr>
<td>Alarm</td>
<td>Displays the current alarm status for each device in NSM:&lt;br&gt;■ If device has any alarms, the most severe alarm severity is displayed (either Major or Minor).&lt;br&gt;■ None—The device has no alarms.&lt;br&gt;■ Unknown—The device status is unknown. For example, the device might not be connected.&lt;br&gt;■ N/A—The device’s alarm is not pollable or discoverable, for example, this column shows “N/A” for ScreenOS and IDP devices.&lt;br&gt;Alarm is colored:&lt;br&gt;■ Red for Major.&lt;br&gt;■ Orange for Minor.&lt;br&gt;■ Green for Ignore, None, Unknown, or N/A.</td>
</tr>
</tbody>
</table>
### Table 74: Device Status Information (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>H/W Inventory Status</strong></td>
<td>Displays the inventory status for hardware on the device:</td>
</tr>
<tr>
<td>■ In Sync</td>
<td>The inventory information in the NSM database is synchronized with the information on the device.</td>
</tr>
<tr>
<td>■ Out Of Sync</td>
<td>The inventory information in the NSM database is not synchronized with the information on the device.</td>
</tr>
<tr>
<td>■ N/A</td>
<td>The connected device is a ScreenOS or IDP device, or the device is not connected and imported.</td>
</tr>
<tr>
<td><strong>S/W Inventory Status</strong></td>
<td>Displays the inventory status for software on the device:</td>
</tr>
<tr>
<td>■ In Sync</td>
<td>The inventory information in the NSM database is synchronized with the software on the device.</td>
</tr>
<tr>
<td>■ Out Of Sync</td>
<td>The inventory information in the NSM database is not synchronized with the software on the device.</td>
</tr>
<tr>
<td>■ N/A</td>
<td>The connected device is a ScreenOS or IDP device, or the device is not connected and imported.</td>
</tr>
<tr>
<td><strong>License Inventory Status</strong></td>
<td>Displays the inventory status for software on the device:</td>
</tr>
<tr>
<td>■ In Sync</td>
<td>The inventory information in the NSM database is synchronized with the licenses on the device.</td>
</tr>
<tr>
<td>■ Out Of Sync</td>
<td>The inventory information in the NSM database is not synchronized with the licenses on the device.</td>
</tr>
<tr>
<td>■ N/A</td>
<td>The connected device is a ScreenOS or IDP device, or the device is not connected and imported.</td>
</tr>
<tr>
<td><strong>First Connect</strong></td>
<td>The first time the security device connected to the NSM Device Server.</td>
</tr>
<tr>
<td><strong>Latest Connect</strong></td>
<td>The last time the security device connected to the NSM Device Server.</td>
</tr>
<tr>
<td><strong>Latest Disconnect</strong></td>
<td>The last time the security device disconnected from the NSM Device Server.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Viewing Device Monitor Alarm Status (NSM Procedure) on page 161
- Configuring the Polling Interval for Device Alarm Status (NSM Procedure) on page 162

### 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 Topics**
- Viewing Device Status on page 158
- Configuring the Polling Interval for Device Alarm Status (NSM Procedure) on page 162

### 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 Topics**
- Viewing Device Status on page 158
- Viewing Device Monitor Alarm Status (NSM Procedure) on page 161
Part 5
Index

- Index on page 165
Index

Symbols
802.1x authentication .................................................. 72

B
BGP
configuring .................................................................. 69

C
classifiers
CoS ............................................................................... 99
code point aliases ....................................................... 102
CoS classifiers .............................................................. 99
CoS code point aliases ................................................ 102
CoS drop profiles ....................................................... 103
CoS forwarding classes ............................................... 105
CoS interfaces ............................................................ 110
CoS rewrite rules ......................................................... 115
CoS scheduler maps ................................................... 120
CoS schedulers ........................................................... 118
customer support ....................................................... xvi
contacting JTAC .......................................................... xvi

drop profiles .............................................................. 103

F
defate sharing
configuring ................................................................ 63

forwarding classes .................................................... 105
forwarding table
configuring ................................................................ 59

G
generated routes
configuring ................................................................ 57
graceful restart
configuring ................................................................ 58

gvrp ............................................................................. 74

I
IGMP
configuring ................................................................ 75
instance export
configuring ................................................................ 67
instance import
configuring ................................................................ 67
interface routes
configuring ................................................................ 66

M
martian addresses
configuring ................................................................ 64
maximum prefixes
configuring ................................................................ 43
MSTP .......................................................................... 77
multicast
configuring ................................................................ 45
multipath
configuring ................................................................ 48

O
Options
configuring ................................................................ 49
OSPF .......................................................................... 79

P
protocols
802.1x ...................................................................... 72
BGP .......................................................................... 69
GVRP ......................................................................... 74
IGMP ......................................................................... 75
OSPF ......................................................................... 79
RIP ............................................................................ 82
VRRP ......................................................................... 86
VSTP ......................................................................... 84
Protocols
MSTP ......................................................................... 77
R
resolution
  configuring ................................................. 50
rewrite rules .................................................... 115
rib
  configuring ................................................... 53
rib groups
  configuring ................................................... 51
RIP ............................................................. 82
routing options
  fate sharing .................................................... 63
  flow ................................................................ 61
  forwarding table .............................................. 59
  generated routes .............................................. 57
  graceful restart .............................................. 58
  instance export ............................................... 67
  instance import ............................................... 67
  interface routes .............................................. 66
  martian addresses ........................................... 64
  maximum prefixes ............................................ 43
  multicast ....................................................... 45
  multipath ....................................................... 48
  Options ........................................................ 49
  resolution ....................................................... 50
  rib .................................................................. 53
  rib groups ....................................................... 51
  source routing ................................................ 55
Static Routes ..................................................... 56

S
scheduler maps ................................................... 120
schedulers .......................................................... 118
source routing
  configuring ...................................................... 55
Static Routes
  configuring ...................................................... 56
support, technical See technical support

T
technical support
  contacting JTAC .............................................. xvi

V
VRRP ............................................................... 86
VSTP ............................................................... 84