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

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

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

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

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

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

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

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

Network and Security Manager M-series and MX-series Devices
Copyright © 2010, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Writing: Merisha Wazna and Remya Naroth
Editing: Joanne McClintock
Cover Design: Edmonds Design

Revision History
May 2010—Revision 1

The information in this document is current as of the date listed in the revision history.
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 7405(b)(2), FAR 52.227-19, or FAR 52.227-14 (ALT III) 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](http://www.gnu.org/licenses/gpl.html), and a copy of the LGPL at [http://www.gnu.org/licenses/lgpl.html](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 présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s’y rattaché, soient redigés 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 ................................................ xxvii

Objectives .......................................................... xxvii

Audience ............................................................ xxvii

Documentation Conventions ...................................... xxvii

Documentation ...................................................... xxix

Requesting Technical Support .................................... xxx

Self-Help Online Tools and Resources ........................... xxxi

Opening a Case with JTAC ........................................ xxxi

## Part 1 Getting Started

### Chapter 1 Getting Started with NSM ......................... 3

Introduction to Network and Security Manager ............... 3

Installing NSM ....................................................... 3

Role-Based Administration ....................................... 4

### Chapter 2 Understanding the JUNOS CLI and NSM ........... 5

NSM and Device Management Overview ....................... 5

Understanding the CLI and NSM ................................ 6

Comparing the CLI To the NSM UI ............................. 7

NSM Services Supported for M-series and MX-series Devices 10

How NSM Works with the CLI and Distributed Data Collection... 11

Device Schemas .................................................... 12

Communication Between a Device and NSM .................. 13

### Chapter 3 Before You Begin Adding M-series and MX-series Devices .............. 15

M-series and MX-series Devices Supported by NSM .......... 15

Considering the Device Status .................................. 16

Configuring a Deployed M-series or MX-series Device for Importing to NSM ........... 16

Configure an IP Address and a User with Full Administrative Privileges for the Device ........................................... 17

Check Network Connectivity ..................................... 17

Check Connectivity to the NSM Server ......................... 17

Configure a Static Route to the NSM Server .................... 18

Establish a Telnet or an SSHv2, and a NETCONF protocol over SSH

Connection to the NSM Server .................................... 19

## Part 2 Integrating M-series and MX-series Devices

### Chapter 4 Adding M-series and MX-series Devices Overview .............. 23

About Device Creation ............................................. 23

Supported Add Device Workflows for M-series and MX-series Devices ............................. 24
### Chapter 5 Updating M-series and MX-series Devices Overview

- **About Updating M-series and MX-series Devices** ........................................... 29
- **How the Update Process Works** ................................................................. 30
- **Job Manager** ................................................................................................ 31
- **Tracking Updated Devices Using Job Manager** ............................................. 32
- **Reviewing Job Information Displayed in Job Manager** ................................... 33
- **Device States Displayed in Job Manager During Update** ............................... 34
- **Understanding Updating Errors Displayed in the Job Manager** .................... 35

### Part 3 Configuring M-series and MX-series Devices

### Chapter 6 Configuring M-series and MX-series Devices Overview

- **About Device Configuration** .......................................................................... 41
- **M-series and MX-series Device Configuration Settings Supported in NSM** ........ 42
- **Configuring Device Features** ......................................................................... 44
- **Example: Configuration of Interfaces for MPLS in the CLI and NSM** .............. 45

### Chapter 7 Configuring Access

- **Configuring Address-Assignment Pools (NSM Procedure)** ......................... 47
- **Configuring Access Address Pools (NSM Procedure)** ................................... 50
- **Configuring Access Group Profile (NSM Procedure)** .................................... 51
- **Configuring the LDAP Options (NSM Procedure)** ....................................... 52
- **Configuring the LDAP Server (NSM Procedure)** ......................................... 53
- **Configuring Access Profiles for L2TP or PPP Parameters (NSM Procedure)** ..... 54
- **Configuring Access Profile (NSM Procedure)** ............................................ 55
  - **Configuring Accounting Parameters for Access Profiles (NSM Procedure)** .... 55
  - **Configuring the Accounting Order (NSM Procedure)** ............................... 56
  - **Configuring the Authentication Order (NSM Procedure)** ............................ 57
  - **Configuring the Authorization Order (NSM Procedure)** .............................. 57
  - **Configuring the L2TP Client (NSM Procedure)** ........................................ 58
  - **Configuring the Client Filter Name (NSM Procedure)** ................................ 59
  - **Configuring the LDAP Options (NSM Procedure)** .................................... 60
  - **Configuring the LDAP Server (NSM Procedure)** ....................................... 61
  - **Configuring the Provisioning Order (NSM Procedure)** ............................... 62
  - **Configuring RADIUS Parameters for AAA Subscriber Management (NSM Procedure)** .......................................................... 63
  - **Configuring the RADIUS Parameters (NSM Procedure)** ........................... 66
  - **Configuring the RADIUS for Subscriber Access Management, L2TP, or PPP (NSM Procedure)** .................................................. 67
  - **Configuring Session Limit (NSM Procedure)** ............................................ 67
  - **Configuring the RADIUS for Subscriber Access Management, L2TP, or PPP (NSM Procedure)** .................................................. 68
  - **Configuring the SecurID Server (NSM Procedure)** .................................... 69
Chapter 8  Configuring Accounting Options ................................................. 71
  Configuring Accounting Options (NSM Procedure) ................................. 71
  Configuring Class Usage Profiles (NSM Procedure) ................................. 71
  Configuring a Log File (NSM Procedure) .............................................. 72
  Configuring the Filter Profile (NSM Procedure) ..................................... 73
  Configuring the Interface Profile (NSM Procedure) .................................. 74
  Configuring the Policy Decision Statistics Profile (NSM Procedure) ............ 75
  Configuring the MIB Profile (NSM Procedure) ...................................... 76
  Configuring the Routing Engine Profile (NSM Procedure) ......................... 77

Chapter 9  Configuring Applications ...................................................... 79
  Configuring the Application and Application Set (NSM Procedure) ............. 79

Chapter 10 Configuring Bridge Domains ............................................... 81
  Configuring Bridge Domains Properties (NSM Procedure) ......................... 81
  Configuring a Bridge Domain (NSM Procedure) ...................................... 81
  Configuring Layer 2 Learning and Forwarding Properties for a Bridge Domain
  (NSM Procedure) ................................................................................. 82
  Configuring Forwarding Options (NSM Procedure) .................................. 84
  Configuring Logical Interfaces (NSM Procedure) .................................... 85
  Configuring Multicast Snooping Options (NSM Procedure) ....................... 86
  Configuring IGMP Snooping (NSM Procedure) ....................................... 89
  Configuring VLAN ID (NSM Procedure) ............................................... 94

Chapter 11 Configuring Chassis ............................................................. 97
  Configuring Aggregated Devices (NSM Procedure) .................................. 97
  Configuring Chassis Alarms (NSM Procedure) ....................................... 98
  Configuring Container Interfaces (NSM Procedure) .................................. 99
  Configuring Chassis FPC (NSM Procedure) .......................................... 100
  Configuring a T640 Router on a Routing Matrix (NSM Procedure) .......... 105
  Configuring Routing Engine Redundancy (NSM Procedure) ..................... 110
  Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors (NSM
  Procedure) ......................................................................................... 111

Chapter 12 Configuring Authentication ............................................... 113
  Configuring RADIUS Authentication (NSM Procedure) ......................... 113
  Configuring TACACS+ Authentication (NSM Procedure) ......................... 114
  Configuring Authentication Order (NSM Procedure) .............................. 115
  Configuring User Access (NSM Procedure) ........................................... 116
    Configuring Login Classes .................................................................. 116
    Configuring User Accounts ............................................................... 117
  Configuring Template Accounts (NSM Procedure) ................................... 117
    Creating a Remote Template Account .................................................. 118
    Creating a Local Template Account .................................................... 119

Chapter 13 Configuring Class of Service Features .................................... 121
  Configuring CoS Classifiers (NSM Procedure) ...................................... 122
  Configuring CoS Code Point Aliases (NSM Procedure) ......................... 124
  Configuring CoS Drop Profile (NSM Procedure) .................................... 125
Chapter 14 Configuring Event Options ......................................... 151

Configuring Destinations for File Archiving (NSM Procedure) ............... 151
Configuring Event Script (NSM Procedure) ..................................... 152
Generating Internal Events (NSM Procedure) .................................... 154
Configuring Event Policy (NSM Procedure) ................................…… 154
Configuring Event Policy Tracing Operations (NSM Procedure) ............. 157

Chapter 15 Configuring Firewall .............................................. 159

Configuring the Firewall Filter for Any Family Type (NSM Procedure) ...... 159
Configuring the Firewall Filter for Bridge Family Type (NSM Procedure) .... 161
Configuring the Firewall Filter for Ccc Family Type (NSM Procedure) ...... 163
Configuring Filters for inet Family Type (NSM Procedure) .................... 165
  Configuring Firewall Filter for inet Family Type (NSM Procedure) ......... 165
  Configuring Prefix-specific Actions (NSM Procedure) ...................... 167
  Configuring Service Filters (NSM Procedure) .................................. 168
  Configuring Simple Filters (NSM Procedure) .................................. 169
Configuring Filters for inet6 Family Type (NSM Procedure) ................... 170
  Configuring Firewall Filter for inet6 Family Type (NSM Procedure) ...... 171
  Configuring Service Filters for inet6 (NSM Procedure) ...................... 173
Configuring the Firewall Filter for MPLS Family Type (NSM Procedure) ... 174
Configuring the Firewall Filter for VPLS Family Type (NSM Procedure) .... 177
Configuring a Policer for a Firewall Filter ....................................... 180

Chapter 16 Configuring Forwarding Options .................................. 183

Configuring Accounting Options (NSM Procedure) ............................ 183
Configuring the Extended DHCP Agent (NSM Procedure) ..................... 185
  Configuring Authentication Support for the DHCP Relay Agent (NSM Procedure) .................................................. 185
Configuring Group (NSM Procedure) ............................................ 186
Overriding the Default Configuration Settings for the Extended DHCP Relay Agent (NSM Procedure) .......................................... 187
Configuring Relay Option 60 Information for Forwarding Client Traffic to Specific DHCP Servers (NSM Procedure) ...................... 189
Configuring Relay Option 82 for a DHCP Server (NSM Procedure) ........... 190
Specifying the Name of a Group of DHCP Server Addresses for Use by the Extended DHCP Relay Agent (NSM Procedure) .................. 191
# Table of Contents

- Configuring Operations for Extended DHCP Relay Agent Processes (NSM Procedure) .................................. 192
- Specifying Address Family for Filters (NSM Procedure) .............................................................. 193
- Configuring Load Balancing Using Hash Key (NSM Procedure) ............................................... 194
- Configuring Helpers (NSM Procedure) ............................................................... 195
- Configuring a Router or Interface to Act as a Bootstrap Protocol Relay Agent ........................................ 196
- Enabling DNS Request Packet Forwarding ............................................................... 199
- Configuring a Port for a DHCP or BOOTP Relay Agent ...................................................... 201
- Configuring Tracing Operations for BOOTP, DNS, and TFTP Packet Forwarding ...................... 202
- Configuring Per-Flow and Per-Prefix Load Balancing (NSM Procedure) .................................... 203
- Configuring Port Mirroring (NSM Procedure) .............................................................. 204

## Chapter 17 Configuring Interfaces ............................................ 207

- Configuring Interfaces on the Routing Platform (NSM Procedure) .............................................. 207
- Configuring Interface Properties (NSM Procedure) .............................................................. 207
- Damping Interface Transitions (NSM Procedure) ........................................................................ 208
- Configuring Receive Bucket Properties on Interfaces (NSM Procedure) ................................... 209
- Configuring Tracing Operations of an Individual Router Interface (NSM Procedure) .................. 210
- Configuring Transmit Leaky Bucket Properties (NSM Procedure) ............................................ 211
- Configuring Logical Interface Properties (NSM Procedure) .................................................... 212
- Configuring Logical Unit Properties (NSM Procedure) .............................................................. 212
- Configuring an IP Demux Underlying Interface (NSM Procedure) ........................................... 213
- Configuring the Logical Demux Source Family Type on the IP Demux Underlying Interface (NSM Procedure) .............................................................. 214
- Configuring Epd Threshold for the Logical Interface (NSM Procedure) ....................................... 214
- Configuring Protocol Family Information for the Logical Interface (NSM Procedure) ............... 215
- Configuring Protocol Family (Ccc) Information for the Logical Interface (NSM Procedure) ...... 215
- Configuring Protocol Family (Inet) Information for the Logical Interface (NSM Procedure) ..... 217
- Configuring Protocol Family (Inet6) Information for the Logical Interface (NSM Procedure) .... 223
- Configuring Protocol Family (ISO) Information for the Logical Interface (NSM Procedure) .. 229
- Configuring Protocol Family (MPLS) Information for the Logical Interface (NSM Procedure) ... 230
- Configuring Protocol Family (TCC) Information for the Logical Interface (NSM Procedure) .... 232
- Configuring the Traffic Shaping Profile (NSM Procedure) .......................................................... 232
- Configuring Interface set on the Routing Platform (NSM Procedure) ....................................... 234
- Configuring Trace Options on the Routing Platform (NSM Procedure) ................................... 235

## Chapter 18 Configuring Multicast Snooping Options .................. 237

- Configuring Multicast Snooping Options (NSM Procedure) ....................................................... 237
<table>
<thead>
<tr>
<th>Chapter 19</th>
<th>Configuring Policy Options ........................................</th>
<th>241</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configuring an AS Path in a BGP Routing Policy (NSM Procedure)</td>
<td>241</td>
</tr>
<tr>
<td></td>
<td>Configuring an AS Path Group in a BGP Routing Policy (NSM Procedure)</td>
<td>242</td>
</tr>
<tr>
<td></td>
<td>Configuring a Community for use in BGP Routing Policy Conditions (NSM Procedure)</td>
<td>243</td>
</tr>
<tr>
<td></td>
<td>Configuring a BGP Export Policy Condition (NSM Procedure)</td>
<td>244</td>
</tr>
<tr>
<td></td>
<td>Configuring Flap Damping to Reduce the Number of BGP Update Messages (NSM Procedure)</td>
<td>245</td>
</tr>
<tr>
<td></td>
<td>Configuring a Routing Policy Statement (NSM Procedure)</td>
<td>247</td>
</tr>
<tr>
<td></td>
<td>Configuring Prefix List (NSM Procedure)</td>
<td>248</td>
</tr>
<tr>
<td>Chapter 20</td>
<td>Configuring Protocols .............................................</td>
<td>251</td>
</tr>
<tr>
<td></td>
<td>Configuring the BFD Protocol (NSM Procedure)</td>
<td>251</td>
</tr>
<tr>
<td></td>
<td>Configuring BGP (NSM Procedure)</td>
<td>252</td>
</tr>
<tr>
<td></td>
<td>Configuring the ILMI Protocol (NSM Procedure)</td>
<td>255</td>
</tr>
<tr>
<td></td>
<td>Configuring Layer 2 Address Learning and Forwarding Properties (NSM Procedure)</td>
<td>256</td>
</tr>
<tr>
<td></td>
<td>Configuring Layer 2 Circuit (NSM Procedure)</td>
<td>257</td>
</tr>
<tr>
<td></td>
<td>Configuring Local Interface Switching (NSM Procedure)</td>
<td>257</td>
</tr>
<tr>
<td></td>
<td>Configuring the Neighbor Interface for the Layer 2 Circuit (NSM Procedure)</td>
<td>258</td>
</tr>
<tr>
<td></td>
<td>Tracing Layer 2 Circuit Creation and Changes (NSM Procedure)</td>
<td>261</td>
</tr>
<tr>
<td></td>
<td>Configuring Layer 2 Protocol Tunneling and BPDU Protection (NSM Procedure)</td>
<td>262</td>
</tr>
<tr>
<td></td>
<td>Configuring Label Distribution Protocol (NSM Procedure)</td>
<td>264</td>
</tr>
<tr>
<td></td>
<td>Configuring Link Management Protocol (NSM Procedure)</td>
<td>275</td>
</tr>
<tr>
<td></td>
<td>Configuring MPLS Protocol (NSM Procedure)</td>
<td>279</td>
</tr>
<tr>
<td></td>
<td>Enabling MPLS on the Router (NSM Procedure)</td>
<td>279</td>
</tr>
<tr>
<td></td>
<td>Configuring Administrative Group (NSM Procedure)</td>
<td>282</td>
</tr>
<tr>
<td></td>
<td>Configuring Administrative Groups (NSM Procedure)</td>
<td>282</td>
</tr>
<tr>
<td></td>
<td>Configuring Bandwidth for the Reroute Path (NSM Procedure)</td>
<td>283</td>
</tr>
<tr>
<td></td>
<td>Configuring DiffServ-Aware Traffic Engineering (NSM Procedure)</td>
<td>284</td>
</tr>
<tr>
<td></td>
<td>Configuring MPLS on Interfaces (NSM Procedure)</td>
<td>285</td>
</tr>
<tr>
<td></td>
<td>Configure a Label Switched Path (LSP) to Use in Dynamic MPLS</td>
<td>287</td>
</tr>
<tr>
<td></td>
<td>Configuring Label Switched Path (NSM Procedure)</td>
<td>287</td>
</tr>
<tr>
<td></td>
<td>Configuring Administrative Group (NSM Procedure)</td>
<td>290</td>
</tr>
<tr>
<td></td>
<td>Configuring Automatic Bandwidth Allocation for LSPs (NSM Procedure)</td>
<td>291</td>
</tr>
<tr>
<td></td>
<td>Configuring Bandwidth for the Reroute Path (NSM Procedure)</td>
<td>292</td>
</tr>
<tr>
<td></td>
<td>Configuring Fast Reroute (NSM Procedure)</td>
<td>293</td>
</tr>
<tr>
<td></td>
<td>Adding LSP-Related Routes to the inet.3 Routing Table (NSM Procedure)</td>
<td>294</td>
</tr>
<tr>
<td></td>
<td>Configuring MPLS LSPs for GMPLS (NSM Procedure)</td>
<td>295</td>
</tr>
<tr>
<td></td>
<td>Configuring BFD for MPLS IPv4 LSPs (NSM Procedure)</td>
<td>296</td>
</tr>
<tr>
<td></td>
<td>Configuring the Primary Point-to-Multipoint LSP (NSM Procedure)</td>
<td>298</td>
</tr>
<tr>
<td></td>
<td>Configuring Policers for LSPs (NSM Procedure)</td>
<td>299</td>
</tr>
<tr>
<td></td>
<td>Configuring Primary Paths for an LSP (NSM Procedure)</td>
<td>300</td>
</tr>
<tr>
<td></td>
<td>Configuring Secondary Paths for an LSP (NSM Procedure)</td>
<td>305</td>
</tr>
</tbody>
</table>
Chapter 21   Configuring Routing Options ........................................ 361

Configuring Confederation (NSM Procedure) .................. 362
Configuring Dynamic Tunnels (NSM Procedure) .......... 363
Configuring Fate Sharing (NSM Procedure) ............... 364
Configuring Flow Route (NSM Procedure) .................. 366
Configuring Forwarding Table (NSM Procedure) ......... 368
Configuring Generated Routes (NSM Procedure) .......... 369
Configuring Instance Export (NSM Procedure) ........... 370
Configuring Instance Import (NSM Procedure) .......... 371
Configuring Interface Routes (NSM Procedure) .......... 372
Configuring Martian Addresses (NSM Procedure) ....... 373

Copyright © 2010, Juniper Networks, Inc.
Chapter 24 Configuring SNMP ............................................... 463
  Configuring Basic System Identification for SNMP (NSM Procedure)  . 463
  Configuring SNMP Communities (NSM Procedure) .................... 464
  Configuring SNMP Trap Groups (NSM Procedure) ..................... 466
  Configuring SNMP Views (NSM Procedure) ........................... 467

Part 4 Managing M-series and MX-series Devices

Chapter 25 Managing M-series and MX-series Devices Overview ............. 471
  Managing M-series and MX-series Device Software Versions ............ 471

Chapter 26 Viewing the M-series and MX-series Device Inventory in NSM and the CLI ................................................................. 473
  Viewing and Reconciling Device Inventory .................................. 473
  Comparing Device Inventory in NSM and the CLI .......................... 474
  Viewing Device Inventory in NSM ........................................... 474
  Viewing Device Inventory from the CLI .................................... 476

Chapter 27 Topology Manager .................................................. 479
  Overview of the NSM Topology Manager .................................. 479
  Requisites for a Topology Discovery ....................................... 479
  About the NSM Topology Manager Toolbar ............................... 480

Part 5 Monitoring M-series and MX-series Devices

Chapter 28 Real Time Monitoring of M-series and MX-series .............. 485
  About the Realtime Monitor .............................................. 485
  Viewing Device Status .................................................... 486
  Viewing Device Monitor Alarm Status .................................... 488
  Setting the Polling Interval For Device Alarm Status ................... 489

Part 6 Index

Index ..................................................................................... 493
# List of Figures

## Part 1 Getting Started

**Chapter 2** Understanding the JUNOS CLI and NSM .............................. 5

- Figure 1: Overview of the User Interface ........................................ 8
- Figure 2: NSM Network Architecture ............................................. 12

## Part 2 Integrating M-series and MX-series Devices

**Chapter 5** Updating M-series and MX-series Devices Overview ................... 29

- Figure 3: Job Information Dialog Box ............................................ 33
- Figure 4: Failed Update Job Information Dialog Box .......................... 36

## Part 3 Configuring M-series and MX-series Devices

**Chapter 6** Configuring M-series and MX-series Devices Overview ................. 41

- Figure 5: MPLS Configuration in the CLI ......................................... 45
- Figure 6: MPLS Configuration in NSM ............................................ 46

## Part 4 Managing M-series and MX-series Devices

**Chapter 26** Viewing the M-series and MX-series Device Inventory in NSM and the CLI .......................................................... 473

- Figure 7: The Device Inventory Window ......................................... 474
- Figure 8: Viewing the Hardware Inventory ....................................... 475
- Figure 9: Viewing the Software Inventory ....................................... 475
About This Guide ................................................ xxvii

Table 1: Notice Icons ............................................. xxviii
Table 2: Text Conventions ....................................... xxviii
Table 3: Syntax Conventions ..................................... xxix
Table 4: Network and Security Manager Publications .......... xxix

Part 1 Getting Started

Chapter 3 Before You Begin Adding M-series and MX-series Devices ..............15
Table 5: M-series Internet Routers and MX-series Internet Service Routers .... 15

Part 2 Integrating M-series and MX-series Devices

Chapter 5 Updating M-series and MX-series Devices Overview ...................29
Table 6: Device States During Update .................................. 35

Part 3 Configuring M-series and MX-series Devices

Chapter 6 Configuring M-series and MX-series Devices Overview .................41
Table 7: The JUNOS Configuration Hierarchy and the NSM Configuration
   Tree ........................................................................ 42

Chapter 7 Configuring Access ................................................47
Table 8: Address Assignment Configuration Details ................................. 48
Table 9: Access Address Pool Configuration Details ............................... 51
Table 10: Access Group Profile Configuration Details .............................. 51
Table 11: LDAP Options Configuration Details ..................................... 53
Table 12: LDAP Server Configuration Details ..................................... 54
Table 13: Access Profile Properties Configuration Details ....................... 55
Table 14: Accounting Parameter Configuration Details ......................... 56
Table 15: Accounting Order Configuration Details ............................... 57
Table 16: Authentication Order Configuration Details .............................. 57
Table 17: Authorization Order Configuration Details ............................... 58
Table 18: Client Configuration Details ......................................... 58
Table 19: Client Filter Name Configuration Details ............................... 60
Table 20: Ldap Options Configuration Details .................................... 60
Table 21: Ldap Server Configuration Details ..................................... 62
Table 22: Provisioning Order Configuration Details .............................. 62
Table 23: RADIUS Parameter Configuration Details ............................. 63
Table 24: RADIUS Parameters Configuration Details ......................... 66
Table 25: RADIUS Server Configuration Details .................................. 67
Table 26: Session Limit Configuration Details ..................................... 68
Table 27: RADIUS Server Configuration Details ........................................ 69
Table 28: SecurID Server Configuration Details ...................................... 70
Table 29: Access Profile Configuration Details ...................................... 70

Chapter 8 Configuring Accounting Options ......................................... 71
Table 30: Class Usage Profile Configuration Details ............................ 72
Table 31: Log File Configuration Details ............................................. 73
Table 32: Filter Profile Configuration Details ....................................... 74
Table 33: Interface Profile Configuration Details .................................. 75
Table 34: Policy Decision Statistics Profile Configuration Details ......... 76
Table 35: MIB Profile Configuration Details ........................................ 77
Table 36: Routing Engine Profile Configuration Details ....................... 78

Chapter 9 Configuring Applications .................................................. 79
Table 37: Applications Configuration Details ....................................... 80

Chapter 10 Configuring Bridge Domains ............................................. 81
Table 38: Bridge Domain Configuration Details .................................... 82
Table 39: Bridge Options Configuration Details .................................. 83
Table 40: Forwarding Options Configuration Details ............................ 84
Table 41: Logical Interface Configuration Details ............................... 86
Table 42: Multicast Snooping Options Configuration Details ............... 87
Table 43: Igmp Snooping Configuration Details .................................... 90
Table 44: VLAN ID Configuration Details ........................................... 95

Chapter 11 Configuring Chassis ....................................................... 97
Table 45: Aggregated Devices Configuration Details ............................ 98
Table 46: Chassis Alarms Configuration Details ................................... 99
Table 47: Container Interfaces Configuration Details ........................... 99
Table 48: FPC Configuration Details .................................................. 100
Table 49: Lcc Configuration Details .................................................. 105
Table 50: Chassis Redundancy Configuration Details ......................... 110
Table 51: Chassis Routing Engine Configuration Details ..................... 112

Chapter 12 Configuring Authentication ............................................. 113
Table 52: RADIUS Authentication Configuration Details ..................... 113
Table 53: TACACS+ Authentication Configuration Details ................... 114
Table 54: Login Class Authentication Configuration Details ............... 116
Table 55: User Authentication Configuration Details ........................... 117
Table 56: Remote Template Account Details ..................................... 118
Table 57: Local Template Account Details ......................................... 119

Chapter 13 Configuring Class of Service Features ............................... 121
Table 58: Configuring and Applying Behavior Aggregate Classifiers .... 122
Table 59: Configuring Code Point Aliases .......................................... 125
Table 60: Drop Profile Configuration Fields ....................................... 126
Table 61: Assigning Forwarding Classes to Output Queues ................ 128
Table 62: Forwarding Policy Configuration Details ............................. 129
Table 63: Fragmentation Maps Configuration Details ......................... 131
Table 64: Host Outbound Traffic Configuration Details ....................... 132
Table 65: Interfaces Configuration Fields ......................................... 133
| Chapter 14 | Configuring Event Options ..................................... | 151 |
| Table 73: Destination Configuration Details ................................ | 151 |
| Table 74: Event Script Configuration Details .................................. | 153 |
| Table 75: Generate Event Details .................................................. | 154 |
| Table 76: Configure Event Policy Details ........................................ | 155 |
| Table 77: Event Options Traceoptions Configuration Details ................ | 158 |
| Chapter 15 | Configuring Firewall .................................................. | 159 |
| Table 78: Firewall Filter Configuration Details .................................. | 160 |
| Table 79: Bridge Filter Configuration Details .................................... | 161 |
| Table 80: Ccc Filter Configuration Details ....................................... | 163 |
| Table 81: Firewall Filter Configuration Details .................................. | 165 |
| Table 82: Prefix Actions Details .................................................... | 168 |
| Table 83: Service Filter Configuration Details ................................. | 168 |
| Table 84: Simple Filter Details ..................................................... | 170 |
| Table 85: Inet6 Firewall Filter Configuration Details .......................... | 171 |
| Table 86: Inet6 Service Filter Configuration Details ............................ | 173 |
| Table 87: MPLS Firewall Filter Configuration Details ........................... | 175 |
| Table 88: VPLS Firewall Filter Configuration Details ............................ | 178 |
| Table 89: Configuring a Policer for a Firewall Filter .......................... | 180 |
| Chapter 16 | Configuring Forwarding Options ...................................... | 183 |
| Table 90: Accounting Options Configuration Details ............................ | 183 |
| Table 91: Authentication Configuration Details ................................... | 186 |
| Table 92: Group Configuration Details ............................................. | 187 |
| Table 93: Overrides Configuration Details ......................................... | 188 |
| Table 94: Relay Option 60 Configuration Details ................................... | 189 |
| Table 95: Relay option 82 Configuration Details ................................... | 191 |
| Table 96: Sever Group Configuration Details ....................................... | 192 |
| Table 97: DHCP Relay Traceoptions Configuration Details ...................... | 192 |
| Table 98: Address Family Details .................................................... | 193 |
| Table 99: Load Balance Configuration Details ..................................... | 195 |
| Table 100: BOOTP Configuration Details ........................................... | 196 |
| Table 101: DNS and TFTP Configuration Details .................................... | 200 |
| Table 102: Port Configuration Details .............................................. | 202 |
| Table 103: Traceoptions Configuration Details ..................................... | 203 |
| Table 104: Load Balancing Configuration Details ................................... | 204 |
| Table 105: Port Mirroring Configuration Details ................................... | 205 |
| Chapter 17 | Configuring Interfaces ................................................... | 207 |
| Table 106: Interface Properties Configuration Details .......................... | 208 |
| Table 107: Hold Time Configuration Details ........................................ | 209 |
Chapter 18 Configuring Multicast Snooping Options ......................... 237
Table 124: Multicast Snooping Options Configuration Details ............... 238

Chapter 19 Configuring Policy Options ................................... 241
Table 125: AS Path Configuration Details .................................. 242
Table 126: AS Path Group Configuration Details ........................... 243
Table 127: Community Configuration Details ............................... 244
Table 128: Condition Configuration Details ................................ 245
Table 129: Damping Configuration Details .................................. 246
Table 130: Configuring Policy Statement Fields ............................. 247
Table 131: Configuring Prefix List Fields ................................. 249

Chapter 20 Configuring Protocols ......................................... 251
Table 132: Configuring Bfd Fields ......................................... 252
Table 133: BGP Configuration Fields ..................................... 253
Table 134: Trace Options Configuration Details ........................... 255
Table 135: L2 Learning Configuration Details .............................. 257
Table 136: Local Switching Configuration Details .......................... 258
Table 137: Neighbor Interface Configuration Details ...................... 259
Table 138: Layer2 Circuit Traceoption Configuration Details ............. 261
Table 139: Layer2 Circuit Configuration Details ............................ 262
Table 140: LDP Configuration Details .................................... 265
Table 141: Link Management Protocol Configuration Details ........... 276
Table 142: MPLS Configuration Details ................................... 280
Table 143: Administrative Group Configuration Details ................. 282
Table 144: Administrative Groups Configuration Details ............... 283
Table 145: Automatic Policers Configuration Details ...................... 284
Table 146: Diffserv-Aware Traffic Engineering Configuration Details .... 285
Table 147: Interface Configuration Details ................................ 286
Table 148: LSP Configuration Details ...................................... 288
Table 149: Administrative Group Configuration Details ................. 291
Table 150: Automatic Bandwidth Configuration Details .................... 292
Table 151: Bandwidth Configuration Details ............................... 293
Table 152: Fast Reroute Configuration Details ............................................. 293
Table 153: Install Configuration Details ..................................................... 295
Table 154: Lsp Attributes Configuration Details ........................................ 296
Table 155: Oam Configuration Details ...................................................... 297
Table 156: P2mp Configuration Details ...................................................... 299
Table 157: Policer Configuration Details ................................................... 299
Table 158: Primary Paths Configuration Details ........................................ 300
Table 159: Administrative Group Configuration Details .............................. 302
Table 160: Bandwidth Configuration Details .............................................. 303
Table 161: Oam Configuration Details ..................................................... 303
Table 162: Secondary Paths Configuration Details ..................................... 306
Table 163: Administrative Group Configuration Details ............................. 308
Table 164: Bandwidth Configuration Details .............................................. 309
Table 165: Oam Configuration Details ..................................................... 309
Table 166: Egress Router Address Configuration Details ............................ 312
Table 167: LSP Traceoptions Configuration Details ..................................... 312
Table 168: Log Updown Configuration Details .......................................... 313
Table 169: Oam Configuration Details ..................................................... 314
Table 170: Named Path Configuration Details .......................................... 317
Table 171: Path MTU Configuration Details .............................................. 317
Table 172: Static Path Configuration Details ............................................ 318
Table 173: MPLS Statistics Configuration Details ....................................... 320
Table 174: Traceoptions Configuration Details .......................................... 321
Table 175: MSDP Configuration Details ................................................... 322
Table 176: Active Source Limit Configuration Details ................................ 323
Table 177: Export Policy Configuration Details ......................................... 323
Table 178: Peer Group Configuration Details ........................................... 324
Table 179: MSDP Peer Configuration Details .......................................... 326
Table 180: Rib Group Configuration Details ............................................. 327
Table 181: Active Source Limit Configuration Details ................................ 328
Table 182: MSDP Traceoption Configuration Details ................................ 329
Table 183: MSTP Configuration Fields .................................................... 330
Table 184: OSPF Configuration Fields ..................................................... 332
Table 185: RIP Configuration Fields ....................................................... 336
Table 186: RIPng Configuration Details .................................................. 338
Table 187: Graceful Restart Configuration Details .................................... 339
Table 188: Group Configuration Details ................................................... 340
Table 189: RIPng Export Policy Configuration Details .............................. 341
Table 190: Import Policy Configuration Details ........................................ 342
Table 191: Neighbor Properties Configuration Details .............................. 343
Table 192: Import Policy Configuration Details ........................................ 343
Table 193: Receive Message Update Configuration Details ........................ 344
Table 194: Send Update Message Configuration Details ............................ 345
Table 195: Receive Message Update Configuration Details ........................ 345
Table 196: RIPng Send Configuration Details .......................................... 346
Table 197: RIPng Traceoption Configuration Details ................................ 347
Table 198: Router Advertisement Configuration Details ............................. 348
Table 199: Router Discovery Configuration Details ................................... 350
Table 200: RSVP Configuration Details ................................................... 352
Table 201: VRRP Configuration Fields ........................................... 358
Table 202: VSTP Configuration Fields ........................................... 360

Chapter 21 Configuring Routing Options ....................................... 361
Table 203: Confederation Fields .................................................. 362
Table 204: Dynamic Tunnels Configuration Details ......................... 363
Table 205: Fate Sharing Fields .................................................... 365
Table 206: Flow Route Fields ...................................................... 367
Table 207: Forwarding Table Fields .............................................. 368
Table 208: Generated Routes Fields .............................................. 370
Table 209: Interface Routes Fields ............................................... 372
Table 210: Configuring Martian Address Fields .............................. 373
Table 211: Configuring Maximum Paths Fields ............................... 375
Table 212: Configuring Maximum Prefixes Fields ........................... 376
Table 213: Configuring Multicast Fields ....................................... 377
Table 214: Configuring Options Fields ......................................... 381
Table 215: Rib Fields ................................................................... 382
Table 216: Rib Group Fields .......................................................... 384
Table 217: Source Routing Fields ................................................. 385
Table 218: Static Fields ................................................................. 386
Table 219: Topology Configuration Details .................................... 387
Table 220: Traceoption Fields ....................................................... 388

Chapter 22 Configuring Security .................................................. 389
Table 221: Security Authentication Key Configuration Details ............. 390

Chapter 23 Configuring Services ............................................... 391
Table 222: Adaptive Services Pics Configuration Details .................. 392
Table 223: Gateway Configuration Details .................................... 393
Table 224: Admission Controller Configuration Details ................... 394
Table 225: Session Policy Decision Configuration Details ................. 395
Table 226: Service Point Configuration Details .............................. 397
Table 227: Message Manipulate Rules Configuration Details .............. 398
Table 228: New Call Usage Policy Configuration Details .................. 400
Table 229: New Call Usage Policy Set Configuration Details .............. 403
Table 230: Transaction Policy Configuration Details ....................... 404
Table 231: Transaction Policy Set Configuration Details ................. 406
Table 232: Timers Configuration Details ....................................... 407
Table 233: Traceoption BSG Configuration Details ........................... 408
Table 234: CoS Configuration Details ............................................ 413
Table 235: IDS Configuration Details ............................................ 416
Table 236: Traceoptions Configuration Details ................................ 420
Table 237: NAT Configuration Details ......................................... 422
Table 238: Virtual BGF Configuration Details ............................... 426
Table 239: Data Inactivity Detection Configuration Details ............... 428
Table 240: Gateway Controller Configuration Details .................... 429
Table 241: Graceful Restart Configuration Details ........................... 430
Table 242: H248 Configuration Details .......................................... 431
Table 243: Encoding Defaults Configuration Details ....................... 431
Table 244: Context indication Configuration Details ....................... 432
Table 245: Control Association Configuration Details . . . . . . . . . . . . . . . . . . . . . 434
Table 246: Virtual Interface Indications Configuration Details . . . . . . . . . . . . . . 436
Table 247: Data Inactivity Detection Configuration Details . . . . . . . . . . . . . . . . . 437
Table 248: Base Root Package Configuration Details . . . . . . . . . . . . . . . . . . . . . 439
Table 249: Diffserv Configuration Details . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 440
Table 250: Event Timestamp Notification Configuration Details . . . . . . . . . . . . . 441
Table 251: Hanging Termination Detection Configuration Details . . . . . . . . . . . . 442
Table 252: Inactivity Timer Configuration Details . . . . . . . . . . . . . . . . . . . . . . . . 443
Table 253: Notification Behavior Configuration Details . . . . . . . . . . . . . . . . . . . . 444
Table 254: Segmentation Package Configuration Details . . . . . . . . . . . . . . . . . . . . 445
Table 255: Traffic Management Configuration Details . . . . . . . . . . . . . . . . . . . . . 446
Table 256: H248 Timers Configuration Details . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 448
Table 257: Monitor Configuration Details . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 449
Table 258: Overload Control Configuration Details . . . . . . . . . . . . . . . . . . . . . . . . 449
Table 259: Session Mirroring Configuration Details . . . . . . . . . . . . . . . . . . . . . . . . 450
Table 260: Media Service Configuration Details . . . . . . . . . . . . . . . . . . . . . . . . . . . . 451
Table 261: Configuring Rule . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 451
Table 262: Configuring Rule Set . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 452
Table 263: Session Mirroring Configuration Details . . . . . . . . . . . . . . . . . . . . . . . . 453
Table 264: Traceoptions Configuration Details . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 454
Table 265: Virtual Interface Configuration Details . . . . . . . . . . . . . . . . . . . . . . . . 455
Table 266: Service Interface Pools Configuration Details . . . . . . . . . . . . . . . . . . . . 456
Table 267: Service Set Configuration Details . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 457
Table 268: Stateful Firewall Configuration Details . . . . . . . . . . . . . . . . . . . . . . . . . . 461

Chapter 24 Configuring SNMP ............................................... 463
Table 269: Basic System Identification Details . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 463
Table 270: Configuring Community Fields . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 463
Table 271: Configuring SNMP Trap Group Fields . . . . . . . . . . . . . . . . . . . . . . . . . . . . 466
Table 272: Configuring SNMP View Fields . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 468

Part 5 Monitoring M-series and MX-series Devices

Chapter 28 Real Time Monitoring of M-series and MX-series ..................... 485
Table 273: Device Status Information . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 486
About This Guide

- Objectives on page xxvii
- Audience on page xxvii
- Documentation Conventions on page xxvii
- Documentation on page xxix
- Requesting Technical Support on page xxx

Objectives

Juniper Networks 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 devices.

M-series and MX-series devices are routers that run JUNOS software using the command-line interface (CLI) for installation and configuration.

This guide provides the information you need to understand, configure, and maintain an M-series or MX-series device using NSM. This guide explains how to use basic NSM functionality, including adding new devices, deploying new device configurations, updating device firmware, and monitoring the status of your M-series or MX-series device. Use this guide in conjunction with the NSM Online Help, which provides step-by-step instructions that complement the information in this guide.

NOTE: If the information in the latest NSM Release Notes differs from the information in this guide, follow the NSM Release Notes.

Auditence

This guide is for the system administrator responsible for configuring the M-series and MX-series devices.

Documentation Conventions

The sample screens used throughout this guide are representations of the screens that appear when you install and configure the NSM software. The actual screens may differ.
All examples show default file paths. If you do not accept the installation defaults, your paths will vary from the examples.

Table 1 on page xxviii defines notice icons used in this guide.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![i]</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>![W]</td>
<td>Warning</td>
<td>Alerts you to the risk of personal injury or death.</td>
</tr>
<tr>
<td>![L]</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 xxviii defines text conventions used in this guide.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold typeface like this</strong></td>
<td>• Represents commands and keywords in text.</td>
<td>• Issue the <code>clock source</code> command.</td>
</tr>
<tr>
<td></td>
<td>• Represents keywords</td>
<td>• Specify the keyword <code>exp-msg</code>.</td>
</tr>
<tr>
<td></td>
<td>• Represents UI elements</td>
<td>• Click User Objects</td>
</tr>
<tr>
<td><strong>Bold typeface like this</strong></td>
<td>Represents text that the user must type.</td>
<td>user input</td>
</tr>
<tr>
<td><strong>fixed-width font</strong></td>
<td>Represents information as displayed on the terminal screen.</td>
<td>host1# show ip ospf</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Routing Process OSPF 2 with Router ID 5.5.0.250</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Router is an area Border Router (ABR)</td>
</tr>
<tr>
<td>Key names linked with a plus (+) sign</td>
<td>Indicates that you must press two or more keys simultaneously.</td>
<td>Ctrl + d</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>• Emphasizes words</td>
<td>• The product supports two levels of access, user and privileged.</td>
</tr>
<tr>
<td></td>
<td>• Identifies variables</td>
<td>• <code>clusterID, ipAddress</code>.</td>
</tr>
<tr>
<td>The angle bracket (&gt; )</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>
</tbody>
</table>
Table 3 on page xxix 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>

**Documentation**

Table 4 on page xxix describes documentation for the NSM.

**Table 4: Network and Security Manager Publications**

<table>
<thead>
<tr>
<th>Book</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Network and Security Manager Installation Guide</em></td>
<td>Describes 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 or upgrade of NSM.</td>
</tr>
<tr>
<td><em>Network and Security Manager Administration Guide</em></td>
<td>Describes how to use and configure key management features in the NSM. It provides conceptual information, suggested workflows, and examples. 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><em>Network and Security Manager Configuring ScreenOS and IDP Devices Guide</em></td>
<td>Provides details about configuring the device features for all supported ScreenOS and IDP platforms.</td>
</tr>
</tbody>
</table>
Table 4: Network and Security Manager Publications (continued)

<table>
<thead>
<tr>
<th>Book</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network and Security Manager Online Help</td>
<td>Provides procedures for 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>Network and Security Manager API Guide</td>
<td>Provides complete syntax and description of the SOAP messaging interface to NSM.</td>
</tr>
<tr>
<td>Network and Security Manager Release Notes</td>
<td>Provides the latest information about features, changes, known problems, resolved problems, and system maximum values. If the information in the Release Notes differs from the information found in the documentation set, follow the Release Notes.</td>
</tr>
<tr>
<td></td>
<td>Release notes are included on the corresponding software CD and are available on the Juniper Networks Website.</td>
</tr>
<tr>
<td>Configuring Infranet Controllers Guide</td>
<td>Provides details about configuring the device features for all supported Infranet Controllers.</td>
</tr>
<tr>
<td>Configuring Secure Access Devices Guide</td>
<td>Provides details about configuring the device features for all supported Secure Access Devices.</td>
</tr>
<tr>
<td>Configuring EX-series Switches Guide</td>
<td>Provides details about configuring the device features for all supported EX-series platforms.</td>
</tr>
<tr>
<td>M-series and MX-series Devices Guide</td>
<td>Provides details about configuring the device features for M-series and MX-series platforms.</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.

- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.
Self-Help Online Tools and Resources

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

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

Opening a Case with JTAC

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

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.
PART 1

Getting Started

• Getting Started with NSM on page 3
• Understanding the JUNOS CLI and NSM on page 5
• Before You Begin Adding M-series and MX-series Devices on page 15
CHAPTER 1

Getting Started with NSM

- Introduction to Network and Security Manager on page 3
- Installing NSM on page 3
- Role-Based Administration on page 4

Introduction to Network and Security Manager

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

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

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

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

Related Topics
- Installing NSM on page 3
- Role-Based Administration on page 4
- NSM and Device Management Overview on page 5

Installing NSM

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

- Management System Installation Process
- User Interface Installation Process

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

**Related Topics**
- Introduction to Network and Security Manager on page 3
- Role-Based Administration on page 4
- NSM and Device Management Overview on page 5

**Role-Based Administration**

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

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

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

**Related Topics**
- Introduction to Network and Security Manager on page 3
- Installing NSM on page 3
- NSM and Device Management Overview on page 5
CHAPTER 2

Understanding the JUNOS CLI and NSM

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

NSM and Device Management Overview

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

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

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

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

Related Topics
- Understanding the CLI and NSM on page 6
- Comparing the CLI To the NSM UI on page 7
- NSM Services Supported for M-series and MX-series Devices on page 10
- How NSM Works with the CLI and Distributed Data Collection on page 11
- Device Schemas on page 12
Understanding the CLI and NSM

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

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

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

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

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

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

Related Topics

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

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

- **Operational mode**—This mode displays the current router status. In operational mode, you enter commands to monitor and troubleshoot the software, network connectivity, and router.

- **Configuration mode**—A router configuration is stored as a hierarchy of statements. In configuration mode, you enter these statements to define all properties of the JUNOS software, including interfaces, general routing information, routing protocols, user access, and several system hardware properties.

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

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

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

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

Copyright © 2010, Juniper Networks, Inc.
For more information about operational and configuration mode, see the JUNOS CLI User Guide.

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

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

Figure 1: Overview of the User Interface
• Menu bar—Contains clickable commands. You can access many menu bar commands using keyboard shortcuts. For a complete list of keyboards shortcuts, see the Network and Security Manager Online Help.

• Toolbar—Contains buttons for common tasks. The buttons displayed in the toolbar are determined by the selected module.

• Domain menu—Contains a pull-down menu above the navigation tree where domains and subdomains are selected. The domains and subdomains displayed are those to which the current user has access.

• Navigation Tree—The navigation tree displays the 11 NSM modules in the left pane of the NSM window.

• Investigate panel—Provides NSM modules with tree structures for monitoring your network.

• Configure panel—Provides NSM modules with tree structures for configuring devices, policies, virtual private networks (VPNs), and other objects.

• Administer panel—Provides NSM modules with tree structures for managing the NSM servers, ongoing jobs, and other actions.

• Main display area—Displays the content for the currently selected module or module contents.

• Common tasks pane—Provides links to commonly accessed tasks throughout the UI. These common tasks change depending on what tasks are often selected in the UI.

• Status bar—Displays additional information for a selected module.

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

Related Topics

• NSM and Device Management Overview on page 5

• Understanding the CLI and NSM on page 6

• NSM Services Supported for M-series and MX-series Devices on page 10

• How NSM Works with the CLI and Distributed Data Collection on page 11

• Device Schemas on page 12

• Communication Between a Device and NSM on page 13
NSM Services Supported for M-series and MX-series Devices

NSM supports the following services for the M-series and MX-series devices:

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

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

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

**Related Topics**

- NSM and Device Management Overview on page 5
- Understanding the CLI and NSM on page 6
- Comparing the CLI To the NSM UI on page 7
Before we can discuss how NSM works with the CLI, the following terms need to be defined:

- **ADM (Abstract Data Model)**—The Abstract Data Model is an XML file that contains all the configuration information for a domain.

- **configlet**—A configlet is a small, static configuration file that contains information on how a device can connect to NSM.

- **Device Server**—The Device Server is the component of the NSM management system that handles communication between the GUI Server and the device, collects data from the managed devices on your network, formats configuration information sent to your managed device, and consolidates log and event data.

- **DM (Data Model)**—A Data Model is an XML file that contains configuration data for an individual device. The DM is stored in the Device Server; when you create, update, or import a device, the GUI Server edits the Abstract Data Model (ADM) to reflect the changes, then translates that information to the DM.

- **GUI Server**—The GUI Server manages the system resources and data that drives NSM functionality. The GUI Server contains the NSM databases and centralizes information for devices and their configurations, attack and server objects, and policies.

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

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

When you create, update, or import a device into NSM, the GUI Server edits the ADM to reflect the changes, then translates that information to the DM. The ADM contains configuration data for all objects in a specific domain. When you use the UI to interface with your managed devices, the ADM and DMs work together.
When you update a device configuration, the GUI Server translates the objects and object attributes in the ADM domain into device configuration information in a DM. For DMI based devices which include the M-series and MX-series, the Device Server converts the DM into an XML configlet and sends the configlet through NetConf protocol to the device.

When you import a device configuration, the device sends the configuration through the NetConf protocol as an XML document to the Device Server, which translates the XML document into a DM with device configuration information. The GUI Server then translates the device configuration in the DM into objects and object attributes in the ADM, and uses the ADM to display current information in the UI.

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

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

**Related Topics**

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

**Device Schemas**

The structure of the ADM and the DMs is defined by a DM schema, which lists all the possible fields and attributes for a type of object or device. The DM schema reads from a capability file, which lists the fields and attributes that a specific operating system version supports, to determine the supported features for the operating system version.
that is running on the managed devices. NSM uses capability files to enable JUNOS software upgrades without changing the device configuration in NSM.

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

**Related Topics**
- NSM and Device Management Overview on page 5
- Understanding the CLI and NSM on page 6
- Comparing the CLI To the NSM UI on page 7
- NSM Services Supported for M-series and MX-series Devices on page 10
- How NSM Works with the CLI and Distributed Data Collection on page 11
- Communication Between a Device and NSM on page 13

### Communication Between a Device and NSM

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

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

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

**Related Topics**
- NSM and Device Management Overview on page 5
- Understanding the CLI and NSM on page 6
- Comparing the CLI To the NSM UI on page 7
- NSM Services Supported for M-series and MX-series Devices on page 10
- How NSM Works with the CLI and Distributed Data Collection on page 11
- Device Schemas on page 12
CHAPTER 3

Before You Begin Adding M-series and MX-series Devices

- M-series and MX-series Devices Supported by NSM on page 15
- Considering the Device Status on page 16
- Configuring a Deployed M-series or MX-series Device for Importing to NSM on page 16

**M-series and MX-series Devices Supported by NSM**

Table 5 on page 15 lists the M-series Internet routers, MX-series Internet Services routers, and the operating system versions supported by NSM.

**Table 5: M-series Internet Routers and MX-series Internet Service Routers**

<table>
<thead>
<tr>
<th>Device</th>
<th>Operating System Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Juniper Networks M7i Internet router</td>
<td>JUNOS Release 9.3</td>
</tr>
<tr>
<td>Juniper Networks M10i Internet router</td>
<td>JUNOS Release 9.3</td>
</tr>
<tr>
<td>Juniper Networks M40e Internet router</td>
<td>JUNOS Release 9.3</td>
</tr>
<tr>
<td>Juniper Networks M120 Internet router</td>
<td>JUNOS Release 9.3</td>
</tr>
<tr>
<td>Juniper Networks M320 Internet router</td>
<td>JUNOS Release 9.3</td>
</tr>
<tr>
<td>Juniper Networks MX240 Internet Services router</td>
<td>JUNOS Release 9.3</td>
</tr>
<tr>
<td>Juniper Networks MX480 Internet Services router</td>
<td>JUNOS Release 9.3</td>
</tr>
<tr>
<td>Juniper Networks MX960 Internet Services router</td>
<td>JUNOS Release 9.3</td>
</tr>
</tbody>
</table>

**Related Topics**

- Considering the Device Status on page 16
- Configuring a Deployed M-series or MX-series Device for Importing to NSM on page 16
Considering the Device Status

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

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

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

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

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

## Related Topics
- M-series and MX-series Devices Supported by NSM on page 15
- Configuring a Deployed M-series or MX-series Device for Importing to NSM on page 16

## Configuring a Deployed M-series or MX-series Device for Importing to NSM

A deployed device is a device you are currently using in your network. Before you can add a deployed device to NSM, you must configure the following parameters on the device, regardless of the static or dynamic nature of the IP address:
• The management interface (fxp0) with the IP address of the device
• A user with full administrative privileges for the NSM administrator
• A physical connection to your network with access to network resources
• Connectivity to the NSM device server, which can be with a static IP address
• Telnet or SSHv2, and NETCONF protocol over SSH

To configure these parameters, perform the following tasks:

• Configure an IP Address and a User with Full Administrative Privileges for the Device on page 17
• Check Network Connectivity on page 17
• Check Connectivity to the NSM Server on page 17
• Configure a Static Route to the NSM Server on page 18
• Establish a Telnet or an SSHv2, and a NETCONF protocol over SSH Connection to the NSM Server on page 19

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

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

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

For information on configuring the router from scratch, see the JUNOS System Basics Configuration Guide.

For step-by-step instructions on reconfiguring names, addresses, and the root password after reinstalling the JUNOS software, see “Configure Names and Addresses” and “Set the Root Password.”

Check Network Connectivity

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

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

  root@ > ping address

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

Check Connectivity to the NSM Server

Purpose Establish that the M-series or MX-series device has a connection to the NSM server.
Action  To check that the device has a connection to the NSM server, log on to the M-series or MX-series device and issue a ping command to the IP address of the NSM server:

```
root@> ping address
```

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

Configure a Static Route to the NSM Server

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

Action  To configure a static route, follow these steps:

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

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

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

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

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

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

4. Verify the configuration:

   ```
   user@host# show
   ```

5. Commit the configuration:

   ```
   user@host# commit
   ```

6. Verify the connection to the NSM server:

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

Sample Output  

```
user@host> edit
Entering configuration mode

[edit]
user@host# edit routing-options

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

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

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

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

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

1. Log on to the M-series or MX-series device.
2. In configuration mode, go to the following hierarchy level:
   
   
   [edit system services]

3. At the [edit system services] hierarchy level, enter the following commands:

   user@host# set ftp
   user@host# set ssh protocol-version v2
   user@host# set telnet
   user@host# set netconf ssh

4. Verify the configuration:

   user@host# show
5. Commit the configuration:

   user@host# commit

Sample Output

[edit]
user@host# edit system services

[edit system services]
user@host# set ftp

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

[edit system services]
user@host# set telnet

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

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

[edit system services]
user@host# commit
commit complete
PART 2

Integrating M-series and MX-series Devices

- Adding M-series and MX-series Devices Overview on page 23
- Updating M-series and MX-series Devices Overview on page 29
CHAPTER 4

Adding M-series and MX-series Devices

Overview

- About Device Creation on page 23
- Supported Add Device Workflows for M-series and MX-series Devices on page 24
- Importing Devices Overview on page 25
- Modeling Devices Overview on page 26
- Adding Multiple Devices Using Automatic Discovery (JUNOS Software Devices Only) on page 27
- Adding Device Groups Overview on page 27

About Device Creation

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

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

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

- Import deployed devices—Deployed devices are the devices you are currently using in your existing network. These devices have already been configured with a static or dynamic IP address and other basic information. For deployed devices, you can import the existing device configuration information into NSM.
NOTE: To import device configurations, the connection between NSM and the managed device must be at least 28.8 Kbps. For details on installing NSM on your network, refer to the Network and Security Manager Installation Guide.

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

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

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

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

**Related Topics**
- Supported Add Device Workflows for M-series and MX-series Devices on page 24
- Importing Devices Overview on page 25
- Modeling Devices Overview on page 26
- Adding Multiple Devices Using Automatic Discovery (JUNOS Software Devices Only) on page 27
- Adding Device Groups Overview on page 27

**Supported Add Device Workflows for M-series and MX-series Devices**

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

- Import device with static IP address
- Import device with dynamic IP address
- Model and activate device
- Rapid deployment (configlets)
- Device discovery
Import many devices (CSV file) with static IP addresses
Import many devices (CSV file) with dynamic IP addresses
The model many devices (CSV file) workflow is not supported.

Related Topics
• About Device Creation on page 23
• Importing Devices Overview on page 25
• Modeling Devices Overview on page 26
• Adding Multiple Devices Using Automatic Discovery (JUNOS Software Devices Only) on page 27
• Adding Device Groups Overview on page 27

Importing Devices Overview

NSM can import device configurations from M-series and MX-series devices running JUNOS 9.3 or later.

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

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

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

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

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

• A physical connection to your network with access to network resources
• Connectivity to the NSM Device Server, which can be with a static IP address
• A Telnet or an SSHv2, and a NETCONF protocol over SSH connection
NOTE: After importing a device configuration, log entries from that device begin to appear in the Log Viewer. However, until you update the device from NSM, the following log fields display 0 (or unknown):

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

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

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

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

Related Topics

- About Device Creation on page 23
- Supported Add Device Workflows for M-series and MX-series Devices on page 24
- Modeling Devices Overview on page 26
- Adding Multiple Devices Using Automatic Discovery (JUNOS Software Devices Only) on page 27
- Adding Device Groups Overview on page 27

Modeling Devices Overview

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

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

1. Model the device in the UI.
2. Create the device object configuration.
3. Activate the device.
4. Update the device configuration.
For more detailed information and steps about modeling a device, see “Modeling Devices” in the Network and Security Manager Administration Guide.

**Related Topics**
- About Device Creation on page 23
- Supported Add Device Workflows for M-series and MX-series Devices on page 24
- Importing Devices Overview on page 25
- Adding Multiple Devices Using Automatic Discovery (JUNOS Software Devices Only) on page 27
- Adding Device Groups Overview on page 27

**Adding Multiple Devices Using Automatic Discovery (JUNOS Software Devices Only)**

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

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

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

**Related Topics**
- About Device Creation on page 23
- Supported Add Device Workflows for M-series and MX-series Devices on page 24
- Importing Devices Overview on page 25
- Modeling Devices Overview on page 26
- Adding Device Groups Overview on page 27

**Adding Device Groups Overview**

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

Use the groups to:
- Deploy new or updated device configurations to the entire device group.
- Deploy new or updated policies to the entire device group.
The devices that you add to a device group must exist; that is, you must have previously added or modeled the devices in the domain. You can group devices before configuring them. You can add a device to more than one device group. You can also add a device group to another device group.

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

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

Related Topics
- About Device Creation on page 23
- Supported Add Device Workflows for M-series and MX-series Devices on page 24
- Importing Devices Overview on page 25
- Modeling Devices Overview on page 26
- Adding Multiple Devices Using Automatic Discovery (JUNOS Software Devices Only) on page 27
CHAPTER 5

Updating M-series and MX-series Devices

Overview

- About Updating M-series and MX-series Devices on page 29
- How the Update Process Works on page 30
- Job Manager on page 31
- Tracking Updated Devices Using Job Manager on page 32
- Reviewing Job Information Displayed in Job Manager on page 33
- Device States Displayed in Job Manager During Update on page 34
- Understanding Updating Errors Displayed in the Job Manager on page 35

About Updating M-series and MX-series Devices

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

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

Updating a device is a three-step process.

1. Ensure that you have configured the device correctly, created and assigned a policy to the device, and established a connection between the device and the management server.

2. From the Device Manager launchpad, select Update Device. The launchpad displays the Update Device(s) dialog box.

   All connected and managed devices appear in the device list. Modeled devices and devices awaiting import for the first time do not appear.
3. Select the devices or device groups you want to update and click **Apply Changes**. NSM updates the selected devices or device groups with the modeled configuration.

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

- **Audit Log Viewer**—This NSM module records changes made to a device configuration. The audit log entry also identifies the administrator who performed the change, shows when the change was updated on the device, and provides a history of change details.

- **Configuration Summaries**—These tools provide a preview of the modeled configuration, enabling you to compare it with the configuration that is running on the device. Use configuration summaries to ensure the modeled configuration is consistent with what you want to update on the device.

- **Job Manager**—This NSM module tracks the status of running and completed update processes. The Job Manager displays details of the update process in a dedicated information window and includes the update’s success or failure and errors involved in a failed update.

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

**Related Topics**
- How the Update Process Works on page 30
- Job Manager on page 31
- Tracking Updated Devices Using Job Manager on page 32
- Reviewing Job Information Displayed in Job Manager on page 33
- Device States Displayed in Job Manager During Update on page 34
- Understanding Updating Errors Displayed in the Job Manager on page 35

**How the Update Process Works**

After you have successfully added the device to NSM, reviewed the device configuration, updated the device, and have the managed device functioning normally, an event might occur on the managed device that requires a change to the device configuration. For example, malicious traffic might have entered your network, requiring you to update the device to detect and prevent that attack.
1. Using the NSM monitoring tools, you learn of the attack and locate the cause of the event. Using NSM modules such as the Realtime Monitor and Log Viewer, you determine the exact attack that penetrated the device. From the Report Manager, you also determine what rule in the security policy was ineffective in blocking the attack.

2. You update the modeled device configuration, editing the configuration to detect and prevent the attack from entering your network again.

3. Before updating the running configuration, you review the modeled device configuration. Using a delta configuration summary, compare the modeled configuration with the running configuration on the device to confirm the differences. Fine-tune the modeled configuration, if needed.

4. When you are confident that the modeled configuration is valid, update the device. NSM updates the running configuration with only the new changes (delta). During the update, you track the update progress using Job Manager in real time and observe the transfer of the configuration from NSM to the device.

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

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

**Related Topics**

- About Updating M-series and MX-series Devices on page 29
- Job Manager on page 31
- Tracking Updated Devices Using Job Manager on page 32
- Reviewing Job Information Displayed in Job Manager on page 33
- Device States Displayed in Job Manager During Update on page 34
- Understanding Updating Errors Displayed in the Job Manager on page 35

**Job Manager**

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

Job Manager tracks the progress of the command as it travels to the device and back to the management system. Each job contains:
• Name of the command
• Date and time the command was sent
• Completion status for each device that received the command
• Detailed description of command progress
• Command output, such as a configuration list or command-line interface (CLI) changes on the device

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

Related Topics
• About Updating M-series and MX-series Devices on page 29
• How the Update Process Works on page 30
• Tracking Updated Devices Using Job Manager on page 32
• Reviewing Job Information Displayed in Job Manager on page 33
• Device States Displayed in Job Manager During Update on page 34
• Understanding Updating Errors Displayed in the Job Manager on page 35

Tracking Updated Devices Using Job Manager

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

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

Job Manager includes the following utilities and information:

• View Controls—Use View controls to set the information level you want displayed in Job Manager:
  • Expand All displays all devices associated with a directive type.
  • Collapse All displays the directive type.

• Job Type (Directive) List—Displays the job type (directives) and associated timestamp completion status information. All current and completed jobs appear, including device updates. However, if you have not yet performed an update using NSM, the Job List does not display an Update Configuration directive.
- Notification Controls—Enables you to manually view job completion status.
- Job Information—Enables you to view job information, including errors, job completion status, job state, automatic job completion notification setting, and start time of job.

**Related Topics**
- About Updating M-series and MX-series Devices on page 29
- How the Update Process Works on page 30
- Job Manager on page 31
- Reviewing Job Information Displayed in Job Manager on page 33
- Device States Displayed in Job Manager During Update on page 34
- Understanding Updating Errors Displayed in the Job Manager on page 35

**Reviewing Job Information Displayed in Job Manager**

The Job Information dialog box displays the changing device states as the directive is executed. Device state changes, error messages, and warning messages are displayed in real time. A sample Job Information dialog box is shown in Figure 3 on page 33.

**Figure 3: Job Information Dialog Box**

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

The job information includes:
Job Type—The type of task being tracked. Job types include Update Device, Reboot Device, and Config Summary. Job type is also known as a directive.

Timestamp—The time at which NSM began executing the directive.

Admin Name—The name of the administrator logged into NSM.

Status—The current state of the job.

Completion—The number of jobs completed out of the total number of jobs.

Percent—The percentage of total jobs successfully executed. When performing multiple jobs on multiple devices, this field displays the percentage complete for each device. When the job has completed, successfully or unsuccessfully, this field displays 100%.

Name—The name of the device on which the job is executed.

Description—The current state of the job.

Completion—The percentage of a job that has executed successfully.

Output—Displays the content of the update, including commands that have been interpreted from the NSM data model into device-specific commands, error messages, and existing commands deleted from the device. The Output Display Region displays all errors, warnings, device verification output, and device state information associated with the job.

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

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

Related Topics

- About Updating M-series and MX-series Devices on page 29
- How the Update Process Works on page 30
- Job Manager on page 31
- Tracking Updated Devices Using Job Manager on page 32
- Device States Displayed in Job Manager During Update on page 34
- Understanding Updating Errors Displayed in the Job Manager on page 35

Device States Displayed in Job Manager During Update

During an update, the managed device changes device state. You can view the current device state in real time in the State Description field of the Job Information dialog box. Table 6 on page 35 lists the states that a device can have.
Table 6: Device States During Update

<table>
<thead>
<tr>
<th>Device State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No update activity has occurred on the device.</td>
</tr>
<tr>
<td>Loading in Progress</td>
<td>NSM is sending the update image to the flash memory of the device.</td>
</tr>
<tr>
<td>Pending</td>
<td>Device is accepting the parameters from the update configuration that has been sent to the device flash memory.</td>
</tr>
<tr>
<td>Converting Data Model to Device Data Model</td>
<td>The parameters that have been set in the NSM configuration are being changed to corresponding device-specific CLI commands that execute on the device.</td>
</tr>
<tr>
<td>Successful Completion</td>
<td>Device has successfully been updated with the modeled configuration.</td>
</tr>
<tr>
<td>Failed</td>
<td>Device has not been successfully updated with the modeled configuration. The Job Information dialog box displays error messages and error codes.</td>
</tr>
</tbody>
</table>

**Related Topics**
- About Updating M-series and MX-series Devices on page 29
- How the Update Process Works on page 30
- Job Manager on page 31
- Tracking Updated Devices Using Job Manager on page 32
- Reviewing Job Information Displayed in Job Manager on page 33
- Understanding Updating Errors Displayed in the Job Manager on page 35

**Understanding Updating Errors Displayed in the Job Manager**

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

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

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

Figure 4 on page 36 shows that on December 4 a configuration update to an MX960 failed. The super user was locked out by the root user as indicated in the text of the error.
that shows **lock Failed** and **configuration database locked by: root**. For an M-series or MX-series device, NSM attempts to acquire an exclusive lock on the candidate configuration so that the update can proceed. In this instance, the root user was updating the configuration, probably from the CLI, preventing NSM from locking and successfully updating the configuration.

**Figure 4: Failed Update Job Information Dialog Box**

In the Job Information dialog box, the update:

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

At the end of the error message, there are some suggestions as to how to proceed. In this particular case, the second solution, `> request system logout pid xxxx`, is the appropriate action. From the CLI, the `request system logout pid pid` command can be used to forcibly log out the root user. The root user is represented by `pid pid`, which indicates the user session using the specified management process identifier (PID). After the root user is locked out, you can try to update the configuration again. NSM should lock the configuration and continue successfully.
After a device is updated, you can run a delta configuration summary to determine any remaining differences between the modeled configuration and the running configuration; the output of this summary appears in the Job Information dialog box. For successful updates, no discrepancies are found or displayed. For failed updates, the Job Information dialog box lists the remaining discrepancies.

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

**Related Topics**

- About Updating M-series and MX-series Devices on page 29
- How the Update Process Works on page 30
- Job Manager on page 31
- Tracking Updated Devices Using Job Manager on page 32
- Reviewing Job Information Displayed in Job Manager on page 33
- Device States Displayed in Job Manager During Update on page 34
PART 3

Configuring M-series and MX-series Devices

- Configuring M-series and MX-series Devices Overview on page 41
- Configuring Access on page 47
- Configuring Accounting Options on page 71
- Configuring Applications on page 79
- Configuring Bridge Domains on page 81
- Configuring Chassis on page 97
- Configuring Authentication on page 113
- Configuring Class of Service Features on page 121
- Configuring Event Options on page 151
- Configuring Firewall on page 159
- Configuring Forwarding Options on page 183
- Configuring Interfaces on page 207
- Configuring Multicast Snooping Options on page 237
- Configuring Policy Options on page 241
- Configuring Protocols on page 251
- Configuring Routing Options on page 361
- Configuring Security on page 389
- Configuring Services on page 391
- Configuring SNMP on page 463
CHAPTER 6

Configuring M-series and MX-series Devices Overview

- About Device Configuration on page 41
- M-series and MX-series Device Configuration Settings Supported in NSM on page 42
- Configuring Device Features on page 44
- Example: Configuration of Interfaces for MPLS in the CLI and NSM on page 45

About Device Configuration

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

- JUNOS System Basics Configuration Guide for system, chassis, security, and access parameters.
- JUNOS Network Interfaces Configuration Guide for interface parameters.
- JUNOS Configuration and Diagnostic Automation Guide for event options parameters.
- JUNOS VPNs Configuration Guide for policy options parameters.
- JUNOS Class of Service Configuration Guide for class of service parameters.
- JUNOS Services Interface Configuration Guide for service parameters.
For more information about editing device configurations in NSM, including using device templates, using configuration groups, and using configuration groups with templates, see “Configuring Devices” in the Network and Security Manager Administration Guide.

**Related Topics**
- M-series and MX-series Device Configuration Settings Supported in NSM on page 42
- Configuring Device Features on page 44
- Example: Configuration of Interfaces for MPLS in the CLI and NSM on page 45

### M-series and MX-series Device Configuration Settings Supported in NSM

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

---

**NOTE:** For detailed information about configuring specific features for M-series and MX-series devices, see the appropriate JUNOS software configuration guide.

---

**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.

Table 7 on page 42 provides a general guideline of the CLI hierarchy levels that are supported in the NSM configuration tree. For the exact parameters available, double-click the device in the Device Manager and select the **Configuration** tab. The configuration tree appears in the main display area with all parameters viewable or configurable from NSM.

### Table 7: The JUNOS Configuration Hierarchy and the NSM Configuration Tree

<table>
<thead>
<tr>
<th>Hierarchy Level</th>
<th>Available in the NSM Configuration Tree</th>
</tr>
</thead>
<tbody>
<tr>
<td>edit access</td>
<td>Yes</td>
</tr>
<tr>
<td>edit accounting-options</td>
<td>Yes</td>
</tr>
<tr>
<td>edit applications</td>
<td>Yes</td>
</tr>
<tr>
<td>edit bridge domains</td>
<td>Yes</td>
</tr>
<tr>
<td>edit chassis</td>
<td>Yes</td>
</tr>
<tr>
<td>edit class-of-service</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 7: The JUNOS Configuration Hierarchy and the NSM Configuration Tree (continued)

<table>
<thead>
<tr>
<th>Hierarchy Level</th>
<th>Available in the NSM Configuration Tree</th>
</tr>
</thead>
<tbody>
<tr>
<td>edit dynamic profiles</td>
<td>Yes</td>
</tr>
<tr>
<td>edit ethernet-switching-options</td>
<td>No</td>
</tr>
<tr>
<td>edit event-options</td>
<td>Yes</td>
</tr>
<tr>
<td>edit firewall</td>
<td>Yes</td>
</tr>
<tr>
<td>edit forwarding-options</td>
<td>Yes</td>
</tr>
<tr>
<td>edit groups</td>
<td>Yes</td>
</tr>
<tr>
<td>edit interfaces</td>
<td>Yes</td>
</tr>
<tr>
<td>edit logical-systems</td>
<td>Yes</td>
</tr>
<tr>
<td>edit multicast-snooping-options</td>
<td>Yes</td>
</tr>
<tr>
<td>edit poe</td>
<td>No</td>
</tr>
<tr>
<td>edit policy-options</td>
<td>Yes</td>
</tr>
<tr>
<td>edit protocols</td>
<td>Yes</td>
</tr>
<tr>
<td>edit routing-instances]</td>
<td>Yes</td>
</tr>
<tr>
<td>edit routing-options</td>
<td>Yes</td>
</tr>
<tr>
<td>edit schedulers</td>
<td>No</td>
</tr>
<tr>
<td>edit security</td>
<td>Yes</td>
</tr>
<tr>
<td>edit services</td>
<td>Yes</td>
</tr>
<tr>
<td>edit snmp</td>
<td>Yes</td>
</tr>
<tr>
<td>edit switch-options</td>
<td>Yes</td>
</tr>
<tr>
<td>edit system</td>
<td>Yes</td>
</tr>
<tr>
<td>edit virtual-chassis</td>
<td>No</td>
</tr>
<tr>
<td>edit vlans</td>
<td>No</td>
</tr>
</tbody>
</table>
When you use NSM to edit the software configuration on the device, you initially make the changes to a device object that models the device in NSM. When you are satisfied with your configuration changes, you use the Update Device directive to push the configuration from the device object in NSM to the device itself. At that point, the edited configuration becomes active.

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

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

### Related Topics
- About Device Configuration on page 41
- Configuring Device Features on page 44
- Example: Configuration of Interfaces for MPLS in the CLI and NSM on page 45

### Configuring Device Features

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

**NOTE:** For detailed information about configuring specific features for M-series and MX-series devices, see the appropriate JUNOS software configuration guide.

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

1. In the navigation tree, select **Device Manager > Devices**.
2. Open the device configuration using one of the following methods:
   - Double-click the device object in the security device tree or the device list.
   - Select the device object and then click the Edit icon.
   - Right-click the device object and select **Edit**.
3. Select the **Configuration** tab.
   - The device configuration tree appears in the left pane.
4. In the device navigation tree, select a function heading to see device parameters, and then select the configuration parameter you want to configure.
5. Make your changes to the device configuration, then choose one of the following:
   - Click **OK** to save your changes and close the device configuration.
   - Click **Apply** to save your changes and continue making changes.
Click **Cancel** to discard all changes and close the device configuration.

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

**Related Topics**

- About Device Configuration on page 41
- M-series and MX-series Device Configuration Settings Supported in NSM on page 42
- Example: Configuration of Interfaces for MPLS in the CLI and NSM on page 45

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

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

The following figures show the same configuration displayed in the CLI and the NSM UI. Figure 5 on page 45 shows the CLI configuration of MPLS at the `[edit protocols mpls]` hierarchy level, and Figure 6 on page 46 shows the same configuration in the NSM UI.

Figure 5 on page 45 shows output for the `show` command in configuration mode. At this level, the `show` command typically displays the entire configuration for the device. For the purpose of this illustration, all parts of the configuration not relevant to our example were removed `[...Output Truncated...]`. The remaining output shows the protocols and MPLS hierarchy levels. Included at the hierarchy level are three interfaces, two Fast Ethernet interfaces (`fe`) and one Gigabit Ethernet interface (`ge`).

**Figure 5: MPLS Configuration in the CLI**

```plaintext
[edit]
user0# show
[...Output Truncated...]
protocols {
    mpls {
        interface ge-1/3/3.0;
        interface fe-0/1/2.0;
        interface fe-0/1/1.0;
    }
}
```

Figure 6 on page 46 shows the NSM UI with the same information as in the CLI example. On the left, the Navigation tree is expanded at Protocols, and then further expanded at MPLS, similar to the CLI hierarchy levels. Within MPLS, Interface is highlighted, indicating that the information on the right relates to interfaces within MPLS. The information in the NSM UI example is similar to the information in the CLI example though the presentation is somewhat different.
Figure 6: MPLS Configuration in NSM

In addition, Figure 6 on page 46 shows parts of the configuration tree that are grayed out, indicating that those particular parameters are not supported for the M-series and MX-series devices.

Related Topics
- About Device Configuration on page 41
- M-series and MX-series Device Configuration Settings Supported in NSM on page 42
- Configuring Device Features on page 44
CHAPTER 7

Configuring Access

- Configuring Address-Assignment Pools (NSM Procedure) on page 47
- Configuring Access Address Pools (NSM Procedure) on page 50
- Configuring Access Group Profile (NSM Procedure) on page 51
- Configuring the LDAP Options (NSM Procedure) on page 52
- Configuring the LDAP Server (NSM Procedure) on page 53
- Configuring Access Profiles for L2TP or PPP Parameters (NSM Procedure) on page 54
- Configuring the RADIUS for Subscriber Access Management, L2TP, or PPP (NSM Procedure) on page 68
- Configuring the SecurID Server (NSM Procedure) on page 69
- Configuring the Access Profile (NSM Procedure) on page 70

Configuring Address-Assignment Pools (NSM Procedure)

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

To configure address assignment pools in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Access.
4. Select Address Assignment.
5. Add or modify settings as specified in Table 8 on page 48.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
## Table 8: Address Assignment Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the name of an address-assignment pool.</td>
<td>1. Click <strong>Pool</strong> next to <strong>Address Assignment</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to <strong>Pool</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the name to be assigned to the address-assignment pool.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td>Configure subnet information for an IPv4 address-assignment pool.</td>
<td>1. Click <strong>Family</strong> next to <strong>Pool</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Enable Feature</strong> check box to enable the option.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Inet</strong> next to <strong>Family</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Network</strong> box, enter the subnet information for an IPv4 address-assignment pool.</td>
</tr>
<tr>
<td>Configure address pools that can be used by different client applications.</td>
<td>1. Click <strong>Dhcp Attributes</strong> next to <strong>Inet</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. From the <strong>Maximum Lease Time</strong> list, select the maximum length of time, in seconds, that the lease is held for a client if the client does not renew the lease. This is equivalent to DHCP option 51.</td>
</tr>
<tr>
<td></td>
<td>4. From the <strong>Grace Period</strong> list, select the amount of time that the client retains the address lease after the lease expires. Range: 0 through 4,294,967,295 seconds Default: 0 (no grace period)</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Domain Name</strong> box, enter the name of the domain in which clients search for a DHCP server host.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Boot File</strong> box, enter the location of the boot file on the boot server. The filename can include a pathname.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Boot Server</strong> box, enter the name of the boot server advertised to DHCP clients.</td>
</tr>
<tr>
<td></td>
<td>8. In the <strong>Tftp Server</strong> box, enter the IP address of the TFTP server.</td>
</tr>
<tr>
<td></td>
<td>9. From the <strong>Netbios Node Type</strong> list, select one of the following node types.</td>
</tr>
<tr>
<td></td>
<td>- <strong>b-node</strong>—Broadcast node</td>
</tr>
<tr>
<td></td>
<td>- <strong>h-node</strong>—Hybrid node</td>
</tr>
<tr>
<td></td>
<td>- <strong>m-node</strong>—Mixed node</td>
</tr>
<tr>
<td></td>
<td>- <strong>p-node</strong>—Peer-to-peer node</td>
</tr>
<tr>
<td></td>
<td>10. In the <strong>Sip Server Domain Name</strong> box, enter the domain name of the SIP outbound proxy server.</td>
</tr>
<tr>
<td>Configure one or more Domain Name System (DNS) name servers available to the client to resolve hostname-to-client mappings.</td>
<td>1. Click <strong>Name Server</strong> next to <strong>Dhcp Attributes</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to <strong>Name Server</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the IP addresses of the domain name servers, listed in order of preference.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
</tbody>
</table>
Table 8: Address Assignment Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify user-defined options that are added to client packets. | 1. Click **Option** next to Dhcp Attributes.  
2. Click **Add new entry** next to Option.  
3. From the Name list, select the ID number to be used to index the option.  
4. In the Comment box, enter the comment.  
5. Click **Flag** next to option.  
6. From the Flag list, select the flag type. |
| Specify a list of match criteria used to determine which named address range in the address-assignment pool to use. | 1. Click **Option Match** next to Dhcp Attributes.  
2. In the Comment box, enter the comment.  
3. Click **Option 82** next to Option Match.  
4. In the Comment box, enter the comment.  
5. Click **Circuit Id** next to Option 82.  
6. Click **Add new entry** next to Circuit Id.  
7. In the Name box, enter the name of the address-assignment pool range to be used.  
8. In the Comment box, enter the comment.  
9. In the Range box, enter the range.  
10. Click **Remote Id** next to Option 82.  
11. Click **Add new entry** next to Remote Id.  
12. In the Name box, enter the name of the address-assignment pool range to be used.  
13. In the Comment box, enter the comment.  
14. In the Range box, enter the range. |
| Specify one or more routers located on the client’s subnet. | 1. Click **Router** next to Dhcp Attributes.  
2. Click **Add new entry** next to Router.  
3. In the Name box, enter the name of the router.  
4. In the Comment box, enter the comment. |
| Specify SIP Servers list of IPv6 addresses available to the client. | 1. Click **Sip Server Address** next to Dhcp Attributes.  
2. Click **Add new entry** next to Sip Server Address.  
3. In the Name box, enter the SIP Servers list of IPv6 addresses available to the client.  
4. In the Comment box, enter the comment. |
| Specify one or more NetBIOS name servers (NBNS) that the client uses to resolve NetBIOS names. | 1. Click **Wins Server** next to Dhcp Attributes.  
2. Click **Add new entry** next to Wins Server.  
3. In the Name box, enter the IP address of each NetBIOS name server.  
4. In the Comment box, enter the comment. |
### Table 8: Address Assignment Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a static binding for the specified client.</td>
<td>1. Click <strong>Host</strong> next to Inet.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Host.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the name of the client.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Hardware Address</strong> box, enter the MAC address of the client.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>IP Address</strong> box, enter the IPv4 address.</td>
</tr>
<tr>
<td>Configure a named range of IPv4 addresses or IPv6 prefixes, used within an address-assignment pool.</td>
<td>1. Click <strong>Range</strong> next to Inet.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Range.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the name assigned to the range of IPv4 addresses or IPv6 prefixes.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Low</strong> box, enter the lower limit of an address range or IPv6 prefix range.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>High</strong> box, enter the upper limit of an address range or IPv6 prefix range.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Configuring Access Address Pools (NSM Procedure) on page 50
- Configuring Access Group Profile (NSM Procedure) on page 51

### Configuring Access Address Pools (NSM Procedure)

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

To configure access address pools in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Address Pool**.
5. Add or modify settings as specified in Table 9 on page 51.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.
Table 9: Access Address Pool Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocate IP addresses</td>
<td>1. Click <code>Address Pool</code> next to <code>Access</code>.</td>
</tr>
<tr>
<td>for clients.</td>
<td>2. Click <code>Add new entry</code> next to <code>Address Pool</code>.</td>
</tr>
<tr>
<td></td>
<td>3. In the <code>Name</code> box, enter the name to be assigned to an address pool.</td>
</tr>
<tr>
<td></td>
<td>4. In the <code>Comment</code> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. Click <code>Address</code> next to <code>address-pool</code>. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Select <code>address</code> to enter the address.</td>
</tr>
<tr>
<td></td>
<td>• Select <code>address-range</code> to configure the address range.</td>
</tr>
<tr>
<td></td>
<td>a. In the <code>Low</code> box, enter the lower limit of an address range.</td>
</tr>
<tr>
<td></td>
<td>b. In the <code>High</code> box, enter the upper limit of an address range.</td>
</tr>
</tbody>
</table>

Allocate IP addresses for clients.

Table 10: Access Group Profile Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the group</td>
<td>1. Click <code>Add new entry</code> next to <code>Group Profile</code>.</td>
</tr>
<tr>
<td>profile.</td>
<td>2. In the <code>Name</code> box, enter the name to be assigned to the group profile.</td>
</tr>
<tr>
<td></td>
<td>3. In the <code>Comment</code> box, enter the comment.</td>
</tr>
</tbody>
</table>

Configure the group profile.

Related Topics

- Configuring Address-Assignment Pools (NSM Procedure) on page 47
- Configuring Access Group Profile (NSM Procedure) on page 51

Configuring Access Group Profile (NSM Procedure)

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

To configure access group profile in NSM:

1. In the NSM navigation tree, select `Device Manager > Devices`.
2. Click the `Device Tree` tab, and then double-click the device to select it.
3. Click the `Configuration` tab. In the configuration tree, expand `Access`.
4. Select `Group Profile`.
5. Add or modify settings as specified in Table 10 on page 51.
6. Click one:
   • OK—Saves the changes.
   • Cancel— Cancels the modifications.
Table 10: Access Group Profile Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure the PPP attributes for a group profile. | 1. Click **PPP** next to group-profile.  
2. Select the **Enable Feature** check box to enable the option.  
3. In the **Comment** box, enter the comment.  
4. From the **Framed Pool** list, select the configured address pool.  
5. From the **Idle Timeout** list, select the number of seconds a user can remain idle before the session is terminated.  
   Range: 0 through 4,294,967,295 seconds  
   Default: 0  
6. From the **Keep Alive** list, select the time period that must elapse before the JUNOS Software checks the status of the Point-to-Point Protocol (PPP) session by sending an echo request to the peer.  
   Range: 0 through 32,767 seconds  
   Default: 10  
7. In the **Primary Dns** box, enter the primary Domain Name System (DNS) server.  
8. In the **Secondary Dns** box, enter the secondary Domain Name System (DNS) server.  
9. In the **Primary Wins** box, enter the primary Windows Internet name server.  
10. In the **Secondary Wins** box, enter the secondary Windows Internet name server.  
11. From the **Encapsulation Overhead** list, select the number of bytes used as encapsulation overhead for the session.  
12. Select the **Cell Overhead** check box to configure the session to use Asynchronous Transfer Mode (ATM)-aware egress shaping on the IQ2 PIC.  
13. In the **Interface id** box, enter the interface identifier. |

**Related Topics**  
- Configuring Access Profiles for L2TP or PPP Parameters (NSM Procedure) on page 54

**Configuring the LDAP Options (NSM Procedure)**

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

To configure LDAP options in NSM:
1. In the NSM navigation tree, select **Device Manager > Devices**.  
2. Click the **Device Tree** tab, and then double-click the device to select it.  
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.  
4. Select **Ldap Options**.  
5. Add or modify settings as specified in Table 11 on page 53.  
6. Click one:
• OK—Saves the changes.
• Cancel—Cancels the modifications.

Table 11: LDAP Options Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure lightweight directory access protocol options. | 1. In the Comment box, enter the comment.  
2. From the Revert Interval list, select the amount of time the router waits after a server has become unreachable.  
Range: 60 through 4,294,967,295  
Default: 600  
3. In the Base Distinguished Name box, enter the suffix when assembling user distinguished name (DN) or base DN under which to search for user DN. |
| Derive user distinguished name from common-name and base-distinguished-name. | 1. Click Assemble next to Ldap Options.  
2. Select one of the following:  
• assemble—To derive user distinguished name from common-name and base-distinguished-name.  
a. In the Comment box, enter the comment.  
b. In the Common Name box, enter the common name.  
• search—To search for user’s distinguished name.  
a. In the Comment box, enter the comment.  
b. In the Search Filter box, enter the filter to use in search.  
c. Click Admin Search next to Search.  
d. In the Comment box, enter the comment.  
e. In the Distinguished Name box, enter the user distinguished name.  
f. In the Password box, enter the password. |

Related Topics
• Configuring the LDAP Server (NSM Procedure) on page 53

Configuring the LDAP Server (NSM Procedure)

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

To configure LDAP server in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Access.
4. Select Ldap Server.
5. Add or modify settings as specified in Table 12 on page 54.
6. Click one:
- OK—Saves the changes.
- Cancel—Cancels the modifications.

**Table 12: LDAP Server Configuration Details**

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure LDAP server.</td>
<td>1. Click <strong>Add new entry</strong> next to Ldap Server.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Name</strong> box, enter the name of the server.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. From the <strong>Port</strong> list, select the port number on which to contact the</td>
</tr>
<tr>
<td></td>
<td>Radius server (LDAP server)</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Source Address</strong> box, enter a valid IPv4 address configured on</td>
</tr>
<tr>
<td></td>
<td>one of the router interfaces. On M Series routers only, the source address</td>
</tr>
<tr>
<td></td>
<td>can be an IPv6 address and the UDP source port is 514.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Routing Instances</strong> list, select the routing instance name.</td>
</tr>
<tr>
<td></td>
<td>7. From the <strong>Retry</strong> list, select the number of times that the router is</td>
</tr>
<tr>
<td></td>
<td>allowed to attempt to contact a Radius server.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 10</td>
</tr>
<tr>
<td></td>
<td>Default: 3</td>
</tr>
<tr>
<td></td>
<td>8. From the <strong>Timeout</strong> list, select the amount of time that the local</td>
</tr>
<tr>
<td></td>
<td>router waits to receive a response from a Radius server.</td>
</tr>
<tr>
<td></td>
<td>Range: 3 through 90</td>
</tr>
<tr>
<td></td>
<td>Default: 5</td>
</tr>
</tbody>
</table>

**Related Topics**
- Configuring the LDAP Options (NSM Procedure) on page 52

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

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

1. Configuring Access Profile (NSM Procedure) on page 55
2. Configuring Accounting Parameters for Access Profiles (NSM Procedure) on page 55
3. Configuring the Accounting Order (NSM Procedure) on page 56
4. Configuring the Authentication Order (NSM Procedure) on page 57
5. Configuring the Authorization Order (NSM Procedure) on page 57
6. Configuring the L2TP Client (NSM Procedure) on page 58
7. Configuring the Client Filter Name (NSM Procedure) on page 59
8. Configuring the LDAP Options (NSM Procedure) on page 60
9. Configuring the LDAP Server (NSM Procedure) on page 61
10. Configuring the Provisioning Order (NSM Procedure) on page 62
Configuring Access Profile (NSM Procedure)

To configure an access profile in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Access.
4. Select Profile.
5. Add or modify settings as specified in Table 13 on page 55.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 13: Access Profile Properties Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure access profile properties. | 1. Click Add new entry next to Profile.  
2. In the Name box, enter the name of the profile.  
3. In the Comment box, enter the comment. |

Configuring Accounting Parameters for Access Profiles (NSM Procedure)

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

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Access.
4. Select Profile.
5. Add or modify settings as specified in Table 14 on page 56.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
Table 14: Accounting Parameter Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure RADIUS accounting parameters and enable RADIUS accounting</td>
<td>1. Click <strong>Add new entry</strong> next to Profile.</td>
</tr>
<tr>
<td>for an access profile.</td>
<td>2. Click <strong>Accounting</strong> next to profile.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. Select the <strong>Accounting Stop On Failure</strong> check box to configure</td>
</tr>
<tr>
<td></td>
<td>RADIUS accounting to send an Acct-Stop message when client access fails</td>
</tr>
<tr>
<td></td>
<td>AAA but the AAA server grants access.</td>
</tr>
<tr>
<td></td>
<td>5. Select the <strong>Accounting Stop On Access Deny</strong> check box to configure</td>
</tr>
<tr>
<td></td>
<td>RADIUS accounting to send an Acct-Stop message when the AAA server denies</td>
</tr>
<tr>
<td></td>
<td>a client access.</td>
</tr>
<tr>
<td></td>
<td>6. Select the <strong>Immediate Update</strong> check box to configure the router to</td>
</tr>
<tr>
<td></td>
<td>send an Acct-Update message to the RADIUS accounting server on receipt of</td>
</tr>
<tr>
<td></td>
<td>a response (for example, an ACK or timeout) to the Acct-Start message.</td>
</tr>
<tr>
<td></td>
<td>7. From the <strong>Update Interval</strong> list, select the amount of time between</td>
</tr>
<tr>
<td></td>
<td>updates, in minutes.</td>
</tr>
<tr>
<td></td>
<td>Range: 10 through 1440 minutes</td>
</tr>
<tr>
<td></td>
<td>Default: no updates</td>
</tr>
<tr>
<td></td>
<td>8. From the <strong>Statistics</strong> list, select the time statistics for the</td>
</tr>
<tr>
<td></td>
<td>sessions being managed by AAA.</td>
</tr>
</tbody>
</table>

Configuring the Accounting Order (NSM Procedure)

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

To configure accounting order in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in Table 15 on page 57.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.
Configuring the Authentication Order (NSM Procedure)

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

To configure authentication order in NSM:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Access.
4. Select Profile.
5. Add or modify settings as specified in Table 16 on page 57.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Configuring the Authorization Order (NSM Procedure)

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

---

**Table 15: Accounting Order Configuration Details**

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure the accounting order. | 1. Click Add new entry next to Profile.  
                                  2. Click Accounting Order next to Profile.  
                                  3. Click Add new entry next to Accounting Order.  
                                  4. In the New accounting-order window, select radius to use RADIUS accounting method. |

**Table 16: Authentication Order Configuration Details**

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure the authentication order. | 1. Click Add new entry next to Profile.  
                                  2. Click Authentication Order next to Profile.  
                                  3. Click Add new entry next to Accounting Order.  
                                  4. In the New authentication-order window, select the order in which the JUNOS Software tries different authentication methods when verifying that a client can access the router. |
5. Add or modify settings as specified in Table 17 on page 58.

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

### Table 17: Authorization Order Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the authorization</td>
<td>1. Click <strong>Add new entry</strong> next to Profile.</td>
</tr>
<tr>
<td>order.</td>
<td>2. Click <strong>Authorization Order</strong> next to Profile.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add new entry</strong> next to Authorization Order.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>New authorization-order</strong> window, select the authorization order.</td>
</tr>
</tbody>
</table>

### Configuring the L2TP Client (NSM Procedure)

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

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in Table 18 on page 58.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

### Table 18: Client Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the client.</td>
<td>1. Click <strong>Add new entry</strong> next to Profile.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Client</strong> next to Profile.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add new entry</strong> next to Client.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Name</strong> box, enter the client name.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Chap Secret</strong> box, enter the secret key associated with a peer.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>pap password</strong> box, enter the Password Authentication Protocol (PAP) password.</td>
</tr>
</tbody>
</table>

| Configure a client group.     | 1. Click **Client Group** next to client.                                   |
|                               | 2. Click **Add new entry** next to Client Group.                           |
|                               | 3. In the **New client-group** window, enter the client group.             |
Table 18: Client Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure a firewall user. | 1. Click **Firewall User** next to client.  
2. In the **Comment** box, enter the comment.  
3. In the **Password** box, enter the password. |
| Configure PPP properties for a client profile. | 1. Click **Ppp** next to client.  
2. Select **ike** to configure an IKE access profile.  
   a. In the **Comment** box, enter the comment.  
   b. Select **Initiate Dead Peer Detection** to detect inactive peers on dynamic IPSec tunnels.  
   c. In the **Interface Id** box, enter the interface identifier.  
   d. Click **Allowed Proxy Pair** next to Ike.  
   e. Click **Add new entry** next to Allowed Proxy Pair.  
   f. In the **Local** box, enter the network address of the local peer.  
   g. In the **Remote** box, enter the network address of the remote peer.  
   h. In the **Comment** box, enter the comment.  
   i. Click **Pre Shared Key** next to Ike.  
      a. Select **pre-shared-key** to configure the key used to authenticate a dynamic peer during IKE phase 1 negotiation and select the key.  
      b. In the **Comment** box, enter the comment.  
      c. Click **Ascii Text** next to Pre Shared key.  
      d. In the **ascii-text** box, enter the string.  
      e. Select **ike-policy** to authenticate dynamic peers during IKE negotiation and select the policy name. |

Configuring the Client Filter Name (NSM Procedure)

To configure restrictions on client names in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in Table 22 on page 62.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.
**Table 19: Client Filter Name Configuration Details**

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the restrictions on client names.</td>
<td>1. Click <strong>Add new entry</strong> next to Profile.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Client Name Filter</strong> next to profile.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Domain Name</strong> box, enter the domain name.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Separator</strong> box, enter the separator character in domain name.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Count</strong> list, select the number of separator instances.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 255</td>
</tr>
</tbody>
</table>

**Configuring the LDAP Options (NSM Procedure)**

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

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in Table 20 on page 60.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

**Table 20: Ldap Options Configuration Details**

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure lightweight directory access protocol options.</td>
<td>1. Click <strong>Add new entry</strong> next to Profile.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Ldap Options</strong> next to profile.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. From the <strong>Revert Interval</strong> list, select the amount of time the router waits after a server has become unreachable.</td>
</tr>
<tr>
<td></td>
<td>Range: 60 through 4294967295</td>
</tr>
<tr>
<td></td>
<td>Default: 600</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Base Distinguished Name</strong> box, enter the suffix when assembling user distinguished name (DN) or base DN under which to search for user DN.</td>
</tr>
</tbody>
</table>
Table 20: Ldap Options Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Derive user distinguished name from common-name and base-distinguished-name. | 1. Click **Assemble** next to Ldap Options.  
2. Select one of the following:  
  • **assemble**—To derive user distinguished name from common-name and base-distinguished-name.  
    a. In the **Comment** box, enter the comment.  
    b. In the **Common Name** box, enter the common name.  
  • **search**—To search for user’s distinguished name.  
    a. In the **Comment** box, enter the comment.  
    b. In the **Search Filter** box, enter the filter to use in search.  
    c. Click **Admin Search** next to Search.  
    d. In the **Comment** box, enter the comment.  
    e. In the **Distinguished Name** box, enter the user distinguished name.  
    f. In the **Password** box, enter the password. |
Table 21: Ldap Server Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure LDAP server.</td>
<td>1. Click <strong>Add new entry</strong> next to Profile.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Ldap Server</strong> next to profile.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add new entry</strong> next to Ldap Server.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Name</strong> box, enter the name of the server.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Port</strong> list, select the port number on which to contact the RADIUS server (LDAP server).</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Source Address</strong> box, enter a valid IPv4 address configured on one of the router interfaces. On M Series routers only, the source address can be an IPv6 address and the UDP source port is 514.</td>
</tr>
<tr>
<td></td>
<td>8. From the <strong>Routing Instances</strong> list, select the routing instance name.</td>
</tr>
<tr>
<td></td>
<td>9. From the <strong>Retry</strong> list, select the number of times that the router is allowed to attempt to contact a RADIUS server.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 10</td>
</tr>
<tr>
<td></td>
<td>Default: 3</td>
</tr>
<tr>
<td></td>
<td>10. From the <strong>Timeout</strong> list, select the amount of time that the local router waits to receive a response from a RADIUS server.</td>
</tr>
<tr>
<td></td>
<td>Range: 3 through 90</td>
</tr>
<tr>
<td></td>
<td>Default: 5</td>
</tr>
</tbody>
</table>

Configuring the Provisioning Order (NSM Procedure)

To configure the provisioning order in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in Table 22 on page 62.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.

Table 22: Provisioning Order Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the provisioning</td>
<td>1. Click <strong>Add new entry</strong> next to Profile.</td>
</tr>
<tr>
<td>order.</td>
<td>2. Click <strong>Provisioning Order</strong> next to profile.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add new entry</strong> next to Provisioning Order.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>New provisioning-order</strong> window, select the order in which provisioning mechanisms are used.</td>
</tr>
</tbody>
</table>
Configuring RADIUS Parameters for AAA Subscriber Management (NSM Procedure)

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

To configure RADIUS parameters for AAA subscriber management in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Access.
4. Select Profile.
5. Add or modify settings as specified in Table 23 on page 63.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

Table 23: RADIUS Parameter Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the RADIUS parameters.</td>
<td>1. Click Add new entry next to Profile.</td>
</tr>
<tr>
<td></td>
<td>2. Click Radius next to Profile.</td>
</tr>
<tr>
<td></td>
<td>3. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td>Specify a list of the RADIUS accounting servers used for accounting</td>
<td>1. Click Attributes next to Radius.</td>
</tr>
<tr>
<td>for Dynamic Host Configuration Protocol (DHCP), Layer 2 Tunneling</td>
<td>2. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td>Protocol (L2TP), and Point-to-Point Protocol (PPP) clients.</td>
<td></td>
</tr>
</tbody>
</table>
Configure the router to exclude the specified attributes from the specified type of RADIUS message.

1. Click Exclude next to Radius.
2. In the Comment box, enter the comment.
3. From the listed RADIUS attribute type, select the attributes to be excluded.

RADIUS attribute types are:
- **accounting-authentic**—RADIUS attribute 45, Acct-Authentic
- **accounting-delay-time**—RADIUS attribute 41, Acct-Delay-Time
- **accounting-session-id**—RADIUS attribute 44, Acct-Session-Id
- **accounting-terminate-cause**—RADIUS attribute 49, Acct-Terminate-Cause
- **called-station-id**—RADIUS attribute 30, Called-Station-Id
- **calling-station-id**—RADIUS attribute 31, Calling-Station-Id
- **class**—RADIUS attribute 25, Class
- **dhcp-gi-address**—Juniper VSA 26-57, DHCP-GI-Address
- **dhcp-mac-address**—Juniper VSA 26-56, DHCP-MAC-Address
- **Dhcp Options**—Excludes RADIUS attribute 26-55
- **event-timestamp**—RADIUS attribute 55, Event-Timestamp
- **framed-ip-address**—RADIUS attribute 8, Framed-IP-Address
- **framed-ip-netmask**—RADIUS attribute 9, Framed-IP-Netmask
- **input-filter**—Juniper VSA 26-10, Ingress-Policy-Name
- **input-gigapackets**—Juniper VSA 26-42, Acct-Input-Gigapackets
- **input-gigawords**—RADIUS attribute 52, Acct-Input-Gigawords
- **interface-description**—Juniper VSA 26-53, Interface-Desc
- **nas-identifier**—RADIUS attribute 32, NAS-Identifier
- **nas-port**—RADIUS attribute 5, NAS-Port
- **nas-port-id**—RADIUS attribute 87, NAS-Port-IId.
- **nas-port-type**—RADIUS attribute 61, NAS-Port-Type
- **output-filter**—Juniper VSA 26-11, Egress-Policy-Name
- **output-gigapackets**—Juniper VSA 25-43, Acct-Output-Gigapackets
- **output-gigawords**—RADIUS attribute 53, Acct-Output-Gigawords

---

**Table 23: RADIUS Parameter Configuration Details (continued)**

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the router to exclude the specified attributes from the</td>
<td>1. Click Exclude next to Radius.</td>
</tr>
<tr>
<td>specified type of RADIUS message.</td>
<td>2. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. From the listed RADIUS attribute type, select the attributes to be</td>
</tr>
<tr>
<td></td>
<td>excluded.</td>
</tr>
</tbody>
</table>

---

**RADIUS attribute types are:**

- **accounting-authentic**—RADIUS attribute 45, Acct-Authentic
- **accounting-delay-time**—RADIUS attribute 41, Acct-Delay-Time
- **accounting-session-id**—RADIUS attribute 44, Acct-Session-Id
- **accounting-terminate-cause**—RADIUS attribute 49, Acct-Terminate-Cause
- **called-station-id**—RADIUS attribute 30, Called-Station-Id
- **calling-station-id**—RADIUS attribute 31, Calling-Station-Id
- **class**—RADIUS attribute 25, Class
- **dhcp-gi-address**—Juniper VSA 26-57, DHCP-GI-Address
- **dhcp-mac-address**—Juniper VSA 26-56, DHCP-MAC-Address
- **Dhcp Options**—Excludes RADIUS attribute 26-55
- **event-timestamp**—RADIUS attribute 55, Event-Timestamp
- **framed-ip-address**—RADIUS attribute 8, Framed-IP-Address
- **framed-ip-netmask**—RADIUS attribute 9, Framed-IP-Netmask
- **input-filter**—Juniper VSA 26-10, Ingress-Policy-Name
- **input-gigapackets**—Juniper VSA 26-42, Acct-Input-Gigapackets
- **input-gigawords**—RADIUS attribute 52, Acct-Input-Gigawords
- **interface-description**—Juniper VSA 26-53, Interface-Desc
- **nas-identifier**—RADIUS attribute 32, NAS-Identifier
- **nas-port**—RADIUS attribute 5, NAS-Port
- **nas-port-id**—RADIUS attribute 87, NAS-Port-IId.
- **nas-port-type**—RADIUS attribute 61, NAS-Port-Type
- **output-filter**—Juniper VSA 26-11, Egress-Policy-Name
- **output-gigapackets**—Juniper VSA 25-43, Acct-Output-Gigapackets
- **output-gigawords**—RADIUS attribute 53, Acct-Output-Gigawords
### Table 23: RADIUS Parameter Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| **Configure the router to ignore the specified attributes in RADIUS Access-Accept messages.** | 1. Click **Ignore** next to client.  
2. In the **Comment** box, enter the comment.  
3. Select the following check boxes to ignore the specified attributes:  
   - **output-filter**—Egress-Policy-Name (VSA 26-11)  
   - **input-filter**—Ingress-Policy-Name (VSA 26-10)  
   - **framed-ip-netmask**—Framed-IP-Netmask (RADIUS attribute 9)  
   - **logical-system-routing-instance**—Virtual-Router (VSA 26-1) |
| **Specify a list of the RADIUS authentication servers used to authenticate DHCP, L2TP, and PPP clients.** | 1. Click **Authentication Server** next to Radius.  
2. Click **Add new entry** next to Authentication Server.  
3. In the **New authentication-server** window, enter the IPv4 address. |
| **Configure the options used by RADIUS authentication and accounting servers.** | 1. Click **Options** next to Radius.  
2. In the **Comment** box, enter the comment.  
3. Select the **Ethernet Port Type Virtual** check box to specify a port type of virtual.  
4. From the **Interface Description Format** list, select the information that is included in or omitted from the interface description that the router passes to RADIUS for inclusion in the RADIUS attribute 87 (NAS-Port-Id).  
   Select one of the following:  
   - **sub-interface**—To specify the subinterface.  
   - **adapter**—To specify the adapter.  
5. In the **NasIdentifier** box, enter a string in the range from 1 to 64 characters.  
6. From the **Accounting Session Id Format** list, select the format the router uses to identify the accounting session.  
   Select one of the following:  
   - **decimal**—To use the decimal format.  
   - **description**—To use the generic format, in the form jnpr interface-specifier:subscriber-session-id.  
   Default: decimal  
7. From the **Revert Interval** list, select the amount of time the router waits after a server has become unreachable.  
   Range: 60 through 4294967295 seconds  
   Default: 600 seconds  
8. Select the **vlan-nas-port-stacked-format** check box to configure RADIUS attribute 5 (NAS-Port) to include the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces. |
Table 23: RADIUS Parameter Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure the RADIUS client to use the extended format for RADIUS attribute 5 (NAS-Port) and specify the width of the fields in the NAS-Port attribute. | 1. Click Nas Port Extended Format next to Options.  
2. In the Comment box, enter the comment.  
3. From the Slot Width list, select the number of bits in the slot field.  
4. From the Adapter Width list, select the number of bits in the adapter field.  
5. From the Port Width list, select the number of bits in the port field.  
6. From the Stacked Vlan Width list, select the number of bits in the SVLAN ID field.  
7. From the Vlan Width list, select the number of bits in the VLAN ID field. |

Configuring the RADIUS Parameters (NSM Procedure)

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

To configure the RADIUS parameters in NSM:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Access.
4. Select Profile.
5. Add or modify settings as specified in Table 24 on page 66.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

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

Table 24: RADIUS Parameters Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure the RADIUS parameters.                                    | 1. Click Add new entry next to Profile.                                     
2. Click Radius Options next to Profile.                              
3. In the Comment box, enter the comment.                             
4. From the Revert Interval list, select the amount of time the router waits after a server has become unreachable. Default: 600 seconds.
Configuring the RADIUS for Subscriber Access Management, L2TP, or PPP (NSM Procedure)

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

To configure the RADIUS server in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Access.
4. Select Profile.
5. Add or modify settings as specified in Table 25 on page 67.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

Table 25: RADIUS Server Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the RADIUS servers.</td>
<td>1. Click Add new entry next to Profile</td>
</tr>
<tr>
<td></td>
<td>2. Click Radius Server next to Profile.</td>
</tr>
<tr>
<td></td>
<td>3. In the Name box, enter the profile name.</td>
</tr>
<tr>
<td></td>
<td>4. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. From the Port list, select the port number on which to contact the RADIUS server. Default: 1812 (as specified in RFC 2865)</td>
</tr>
<tr>
<td></td>
<td>6. In the Secret box, enter the password to use with the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td>The secret password used by the local router must match that used by the server.</td>
</tr>
<tr>
<td></td>
<td>7. From the Timeout list, select the amount of time that the local router waits to receive a response from a RADIUS server. Range: 3 through 90 seconds Default: 3 seconds</td>
</tr>
<tr>
<td></td>
<td>8. From the Retry list, select the number of times that the router is allowed to attempt to contact a RADIUS server. Range: 1 through 10 Default: 3</td>
</tr>
<tr>
<td></td>
<td>9. In the Source Address box, enter a valid IPv4 address configured on one of the router interfaces.</td>
</tr>
<tr>
<td></td>
<td>10. From the Routing Instance list, select the routing instance name.</td>
</tr>
</tbody>
</table>

Configuring Session Limit (NSM Procedure)

To configure the timeout limit in NSM:
1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Profile**.
5. Add or modify settings as specified in Table 26 on page 68.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

---

**Table 26: Session Limit Configuration Details**

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure the timeout interval. | 1. Click **Add new entry** next to Profile.  
                                | 2. Click **Session Options** next to Profile.  
                                | 3. In the **Comment** box, enter the comment.  
                                | 4. From the **Client Idle Timeout** list, select the time in minutes of idleness after which access is denied.  
                                | Range: 1 through 255 minutes  
                                | 5. From the **Client Session Timeout** list, select the time in minutes since initial access after which access is denied. |
| Configure a client group.   | 1. Click **Client Group** next to Session Option.  
                                | 2. Click **Add new entry** next to Client Group.  
                                | 3. In the **New client-group** window, enter the client group.                        |

---

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

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

To configure the RADIUS server in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Access**.
4. Select **Radius Server**.
5. Add or modify settings as specified in Table 27 on page 69.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
Table 27: RADIUS Server Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the RADIUS servers.</td>
<td>1. Click Add new entry next to Radius Server</td>
</tr>
<tr>
<td></td>
<td>2. In the Name box, enter the profile name.</td>
</tr>
<tr>
<td></td>
<td>3. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. From the Accounting Port list, select the port number on which to contact the accounting server. Default: 1813 (as specified in RFC 2865)</td>
</tr>
<tr>
<td></td>
<td>5. From the Port list, select the port number on which to contact the RADIUS server. Default: 1812 (as specified in RFC 2865)</td>
</tr>
<tr>
<td></td>
<td>6. In the Secret box, enter the password to use with the RADIUS server. The secret password used by the local router must match that used by the server.</td>
</tr>
<tr>
<td></td>
<td>7. From the Timeout list, select the amount of time that the local router waits to receive a response from a RADIUS server. Range: 1 through 90 seconds Default: 3 seconds</td>
</tr>
<tr>
<td></td>
<td>8. From the Retry list, select the number of times that the router is allowed to attempt to contact a RADIUS server. Range: 1 through 10 Default: 3</td>
</tr>
<tr>
<td></td>
<td>9. In the Source Address box, enter a valid IPv4 address configured on one of the router interfaces.</td>
</tr>
<tr>
<td></td>
<td>10. From the Routing Instance list, select the routing instance name.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring the RADIUS Parameters (NSM Procedure) on page 66

Configuring the SecurID Server (NSM Procedure)

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

To configure the SecurID server in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Access.
4. Select Securid Server.
5. Add or modify settings as specified in Table 28 on page 70.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
Table 28: SecurID Server Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure the SecurID server. | 1. Click Add new entry next to SecurID Server  
|                           | 2. In the Name box, enter the name of the SecurID server.  
|                           | 3. In the Comment box, enter the comment.  
|                           | 4. In the Configuration File box, enter the path to the SecurID server configuration (sdconf.rec) file. |

Related Topics

- Configuring the RADIUS for Subscriber Access Management, L2TP, or PPP (NSM Procedure) on page 68

Configuring the Access Profile (NSM Procedure)

To configure the access profile in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, select Access Profile.
4. Add or modify settings as specified in Table 29 on page 70.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 29: Access Profile Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configuring the access profile. | 1. In the Comment box, enter the comment.  
|                           | 2. In the Name box, enter the name of the access profile. |
**CHAPTER 8**

**Configuring Accounting Options**

- Configuring Accounting Options (NSM Procedure) on page 71

**Configuring Accounting Options (NSM Procedure)**

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

- Configuring Class Usage Profiles (NSM Procedure) on page 71
- Configuring a Log File (NSM Procedure) on page 72
- Configuring the Filter Profile (NSM Procedure) on page 73
- Configuring the Interface Profile (NSM Procedure) on page 74
- Configuring the Policy Decision Statistics Profile (NSM Procedure) on page 75
- Configuring the MIB Profile (NSM Procedure) on page 76
- Configuring the Routing Engine Profile (NSM Procedure) on page 77

**Configuring Class Usage Profiles (NSM Procedure)**

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

To configure class usage profiles in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Accounting Options.
4. Select Class Usage Profile.
5. Add or modify the settings as specified in Table 30 on page 72.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.
### Table 30: Class Usage Profile Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the class usage profile.</td>
<td>1. Click <strong>Add new entry</strong> next to Class Usage Profile.</td>
</tr>
<tr>
<td></td>
<td>2. Expand <strong>class-usage-profile</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the name of the destination class profile.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment for the class usage profile.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>File</strong> box, enter the name of the log file.</td>
</tr>
</tbody>
</table>
|                                           | 6. From the **Interval** list, select the amount of time between each collection of statistics.  
                                           | Range: 1 through 1048576 minutes  
                                           | Default: 30 minutes |
|                                           | 7. Click **Destination Classes** next to class-usage-profile and select one of the following: |
|                                           | • **destination-classes**—To configure the class usage profile to filter by source classes. |
|                                           | • **source-classes**—To configure the class usage profile to filter by destination classes. |
|                                           | 8. In the **Name** box, enter the name of the source classes or the destination classes. |
|                                           | 9. In the **Comment** box, enter the comment. |

#### Configuring a Log File (NSM Procedure)

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

To configure a log file in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Accounting Options**.
4. Select **File**.
5. Add or modify the settings as specified in Table 31 on page 73.
6. Click one:
   • **OK**—Saves the changes.
   • **Cancel**— Cancels the modifications.
Table 31: Log File Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure an accounting-data log file. | 1. Click Add new entry next to File.  
2. In the Name box, enter the filename.  
3. In the Comment box, enter the comment for the file.  
4. In the Size box, enter the maximum size of each log file in the range from 262144 through 1073741824 bytes.  
5. From the Files list, select the maximum number of files. Range: 1 through 1000  
Default: 10  
6. From the Transfer Interval list, select the time the file remains open and receives new statistics before it is closed and transferred to an archive site. Range: 5 through 2880 minutes  
Default: 30 minutes  
7. In the Start Time box, enter the start time for transfer of an accounting-data log file in the format yyyy-mm-dd.hh:mm |

Configure archive sites. | 1. Click Add new entry next to Archive Sites.  
2. In the Name box, enter the site name.  
3. In the Comment box, enter the comment.  
4. In the Password box, enter the password. |

Configuring the Filter Profile (NSM Procedure)

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

To configure the filter profile in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.  
2. Click the Device Tree tab, and then double-click the device to select it.  
3. Click the Configuration tab. In the configuration tree, expand Accounting Options.  
4. Select Filter Profile.  
5. Add or modify the settings as specified in Table 32 on page 74.  
6. Click one:  
   - OK—Saves the changes.  
   - Cancel— Cancels the modifications.
### Table 32: Filter Profile Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure a filter profile. | 1. Click **Add new entry** next to Filter Profile.  
2. Expand **filter-profile**.  
3. In the **Name** box, enter the filename.  
4. In the **Comment** box, enter the comment for the file.  
5. In the **File** box, enter the name of the file.  
6. From the **Interval** list, select the amount of time between each collection of statistics.  
   Range: 1 through 1048576 minutes  
   Default: 30 minutes |

| Configure the counters. | 1. Click **Counters** next to filter-profile.  
2. Click **Add new entry** next to Counters.  
3. In the **Name** box, enter the site name.  
4. In the **Comment** box, enter the comment. |

### Configuring the Interface Profile (NSM Procedure)

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

To configure the interface profile in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Accounting Options**.
4. Select **Interface Profile**.
5. Add or modify the settings as specified in Table 33 on page 75.
6. Click one:  
   - OK—Saves the changes.  
   - Cancel—Cancels the modifications.
Table 33: Interface Profile Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure an interface profile. | 1. Click **Add new entry** next to Interface Profile.  
2. Expand **interface-profile**.  
3. In the **Name** box, enter the name of the log file.  
4. In the **Comment** box, enter the comment for the interface profile.  
5. In the **File** box, enter the name of the log file.  
6. From the **Interval** list, select the amount of time between each collection of statistics.  
   Range: 1 through 2880 minutes  
   Default: 30 minutes |

Configure the statistics to be collected in an accounting-data log file for an interface. | 1. Click **Fields** next to interface-profile.  
2. In the **Comment** box, enter the comment.  
3. Select the corresponding field name:  
   • **Input Bytes**—Input bytes  
   • **Output Bytes**—Output bytes  
   • **Input Packets**—Input packets  
   • **Output Packets**—Output packets  
   • **Input Errors**—Generic input error packets  
   • **Output Errors**—Generic output error packets  
   • **Input Multicast**—Input packets arriving by multicast  
   • **Output Multicast**—Output packets sent by multicast  
   • **Input Unicast**—Input unicast packets  
   • **Output Unicast**—Output unicast packets  
   • **Unsupported Protocol**—Log Packets of unsupported protocols  
   • **Rpf Check Bytes**—Number of bytes that have failed the RPF check  
   • **Rpf Check Packets**—Number of packets that have failed the RPF check  
   • **Rpf Check6 Bytes**—Log number of bytes that have failed the IPv6 reverse-path-forwarding check  
   • **Rpf Check6 Packets**—Log number of packets that have failed the IPv6 reverse-path-forwarding check |

**Configuring the Policy Decision Statistics Profile (NSM Procedure)**

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

To configure the policy decision statistics profile in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Accounting Options.
5. Add or modify the settings as specified in Table 34 on page 76.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 34: Policy Decision Statistics Profile Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure policy decision statistics profile | 1. Click Add new entry next to Policy Decision Statistics Profile.  
|                                          | 2. Expand policy-decision-statistics-profile.  
|                                          | 3. In the Name box, enter the name of the policy decision statistics profile.  
|                                          | 4. In the Comment box, enter the comment for the policy decision statistics profile.  
|                                          | 5. In the File box, enter the name of the log file.  |
| Configure application awareness access list | 1. Click Application Awareness Access List next to policy-decision-statistics-profile.  
|                                          | 2. Select the name of the field:  
|                                          | • address—Address of subscriber  
|                                          | • application—Application  
|                                          | • application-group—Application group  
|                                          | • input-bytes—Input bytes  
|                                          | • input-interface—Interface of subscriber  
|                                          | • input-packets—Input packets  
|                                          | • mask—Mask of subscriber  
|                                          | • output-bytes—Output bytes  
|                                          | • output-packets—Output packets  
|                                          | • subscriber-name—Name of subscriber  
|                                          | • timestamp—Timestamp of statistics record  
|                                          | • vrf-name—VRF where subscriber resides  |

Configuring the MIB Profile (NSM Procedure)

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

To configure the MIB profile in NSM:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Accounting Options.
4. Select MIB Profile.
5. Add or modify the settings as specified in Table 35 on page 77.

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

Table 35: MIB Profile Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure mib profile.</td>
<td>1. Click Add new entry next to Mib Profile.</td>
</tr>
<tr>
<td></td>
<td>2. Expand mib-profile.</td>
</tr>
<tr>
<td></td>
<td>3. In the Name box, enter the name of the MIB statistics profile.</td>
</tr>
<tr>
<td></td>
<td>4. In the Comment box, enter the comment for the MIB profile.</td>
</tr>
<tr>
<td></td>
<td>5. In the File box, enter the name of the log file.</td>
</tr>
<tr>
<td></td>
<td>6. From the Interval list, select the amount of time between each collection of statistics.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 2880 minutes</td>
</tr>
<tr>
<td></td>
<td>Default: 30 minutes</td>
</tr>
<tr>
<td></td>
<td>7. From the Operation list, select the name of the operation to use. You can select a get, get-next, or walk operation.</td>
</tr>
<tr>
<td></td>
<td>Default: walk</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configure the name of the MIB objects for which MIB statistics are collected for an accounting-data log file.</th>
<th>1. Click Object Names next to mib-profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. In the Name box, enter the name of a MIB object. You can specify more than one MIB object name.</td>
</tr>
<tr>
<td></td>
<td>3. In the Comment box, enter the comment.</td>
</tr>
</tbody>
</table>

Configuring the Routing Engine Profile (NSM Procedure)

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

To configure the Routing Engine profile in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Accounting Options.
4. Select Routing Engine Profile.
5. Add or modify the settings as specified in Table 36 on page 78.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.
### Table 36: Routing Engine Profile Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| **Configure Routing Engine profile.** | 1. Click Add new entry next to Routing Engine Profile.  
2. Expand routing-engine-profile.  
3. In the Name box, enter the name of the Routing Engine statistics profile.  
4. In the Comment box, enter the comment for the routing engine profile.  
5. In the File box, enter the name of the log file.  
6. From the Interval list, select the amount of time between each collection of statistics.  
   Range: 1 through 2880 minutes  
   Default: 30 minutes |

| **Configure the statistics to collect in an accounting-data log file for a Routing Engine.** | 1. Click Fields next to routing-engine-profile.  
2. In the Comment box, enter the comment.  
3. Select the name of the field:  
   • host-name—Hostname for the router.  
   • date—Date, in yyyyMMdd format.  
   • time-of-day—Time of day, in hhmmss format.  
   • uptime—Time since last reboot, in seconds.  
   • cpu-load-1—Average system load over the last 1 minute.  
   • cpu-load-5—Average system load over the last 5 minutes.  
   • cpu-load-15—Average system load over the last 15 minutes.  
   • Memory Usage—Memory usage in bytes.  
   • Total Cpu Usage—Amount of CPU time used. |
CHAPTER 9

Configuring Applications

- Configuring the Application and Application Set (NSM Procedure) on page 79

Configuring the Application and Application Set (NSM Procedure)

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

To configure an application set in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Applications.
4. Add or modify settings as specified in Table 37 on page 80.
5. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

NOTE: Application and application set are configurable, only if the device is in the in-device policy mode.
Table 37: Applications Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure properties of an application and whether to include it in an application set. | 1. Click **Application** next to Applications.  
2. Click **Add new entry** next to Application.  
3. In the **Name** box, enter the identifier of the application.  
4. In the **Comment** box, enter the comment.  
5. From the **Application Protocol** list, select the name of the protocol.  
6. From the **Protocol** list, select the networking protocol type.  
7. From the **Source Port** list, select the identifier for the port.  
8. From the **Destination Port** list, select the Identifier for the port.  
9. From the **Snmp Command** list, select the SNMP command format.  
10. From the **Icmp Type** list, select the ICMP packet type value.  
11. From the **Icmp Code** list, select the Internet Control Message Protocol (ICMP) code value.  
12. From the **Ttl Threshold** list, select the TTL threshold value.  
13. In the **Rpc Program number** box, enter the Remote procedure call (RPC) or Distributed Computing Environment (DCE) value.  
   Range: 100,000 through 400,000  
14. In the **Uuid** box, enter the Universal Unique Identifier (UUID) for DCE RPC objects.  
15. From the **Inactivity Timeout** list, select the length of time the application is inactive before it times out.  
16. Select the **Learn Sip Register** check box to activate SIP register to accept potential incoming SIP calls.  
17. From the **Sip Call Hold Timeout** list select the length of time the application holds a SIP call open before it times out.  
   Default: 7200 seconds  
   Range: 0 through 36,000 seconds (10 hours)  
18. Select one of the following:  
   - **do-not-translate-AAAA-query-to-A-query**—To control the translation of AAAA query to A query.  
   - **do-not-translate-A-query-to-AAAA**—To control the translation of A query to AAAA query. |

Configuring application sets. | 1. Click **Application Set** next to Applications.  
2. Click **Add new entry** next to Application Set.  
3. Expand **application-set**.  
4. In the **Name** box, enter the identifier of an application set.  
5. In the **Comment** box, enter the comment.  
6. Click **Application** next to application-set.  
7. Click **Add new entry** next to Application.  
8. From the **Name** list, select the identifier of the application.  
9. In the **Comment** box, enter the comment.
CHAPTER 10

Configuring Bridge Domains

- Configuring Bridge Domains Properties (NSM Procedure) on page 81

Configuring Bridge Domains Properties (NSM Procedure)

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

- Configuring a Bridge Domain (NSM Procedure) on page 81
- Configuring Layer 2 Learning and Forwarding Properties for a Bridge Domain (NSM Procedure) on page 82
- Configuring Forwarding Options (NSM Procedure) on page 84
- Configuring Logical Interfaces (NSM Procedure) on page 85
- Configuring Multicast Snooping Options (NSM Procedure) on page 86
- Configuring IGMP Snooping (NSM Procedure) on page 89
- Configuring VLAN ID (NSM Procedure) on page 94

Configuring a Bridge Domain (NSM Procedure)

A bridge domain must include a set of logical interfaces that participate in Layer 2 learning and forwarding. You can optionally configure a VLAN identifier and a routing interface for the bridge domain to also support Layer 3 IP routing.

To configure bridge domain in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Bridge Domains.
4. Select Domain.
5. Add or modify settings as specified in Table 38 on page 82.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.
Table 38: Bridge Domain Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure bridge domain.</td>
<td>1. Click <strong>Add new entry</strong> next to Domain.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>domain</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the name of the bridge domain.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Description</strong> box, enter the text to describe the bridge domain.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Domain Type</strong> list, select the type of domain for a Layer 2 bridge domain.</td>
</tr>
<tr>
<td></td>
<td>7. Select the <strong>No Local Switching</strong> check box to enable or disable local switching within customer edge(ce)-facing interfaces.</td>
</tr>
<tr>
<td></td>
<td>8. In the <strong>Routing Interface</strong> box, enter the interface name.</td>
</tr>
</tbody>
</table>

Configuring Layer 2 Learning and Forwarding Properties for a Bridge Domain (NSM Procedure)

When you configure a bridge domain, Layer 2 address learning is enabled by default. The bridge domain learns unicast media access control (MAC) addresses to avoid flooding the packets to all the ports in the bridge domain. Each bridge domain creates a source MAC entry in its source and destination MAC tables for each source MAC address learned from packets received on the ports that belong to the bridge domain.

To configure bridge options in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Bridge Domains**.
4. Select **Domain**.
5. Add or modify settings as specified in Table 39 on page 83.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.
### Table 39: Bridge Options Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure bridge domain.</strong></td>
<td>1. Click <strong>Add new entry</strong> next to Domain.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Bridge Options</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Expand <strong>Bridge Options</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Mac Table Aging Time</strong> list, select the timeout interval for entries in the MAC table.</td>
</tr>
<tr>
<td></td>
<td>6. Select the <strong>No Mac Learning</strong> check box to disable MAC learning.</td>
</tr>
<tr>
<td></td>
<td>7. Select the <strong>Mac Statistics</strong> check box to enable MAC accounting either for a specific bridge domain, or for a set of bridge domains associated with a Layer 2 trunk port.</td>
</tr>
<tr>
<td></td>
<td>8. In the <strong>Routing Interface</strong> box, enter the interface name.</td>
</tr>
<tr>
<td><strong>Specify the logical interfaces to include in the bridge domain.</strong></td>
<td>1. Click <strong>Interface</strong> next to Bridge Options.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Interface.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the interface name.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. From the <strong>Remote Site Id</strong> list, select the remote site ID.</td>
</tr>
<tr>
<td></td>
<td>6. Select the <strong>No Mac Learning</strong> check box to disable MAC learning.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Description</strong> box, enter the description.</td>
</tr>
<tr>
<td></td>
<td>8. Click <strong>Interface Mac Limit</strong> next to interface.</td>
</tr>
<tr>
<td></td>
<td>9. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>10. From the <strong>Limit</strong> list, select the maximum number of MAC addresses learned from an interface. Range: 1 through 131,071 MAC addresses per interface</td>
</tr>
<tr>
<td></td>
<td>11. From the <strong>Packet Action</strong> list, select the packet action for the packets for new source MAC addresses.</td>
</tr>
<tr>
<td></td>
<td>12. Click <strong>Static Mac</strong> next to interface.</td>
</tr>
<tr>
<td></td>
<td>13. Click <strong>Add new entry</strong> next to Static Mac.</td>
</tr>
<tr>
<td></td>
<td>14. In the <strong>Name</strong> box, enter the interface name.</td>
</tr>
<tr>
<td></td>
<td>15. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>16. Click <strong>Vlan Id</strong> next to static-mac.</td>
</tr>
<tr>
<td></td>
<td>17. Click <strong>Add new entry</strong> next to Vlan Id.</td>
</tr>
<tr>
<td></td>
<td>18. From the <strong>Name</strong> list, select the VLAN identifier to associate with the static MAC address. Range: 1 to 4094</td>
</tr>
<tr>
<td></td>
<td>19. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td><strong>Configure a limit to the number of MAC addresses that can be learned from a bridge domain, virtual switch, or set of bridge domains.</strong></td>
<td>1. Click <strong>Interface Mac Limit</strong> next to Bridge Options.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. From the <strong>Limit</strong> list, select the maximum number of MAC addresses learned from an interface. Range: 1 through 131,071 MAC addresses per interface</td>
</tr>
</tbody>
</table>

---

Copyright © 2010, Juniper Networks, Inc.
Table 39: Bridge Options Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Modify the size of the MAC address table for the bridge domain, a set of bridge domains associated with a trunk port, or a virtual switch. | 1. Click Mac Table Size next to Bridge Options.  
2. In the Comment box, enter the comment.  
3. From the Limit list, select the maximum number of addresses in the MAC address table.  
Range: 16 through 1,048,575 MAC addresses  
Default: 5120 MAC addresses |

Configuring Forwarding Options (NSM Procedure)

To configure forwarding options in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Bridge Domains.
4. Select Domain.
5. Add or modify settings as specified in Table 40 on page 84.
6. Click one:  
   - OK—Saves the changes.  
   - Cancel—Cancels the modifications.

Table 40: Forwarding Options Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configuring the extended DHCP relay agent. | 1. Click Add new entry next to Domain.  
2. Click Forwarding Options.  
3. Expand Dhcp Relay.  
4. Select Authentication.  
5. For Configuring Authentication Support for the DHCP Relay Agent, see “Configuring Authentication Support for the DHCP Relay Agent (NSM Procedure)” on page 185. |
| Configuring Group.                        | 1. Click Group next to Dhcp Relay.  
2. For configuring group, see “Configuring Group (NSM Procedure)” on page 186. |
| Overriding the default configuration settings for the extended DHCP relay agent. | 1. Click Overrides next to Dhcp Relay.  
2. For overriding the default configuration settings for the extended DHCP relay agent, see “Overriding the Default Configuration Settings for the Extended DHCP Relay Agent (NSM Procedure)” on page 187. |
Table 40: Forwarding Options Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring relay option 60 information for forwarding client traffic to specific DHCP servers.</td>
<td>1. Click <strong>Relay option 60</strong> next to Dhcp Relay.</td>
</tr>
<tr>
<td></td>
<td>2. For configuring relay option 60 information for forwarding client traffic to specific DHCP servers, see “Configuring Relay Option 60 Information for Forwarding Client Traffic to Specific DHCP Servers (NSM Procedure)” on page 189.</td>
</tr>
<tr>
<td>Configuring relay option 82 for a DHCP server.</td>
<td>1. Click <strong>Relay option 82</strong> next to Dhcp Relay.</td>
</tr>
<tr>
<td></td>
<td>2. For configuring relay option 82 for a DHCP server, see “Configuring Relay Option 82 for a DHCP Server (NSM Procedure)” on page 190.</td>
</tr>
<tr>
<td>Specifying the name of a group of DHCP server addresses for use by the extended DHCP relay agent.</td>
<td>1. Click <strong>Server Group</strong> next to Dhcp Relay.</td>
</tr>
<tr>
<td></td>
<td>2. For specifying the name of a group of DHCP server addresses for use by the extended DHCP relay agent, see “Specifying the Name of a Group of DHCP Server Addresses for Use by the Extended DHCP Relay Agent (NSM Procedure)” on page 191</td>
</tr>
<tr>
<td>Configuring tracing operations for extended DHCP relay agent processes.</td>
<td>1. Click <strong>Traceoptions</strong> next to Dhcp Relay.</td>
</tr>
<tr>
<td></td>
<td>2. For configuring tracing operations for extended DHCP relay agent processes see “Configuring Operations for Extended DHCP Relay Agent Processes (NSM Procedure)” on page 192</td>
</tr>
<tr>
<td>Apply a forwarding table filter at the ingress of a forwarding table.</td>
<td>1. Click <strong>Filter</strong> next to Forwarding Options.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. From the <strong>Input</strong> list, select the name of the applied filter.</td>
</tr>
<tr>
<td>Apply a forwarding table filter to a flood table.</td>
<td>1. Click <strong>Flood</strong> next to Forwarding Options.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. From the <strong>Input</strong> list, select the name of the forwarding table filter.</td>
</tr>
</tbody>
</table>

Configuring Logical Interfaces (NSM Procedure)

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

To configure logical interfaces in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Bridge Domains**.
4. Select **Domain**.
5. Add or modify settings as specified in Table 41 on page 86.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.
### Table 41: Logical Interface Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure logical interface to include in the bridge domain, VPLS instance, or virtual switch.</td>
<td>1. Click <strong>Add new entry</strong> next to Domain.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Interface</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add new entry</strong> next to Interface.</td>
</tr>
<tr>
<td></td>
<td>4. From the <strong>Name</strong> list, select the name of a logical interface.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
</tbody>
</table>

---

**Configuring Multicast Snooping Options (NSM Procedure)**

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

To configure Multicast Snooping:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Bridge Domains**.
4. Select **Domain**.
5. Add or modify the settings as specified in Table 42 on page 87.
6. Click one:
   - **OK**—saves the changes
   - **Cancel**—cancels the modifications
### Table 42: Multicast Snooping Options Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish multicast snooping option values.</td>
<td>1. Click <a href="#">Add new entry</a> next to Domain.</td>
</tr>
<tr>
<td></td>
<td>2. Click <a href="#">Multicast Snooping Options</a> next to Domain.</td>
</tr>
<tr>
<td>Establish a list of flood group addresses for</td>
<td>1. Click <a href="#">Flood Groups</a> next to Multicast Snooping Options.</td>
</tr>
<tr>
<td>multicast snooping.</td>
<td>2. Click <a href="#">Add new entry</a> next to Flood Groups.</td>
</tr>
<tr>
<td></td>
<td>3. In the dialog box, enter the IP addresses.</td>
</tr>
<tr>
<td>Configure multicast forwarding cache properties.</td>
<td>1. Click <a href="#">Forwarding Cache</a> next to Multicast Snooping Options.</td>
</tr>
<tr>
<td></td>
<td>2. In the <a href="#">Comment</a> box, enter the comments.</td>
</tr>
<tr>
<td></td>
<td>3. Expand <a href="#">Forwarding Cache</a>.</td>
</tr>
<tr>
<td></td>
<td>4. Click <a href="#">Threshold</a> next to Forwarding Cache.</td>
</tr>
<tr>
<td></td>
<td>5. In the <a href="#">Comment</a> box, enter the comments.</td>
</tr>
<tr>
<td></td>
<td>6. From the <a href="#">Suppress</a> list, select the threshold value for a forwarding cache.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 200,000</td>
</tr>
<tr>
<td></td>
<td>7. From the <a href="#">Reuse</a> list, select the reuse value for the threshold.</td>
</tr>
<tr>
<td></td>
<td>The reuse value must be less than the suppression threshold value.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 200,000</td>
</tr>
<tr>
<td>Establish the graceful restart duration for</td>
<td>1. Click <a href="#">Graceful Restart</a> next to Multicast Snooping Options.</td>
</tr>
<tr>
<td>multicast snooping.</td>
<td>2. In the <a href="#">Comment</a> box, enter the comments.</td>
</tr>
<tr>
<td></td>
<td>3. From the <a href="#">Restart Duration</a> list, select the duration for graceful restart.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 to 300 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 180 seconds</td>
</tr>
</tbody>
</table>
### Table 42: Multicast Snooping Options Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Establish multicast snooping option values. | 1. Click **Option** next to Multicast Snooping Options.  
2. In the **Comment** box, enter the comments.  
3. Expand **Options**.  
4. Click **Syslog** next to Options.  
5. In the **Comment** box, enter the comments.  
6. From the **Upto** list, select the level up to which severity the messages are to be syslogged.  
7. From the **Mark** list, select the time interval in seconds to mark the trace file.  
   Range : -2147483647 seconds to 2147483647 Seconds  
   Default : 0  
8. Expand **Syslog**.  
9. Click **Level** next to Syslog.  
10. Select the Level of severity to be logged. |
| Configure tracing options. | 1. Click **Traceoptions** next to Multicast Snooping Options.  
2. In the **Comment** box, enter the comments.  
3. Expand **Traceoptions**.  
4. Click **File** next to Trace Options.  
5. In the **Comment** box, enter the comments.  
6. In the **Filename** box, enter the name of the file to receive the output of the tracing operation. Enclose the name within quotation marks.  
7. In the **Size** box, enter the maximum size of each trace file in bytes.  
   Range : 10240 to 4294967295 bytes  
8. From the **Files** list, select the maximum number of files.  
9. Select one of the following:  
   - *world-readable*—To enable log file access to all users.  
   - *no-world-readable*—To prevent all users from reading the log file.  
10. Click **Flag** next to Trace Options.  
11. Click Add new entry next to flag.  
12. From the **Name** list, select a tracing operation to perform.  
13. In the **Comment** box, enter the comments. |
Configuring IGMP Snooping (NSM Procedure)

The Internet Group Management Protocol (IGMP) manages the membership of hosts and routers in multicast groups. IP hosts use IGMP to report their multicast group memberships to any immediately neighboring multicast routers. Multicast routers use IGMP to learn, for each of their attached physical networks, which groups have members. IGMP is also used as the transport for several related multicast protocols (for example, Distance Vector Multicast Routing Protocol [DVMRP] and Protocol Independent Multicast version 1 [PIMv1]). IGMP is an integral part of IP and must be enabled on all routers and hosts that need to receive IP multicast traffic.

To configure IGMP snooping in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Bridge Domains.
4. Select Domain.
5. Add or modify settings as specified in Table 43 on page 90.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.
Configure IGMP snooping.

1. Click **Add new entry** next to Domain.
2. Click and expand Protocol.
3. Select **Igmp Snooping**.
4. In the **Comment** box, enter the comment.
5. From the **Query Interval** list, select the time interval the querier router sends general host-query messages.
   Range: 1 through 1024
   Default: 125 seconds
6. In the **Query Response Interval** box, enter the time interval the querier router waits to receive a response to a host-query message from a host. This interval must be less than the interval between general host-query messages.
   Range: 1 through 1024
   Default: 10 seconds
7. In the **Query Last Member Interval** box, enter the time interval the querier router sends group-specific query messages.
   Range: 0.1 through 0.9, then in 1-second intervals 1 through 1024
   Default: 1 second
8. From the **Robust Count** list, select the robustness variable used to calculate several IGMP message intervals.
   Range: 2 through 10
   Default: 2
9. Select the **Immediate Leave** check box to enable immediate leave.

   When this statement is enabled on a router running IGMP version 2 (IGMPv2), after the router receives a leave group membership message from a host associated with the interface, the router immediately removes the group membership from the interface and suppresses the sending of any group-specific queries for the multicast group.

   When this statement is enabled on a router running IGMP version 3 (IGMPv3), after the router receives a report with the type BLOCK_OLD_SOURCES, the router suppresses the sending of group-and-source queries but relies on the host-tracking mechanism supported by the JUNOS Software to determine whether or not it removes a particular source group membership from the interface.

**NOTE:** When issuing this command on IGMPv2 interfaces, ensure that the IGMP interface has only one IGMP host connected. If more than one IGMPv2 host is connected to a LAN through the same interface, and one host sends a done message, the router removes all hosts on the interface from the multicast group. The router loses contact with the hosts that properly remain in the multicast group until they send join requests in response to the next general multicast listener query from the router.
### Table 43: Igmp Snooping Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| **Enable IGMP on an interface and configure interface-specific properties.** | 1. Click **Interface** next to Igmp Snooping.  
2. Click **Add new entry** next to Interface.  
3. In the **Name** box, enter the interface name.  
4. In the **Comment** box, enter the comment.  
5. Select the **Multicast Router Interface** check box if the interface is a multicast router interface.  
6. Select the **Immediate Leave** check box to enable immediate leave on a router.  
7. Select the **Host Only Interface** check box if the interface is to be configured as a host-facing interface.  
8. From the **Group Limit** list, select the limit for the number of multicast groups (or [S,G] channels in IGMPv3) allowed on an interface.  
   After this limit is reached, new reports will be ignored and all related flows are not flooded on the interface.  
9. Click **Static** next to Interface.  
10. In the **Comment** box, enter the comment.  
11. Expand **Static**.  
12. Click **Group** next to Static.  
13. Click **Add new entry** next to Group.  
14. In the **Name** box, enter the IGMP multicast group address.  
15. In the **Comment** box, enter the comment.  
16. Click **Source** next to group.  
17. Click **Add new entry** next to Source.  
18. In the **Name** box, enter the IP version 4 (IPv4) unicast source address for the multicast group being statically configured on an interface.  
19. In the **Comment** box, enter the comment. |

**Configuring IGMP snooping proxy mode.** | 1. Click **Proxy** next to Igmp Snooping.  
2. In the **Comment** box, enter the comment.  
3. In the **Source Address** box, enter the IP address to use as the source for IGMP snooping reports in proxy mode. |
Configure IGMP tracing options.

1. In the **Comment** box, enter the comment for the trace options.
2. Click **File** next to Trace options.
3. In the **Comment** box, enter the comment for the filename.
4. In the **Filename** box, enter the name of the file to receive the output of the tracing operation.
5. In the **Size** box, enter the maximum trace file size in bytes.
   Range: 10240 to 4294967295
6. From the **Files** list, select the maximum number of trace files.
   Range: 2 through 1000 files
   Default: 2 files
7. Select one of the following:
   - **no-world-readable**—To restrict the file access to owner.
   - **world-readable**—To enable unrestricted access.
8. Click **Flag** next to Trace options.
9. Click **Add new entry** next to Flag.
10. From the **Name** list, select the flag to perform the trace operation.
11. In the **Comment** box, enter the comment for the flag.
12. Select the corresponding flag modifier check box.

### Table 43: Igmp Snooping Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure IGMP tracing options. | 1. In the **Comment** box, enter the comment for the trace options.  
2. Click **File** next to Trace options.  
3. In the **Comment** box, enter the comment for the filename.  
4. In the **Filename** box, enter the name of the file to receive the output of the tracing operation.  
5. In the **Size** box, enter the maximum trace file size in bytes.  
   Range: 10240 to 4294967295  
6. From the **Files** list, select the maximum number of trace files.  
   Range: 2 through 1000 files  
   Default: 2 files  
7. Select one of the following:  
   - **no-world-readable**—To restrict the file access to owner.  
   - **world-readable**—To enable unrestricted access.  
8. Click **Flag** next to Trace options.  
9. Click **Add new entry** next to Flag.  
10. From the **Name** list, select the flag to perform the trace operation.  
11. In the **Comment** box, enter the comment for the flag.  
12. Select the corresponding flag modifier check box. |
Table 43: Igmp Snooping Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure IGMP snooping parameters for a particular VLAN. | 1. From the Name list, select the VLAN ID.  
2. In the Comment box, enter the comment.  
3. From the Query Interval list, select the time interval the querier router sends general host-query messages.  
   Range: 1 through 1024  
   Default: 125 seconds  
4. In the Query Response Interval box, enter the time interval the querier router waits to receive a response to a host-query message from a host. This interval must be less than the interval between general host-query messages.  
   Range: 1 through 1024  
   Default: 10 seconds  
5. In the Query Last Member Interval box, enter the time interval the querier router sends group-specific query messages.  
   Range: 0.1 through 0.9, then in 1-second intervals 1 through 1024  
   Default: 1 second  
6. From the Robust Count list, select the robustness variable used to calculate several IGMP message intervals.  
   Range: 2 through 10  
   Default: 2  
7. Select the Immediate Leave check box to enable immediate leave.  
   When this statement is enabled on a router running IGMP version 2 (IGMPv2), after the router receives a leave group membership message from a host associated with the interface, the router immediately removes the group membership from the interface and suppresses the sending of any group-specific queries for the multicast group.  
   When this statement is enabled on a router running IGMP version 3 (IGMPv3), after the router receives a report with the type BLOCK_OLD_SOURCES, the router suppresses the sending of group-and-source queries but relies on the host-tracking mechanism supported by the JUNOS Software to determine whether or not it removes a particular source group membership from the interface.  

NOTE: When issuing this command on IGMPv2 interfaces, ensure that the IGMP interface has only one IGMP host connected. If more than one IGMPv2 host is connected to a LAN through the same interface, and one host sends a done message, the router removes all hosts on the interface from the multicast group. The router loses contact with the hosts that properly remain in the multicast group until they send join requests in response to the next general multicast listener query from the router.
### Table 43: Igmp Snooping Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure interface specific properties. | 1. Click Interface next to vlan.  
2. Click Add new entry next to interface.  
3. In the Name box, enter the interface name.  
4. In the Comment box, enter the comment.  
5. Select the Multicast Router Interface check box if the interface is a multicast router interface.  
6. Select the Immediate Leave check box to enable immediate group leave on a router.  
7. Select the Host Only Interface check box if the interface is to be configured as a host-facing interface.  
8. From the Group Limit list, select the limit for the number of multicast groups (or [S,G] channels in IGMPv3) allowed on an interface. After this limit is reached, new reports will be ignored and all related flows are not flooded on the interface.  
9. Click Static next to interface.  
10. In the Comment box, enter the comment.  
11. Expand Static.  
12. Click Group next to Static.  
13. Click Add new entry next to Group.  
14. In the Name box, enter the IGMP multicast group address.  
15. In the Comment box, enter the comment.  
16. Click Source next to group.  
17. Click Add new entry next to Source.  
18. In the Name box, enter the IP version 4 (IPv4) unicast source address for the multicast group being statically configured on an interface.  
19. In the Comment box, enter the comment.  
20. Click Proxy next to vlan.  
21. In the Comment box, enter the comment.  
22. In the Source Address box, enter the IP address to use as the source for IGMP snooping reports in proxy mode. |

### Configuring VLAN ID (NSM Procedure)

You can configure VLAN IDs using the Vlan Id option.

To configure VLAN ID in NSM:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Bridge Domains.
4. Select Domain.
5. Add or modify settings as specified in Table 44 on page 95.
6. Click one:
- OK—Saves the changes.
- Cancel— Cancels the modifications.

### Table 44: VLAN ID Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a VLAN ID</td>
<td>1. Click Add new entry next to Domain.</td>
</tr>
<tr>
<td></td>
<td>2. Click Vlan Id.</td>
</tr>
<tr>
<td></td>
<td>3. Select vlan-id and enter the VLAN ID.</td>
</tr>
<tr>
<td></td>
<td>4. Select vlan tag to tag the VLAN interface so that it can be compared with the normalizing VLAN identifier.</td>
</tr>
<tr>
<td></td>
<td>5. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. In the Inner box, enter the VLAN identifier.</td>
</tr>
<tr>
<td></td>
<td>7. In the Outer box, enter the VLAN identifier.</td>
</tr>
</tbody>
</table>
Configuring Chassis

- Configuring Aggregated Devices (NSM Procedure) on page 97
- Configuring Chassis Alarms (NSM Procedure) on page 98
- Configuring Container Interfaces (NSM Procedure) on page 99
- Configuring Chassis FPC (NSM Procedure) on page 100
- Configuring a T640 Router on a Routing Matrix (NSM Procedure) on page 105
- Configuring Routing Engine Redundancy (NSM Procedure) on page 110
- Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors (NSM Procedure) on page 111

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 45 on page 98.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
Table 45: Aggregated Devices Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure properties for Ethernet aggregated devices. | 1. Click Ethernet next to Aggregated Devices.  
2. Enter the number of aggregated logical devices available to the router.  
Range: 1 through 256 devices  
3. Click Lacp next to Ethernet.  
4. In the SystemPriority box, enter the priority for the aggregated Ethernet system.  
5. Click Link Protection next to Lacp.  
6. Select the NonRevertive check box if you want to disable the ability to switch to a better priority link (if one is available) once a link is established as active and a collection or distribution is enabled. |
| Configure properties for sonet aggregated devices. | 1. Click Sonet next to Aggregated Devices.  
2. From the DeviceCount 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 98
- Configuring a T640 Router on a Routing Matrix (NSM Procedure) on page 105
- Configuring Routing Engine Redundancy (NSM Procedure) on page 110
- Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors (NSM Procedure) on page 111

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 46 on page 99.
5. Click one:  
   - OK—Saves the changes.  
   - Cancel—Cancels the modifications.
### Table 46: 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 97
- Configuring Chassis FPC (NSM Procedure) on page 100
- Configuring Routing Engine Redundancy (NSM Procedure) on page 110

### Configuring Container Interfaces (NSM Procedure)

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

To configure container interfaces in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Chassis**.
4. Select **Container Devices**.
5. Add or modify settings as specified in Table 47 on page 99.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

### Table 47: Container Interfaces Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the container devices configuration.</td>
<td>1. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>2. From the <strong>Device</strong> list, select the number of container devices. Range: 1 through 128</td>
</tr>
</tbody>
</table>

### Related Topics
- Configuring Aggregated Devices (NSM Procedure) on page 97
- Configuring Chassis FPC (NSM Procedure) on page 100
Configuring Chassis FPC (NSM Procedure)

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

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

To configure chassis FPC in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Chassis > Fpc.
4. Add or modify settings as specified in Table 48 on page 100.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 48: FPC Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure a port-mirroring instance for the DPC and its corresponding Packet Forwarding Engines. | 1. Click Add new entry next to Fpc.  
2. From the Name list, select the slot number of the DPC.  
3. From the Power list, configure the Flexible PIC Concentrator (FPC) to stay offline or to come online automatically. |
### Table 48: FPC Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure aggregate port, maximum queues per interface and port mirroring instances for the PICs.</td>
<td>1. Click <strong>Add new entry</strong> next to Fpc.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Pic</strong> next to fpc.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add new entry</strong> next to Pic.</td>
</tr>
<tr>
<td></td>
<td>4. From the <strong>Name</strong> list, select the slot number of the DPC.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Framing</strong> list, select the framing type.</td>
</tr>
<tr>
<td></td>
<td>7. From the <strong>Vtmapping</strong> list, select one of the virtual tributary mapping.</td>
</tr>
<tr>
<td></td>
<td>• klm—KLM standard.</td>
</tr>
<tr>
<td></td>
<td>• itu-t—International Telephony Union standard.</td>
</tr>
<tr>
<td></td>
<td>8. Select the <strong>No Concatenate</strong> check box to not concatenate (multiplex) the output of a SONET/SDH PIC (an interface with a name so-fpc/pic/port).</td>
</tr>
<tr>
<td></td>
<td>9. Select the <strong>Aggregate Ports</strong> check box if you want to aggregate multiple ports on a PIC as a single port.</td>
</tr>
<tr>
<td></td>
<td>10. Select the <strong>Sparse Dics</strong> check box to support a full data-link connection identifier (DLCI) range (1 through 1022).</td>
</tr>
<tr>
<td></td>
<td>11. From the <strong>Mlfr Uni Nni Bundles</strong> list, select the number of multilink frame relay user-to-network interface network-to-network interface (UNI-NNI) (FRF.16) bundles to allocate on a link services PIC.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 255</td>
</tr>
<tr>
<td></td>
<td>12. From the <strong>Max Queues Per Interface</strong> list, select the required egress queues on IQ interfaces.</td>
</tr>
<tr>
<td>Enable a service package on adaptive services interfaces.</td>
<td>1. Click <strong>Add new entry</strong> next to Fpc.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Pic</strong> next to fpc.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add new entry</strong> next to Pic.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Adaptive Services</strong> next to pic.</td>
</tr>
<tr>
<td></td>
<td>5. Select <strong>Adaptive Services</strong> to enable a service package on adaptive services interfaces.</td>
</tr>
<tr>
<td>Configure channelized E1 port and channel specifications.</td>
<td>1. Click <strong>Add new entry</strong> next to Fpc.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Pic</strong> next to fpc.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add new entry</strong> next to Pic.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Ce1</strong> next to pic.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. Click <strong>E1</strong> next to Ce1.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>Add new entry</strong> next to E1.</td>
</tr>
<tr>
<td></td>
<td>8. From the <strong>Name</strong> list, select the port number.</td>
</tr>
<tr>
<td></td>
<td>9. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>10. Click <strong>Channel Group</strong> next to e1.</td>
</tr>
<tr>
<td></td>
<td>11. Click <strong>Add new entry</strong> next to Channel Group.</td>
</tr>
<tr>
<td></td>
<td>12. From the <strong>Name</strong> list, select the channel number.</td>
</tr>
<tr>
<td></td>
<td>13. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>14. In the <strong>Timeslots</strong> box, enter the actual time slot number.</td>
</tr>
</tbody>
</table>
### Table 48: FPC Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure channelized T3 port and channel specifications.</td>
<td>1. Click <strong>Add new entry</strong> next to Fpc.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Pic</strong> next to fpc.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add new entry</strong> next to Pic.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Ct3</strong> next to pic.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. Click <strong>Port</strong> next to Ct3.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>Add new entry</strong> next to Port.</td>
</tr>
<tr>
<td></td>
<td>8. From the <strong>Name</strong> list, select the port number.</td>
</tr>
<tr>
<td></td>
<td>9. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>10. Click <strong>T1</strong> next to Port.</td>
</tr>
<tr>
<td></td>
<td>11. Click <strong>Add new entry</strong> next to T1.</td>
</tr>
<tr>
<td></td>
<td>12. From the <strong>Name</strong> list, select the link number.</td>
</tr>
<tr>
<td></td>
<td>13. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>14. Click <strong>Channel Group</strong> next to t1.</td>
</tr>
<tr>
<td></td>
<td>15. Click <strong>Add new entry</strong> next to Channel Group.</td>
</tr>
<tr>
<td></td>
<td>16. From the <strong>Name</strong> list, select the channel number.</td>
</tr>
<tr>
<td></td>
<td>17. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>18. In the <strong>Timeslots</strong> box, enter the actual time slot number.</td>
</tr>
</tbody>
</table>

| Configure data used in a hash key for a protocol family.             | 1. Click **Add new entry** next to Fpc.                                      |
|                                                                      | 2. Click **Pic** next to fpc.                                                |
|                                                                      | 3. Click **Add new entry** next to Pic.                                      |
|                                                                      | 4. Click **Hash Key** next to pic.                                           |
|                                                                      | 5. In the **Comment** box, enter the comment.                               |
| Configure data used in a hash key for the **inet** protocol family when configuring PIC-level symmetrical load balancing on an 802.3ad link aggregation group. | 1. Click **Inet** next to Family.                                            |
|                                                                      | 2. In the **Comment** box, enter the comment.                               |
|                                                                      | 3. Click **Layer 3** next to Inet.                                           |
|                                                                      | 4. In the **Comment** box, enter the comment.                               |
|                                                                      | 5. Select the **Destination Address** check box to compute symmetrical hashing based on the destination address. |
|                                                                      | 6. Click **Layer 4** next to Inet.                                           |
|                                                                      | 7. In the **Comment** box, enter the comment.                               |
|                                                                      | 8. Click **Symmetric Hash** next to Inet.                                   |
|                                                                      | 9. In the **Comment** box, enter the comment.                               |
|                                                                      | 10. Select the **Complement** check box to include the complement of the symmetric hash in the hash key. |
Table 48: FPC Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure data used in a hash key for the multiservice protocol family when configuring PIC-level symmetrical hashing for load balancing on an 802.3ad link aggregation group. | 1. Click **Multiservice** next to Family.  
2. In the **Comment** box, enter the comment.  
3. Select the **Source Mac** check box to include source MAC address in the hash key.  
4. Select the **Destination Mac** check box to include destination MAC address in the hash key.  
5. Click **Payload** next to Multiservice.  
6. Click **Ip** next to Payload.  
7. In the **Comment** box, enter the comment.  
8. Select the **Layer 4** check box to include Layer 4 IP information in the hash key.  
9. Click **Layer 3** next to Ip.  
10. Select one of the following:  
    • **source-ip-only**—To include source IP only in hash-key.  
    • **destination-ip-only**—To include destination IP only in hash-key.  
11. Click **Symmetric Hash** next to Multiservice.  
12. In the **Comment** box, enter the comment.  
13. Select the **Complement** check box to include the complement of the symmetric hash in the hash key. |
| Configure the channelized T3 port number on the PIC. | 1. Click **Add new entry** next to Fpc.  
2. Click **Pic** next to fpc.  
3. Click **Add new entry** next to Pic.  
4. Click **Port** next to pic.  
5. From the **Name** list, select the port number.  
6. In the **Comment** box, enter the comment.  
7. From the **Framing** list, select the framing type. |
| Configure delay buffers. | 1. Click **Add new entry** next to Fpc.  
2. Click **Pic** next to fpc.  
3. Click **Add new entry** next to Pic.  
4. Click **Q Pic Large Buffer** next to pic.  
5. In the **Comment** box, enter the comment. |
Table 48: FPC Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure port-mirroring instances. | 1. Click **Add new entry** next to Fpc.  
2. Click **Pic** next to fpc.  
3. Click **Add new entry** next to Pic.  
4. Click **Port Mirror Instance** next to pic and perform the following:  
   • **Add**—Adds the selected port-mirroring instances from the Non member list to the Members list.  
   • **Remove**—Removes the selected port-mirroring instances from the Members list.  
   • **Add All**—Adds all the port-mirroring instances from the Non-members list to the Members list.  
   • **Remove All**—Removes all the port-mirroring instances from the Members list. |
| Enable shaping on an L2TP session. | 1. Click **Add new entry** next to Fpc.  
2. Click **Pic** next to fpc.  
3. Click **Add new entry** next to Pic.  
4. Click **Traffic Manager** next to pic.  
5. From the **Ingress Shaping Overhead** list, select the number of CoS shaping overhead bytes to add to the packets on the ingress side of the L2TP tunnel to determine the shaped session packet length.  
   Range: 0 through 255  
6. From the **Egress Shaping Overhead** list, select the number of CoS shaping overhead bytes to add to the packets on the egress interface.  
   Range: 0 through 255  
7. From the **Mode** list, select the mode of shaping. |
| Configure the amount of bandwidth for tunnel services. | 1. Click **Add new entry** next to Fpc.  
2. Click **Pic** next to fpc.  
3. Click **Add new entry** next to Pic.  
4. Click **Tunnel Service** next to pic.  
5. From the **Bandwidth** list, select the bandwidth of 1 Gbps or 10Gbps on the Packet Forwarding Engine connected to a Gigabit Ethernet 40-port DPC. |
| Configure Port-Mirroring Instances. | 1. Click **Add new entry** next to Fpc.  
2. Click **Port Mirror Instance** next to fpc and perform the following:  
   • **Add**—Adds the selected port-mirroring instances from the Non member list to the Members list.  
   • **Remove**—Removes the selected port-mirroring instances from the Members list.  
   • **Add All**—Adds all the port-mirroring instances from the Non-members list to the Members list.  
   • **Remove All**—Removes all the port-mirroring instances from the Members list. |
Table 48: FPC Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associate a sampling instance.</td>
<td>1. Click Add new entry next to Fpc.</td>
</tr>
<tr>
<td></td>
<td>2. Click Sampling Instances next to fp.</td>
</tr>
<tr>
<td></td>
<td>3. Click Add new entry next to Sampling Instances.</td>
</tr>
<tr>
<td></td>
<td>4. From the Name list, select the sampling instance name.</td>
</tr>
<tr>
<td></td>
<td>5. In the Comment box, enter the comment.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring Aggregated Devices (NSM Procedure) on page 97
- Configuring Chassis Alarms (NSM Procedure) on page 98
- Configuring a T640 Router on a Routing Matrix (NSM Procedure) on page 105

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

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

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Chassis > Lcc.
4. Add or modify settings as specified in Table 49 on page 105.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 49: Lcc Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the T640 routing node.</td>
<td>1. Click Add new entry next to Lcc.</td>
</tr>
<tr>
<td></td>
<td>2. From the Name list, select the number that specifies a T640 router on a routing matrix. Range: 0 through 3</td>
</tr>
<tr>
<td></td>
<td>3. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>- online-expected—On a TX Matrix router, configures a T640 router so that if it does not come online, an alarm is sent to the TX Matrix router. On a TX Matrix Plus router, configure a T1600 router so that if it does not come online, an alarm is sent to the TX Matrix Plus router.</td>
</tr>
<tr>
<td></td>
<td>- offline—On a TX Matrix router, configures a T640 router so that it is not part of the routing matrix. On a TX Matrix Plus router, configure a T1600 router so that it is not part of the routing matrix.</td>
</tr>
</tbody>
</table>
### Table 49: Lcc Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure a port-mirroring instance for the DPC and its corresponding Packet Forwarding Engines. | 1. Click **Fpc** next to Lcc.  
2. Click **Add new entry** next to Fpc.  
3. From the **Name** list, select the slot number of the DPC.  
4. From the **Power** list, configure the Flexible PIC Concentrator (FPC) to stay offline or to come online automatically. |
| Configures aggregate port, maximum queues per interface and port-mirroring instances for the PICs. | 1. Click **Add new entry** next to Fpc.  
2. Click **Pic** next to fpc.  
3. Click **Add new entry** next to PIC.  
4. From the **Name** list, select the slot number of the DPC.  
5. In the **Comment** box, enter the comment.  
6. From the **Framing** list, select the framing type.  
7. From the **Vtmapping** list, select one of the virtual tributary mapping.  
   - **klm**—KLM standard.  
   - **itu-t**—International Telephony Union standard.  
8. Select the **No Concatenate** check box to not concatenate (multiplex) the output of a SONET/SDH PIC (an interface with a name so-fpc/pic/port).  
9. Select the **Aggregate Ports** check box if you want to aggregate multiple ports on a PIC as a single port.  
10. Select the **Sparse Dlics** check box to support a full data-link connection identifier (DLCI) range (1 through 1022).  
11. From the **Mlfr Uni Nni Bundles** list, select the number of multilink frame relay user-to-network interface network-to-network interface (UNI-NNI) (FRF.16) bundles to allocate on a Link Services PIC.  
   Range: 1 through 255  
12. From the **Max Queues Per Interface** list, select the required egress queues on IQ interfaces. |
| Enable a service package on adaptive services interfaces. | 1. Click **Add new entry** next to Fpc.  
2. Click **Pic** next to fpc.  
3. Click **Add new entry** next to Pic.  
4. Click **Adaptive Services** next to pic.  
5. Choose **Adaptive Services** to enable a service package on adaptive services interfaces. |
Table 49: Lcc Configuration Details *(continued)*

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure channelized E1 port and channel specifications. | 1. Click *Add new entry* next to Fpc.  
2. Click *Pic* next to fpc.  
3. Click *Add new entry* next to pic.  
4. Click *Ce1* next to pic.  
5. In the *Comment* box, enter the comment.  
6. Click *E1* next to Ce1.  
7. Click *Add new entry* next to E1.  
8. From the *Name* list, select the port number.  
9. In the *Comment* box, enter the comment.  
10. Click *Channel Group* next to e1.  
11. Click *Add new entry* next to Channel Group.  
12. From the *Name* list, select the channel number.  
13. In the *Comment* box, enter the comment.  
14. In the *Timeslots* box, enter the actual time slot number. |
| Configure channelized T3 port and channel specifications. | 1. Click *Add new entry* next to Fpc.  
2. Click *Pic* next to fpc.  
3. Click *Add new entry* next to Pic.  
4. Click *Ct3* next to pic.  
5. In the *Comment* box, enter the comment.  
6. Click *Port* next to Ct3.  
7. Click *Add new entry* next to Port.  
8. From the *Name* list, select the port number.  
9. In the *Comment* box, enter the comment.  
10. Click *T1* next to Port.  
11. Click *Add new entry* next to T1.  
12. From the *Name* list, select the link number.  
13. In the *Comment* box, enter the comment.  
14. Click *Channel Group* next to t1.  
15. Click *Add new entry* next to Channel Group.  
16. From the *Name* list, select the channel number.  
17. In the *Comment* box, enter the comment.  
18. In the *Timeslots* box, enter the actual time slot number. |
| Configure data used in a hash key for a protocol family. | 1. Click *Add new entry* next to Fpc.  
2. Click *Pic* next to fpc.  
3. Click *Add new entry* next to Pic.  
4. Click *Hash Key* next to pic.  
5. In the *Comment* box, enter the comment.  
6. Click *Family* next to Hash Key.  
7. In the *Comment* box, enter the comment. |
### Table 49: Lcc Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| **Configure data used in a hash key for the **inet** protocol family when configuring PIC-level symmetrical load balancing on an 802.3ad link aggregation group.** | 1. Click **Inet** next to Family.  
2. In the **Comment** box, enter the comment.  
3. Click **Layer 3** next to Inet.  
4. In the **Comment** box, enter the comment.  
5. Select the **Destination Address** check box to compute symmetrical hashing based on the destination address.  
6. Click **Layer 4** next to Inet.  
7. In the **Comment** box, enter the comment.  
8. Click **Symmetric Hash** next to Inet.  
9. In the **Comment** box, enter the comment.  
10. Select the **Complement** check box to include the complement of the symmetric hash in the hash key. |
| **Configure data used in a hash key for the **multiservice** protocol family when configuring PIC-level symmetrical hashing for load balancing on an 802.3ad link aggregation group.** | 1. Click **Multiservice** next to Family.  
2. In the **Comment** box, enter the comment.  
3. Select the **Source Mac** check box to include source MAC address in the hash key.  
4. Select the **Destination Mac** check box to include destination MAC address in the hash key.  
5. Click **Payload** next to Multiservice.  
6. Click **Ip** next to Payload.  
7. In the **Comment** box, enter the comment.  
8. Select the **Layer 4** check box to include Layer 4 IP information in the hash key.  
9. Click **Layer 3** next to Ip.  
10. Select one of the following:  
    - **source-ip-only**—To include source IP only in hash-key.  
    - **destination-ip-only**—To include desintation IP only in hash-key.  
11. Click **Symmetric Hash** next to Multiservice.  
12. In the **Comment** box, enter the comment.  
13. Select the **Complement** check box to include the complement of the symmetric hash in the hash key. |
| **Configure the channelized T3 port number on the PIC.** | 1. Click **Add new entry** next to Fpc.  
2. Click **Pic** next to fpc.  
3. Click **Add new entry** next to Pic.  
4. Click **Port** next to pic.  
5. From the **Name** list, select the port number.  
6. In the **Comment** box, enter the comment.  
7. From the **Framing** list, select the framing type. |
| **Configure delay buffers.** | 1. Click **Add new entry** next to Fpc.  
2. Click **Pic** next to fpc.  
3. Click **Add new entry** next to Pic.  
4. Click **Q Pic Large Buffer** next to pic.  
5. In the **Comment** box, enter the comment. |
Table 49: Lcc Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure port-mirroring instances for PIC.| 1. Click **Add new entry** next to Fpc.  
2. Click **Pic** next to fpc.  
3. Click **Add new entry** next to Pic.  
4. Click **Port Mirror Instance** next to pic and perform the following:  
   • **Add**—Adds the selected port-mirroring instances from the Non member list to the Members list.  
   • **Remove**—Removes the selected port-mirroring instances from the Members list.  
   • **Add All**—Adds all the port-mirroring instances from the Non-members list to the Members list.  
   • **Remove All**—Removes all the port-mirroring instances from the Members list. |
| Enable shaping on an L2TP session.        | 1. Click **Add new entry** next to Fpc.  
2. Click **Pic** next to fpc.  
3. Click **Add new entry** next to Pic.  
4. Click **Traffic Manager** next to pic.  
5. From the **Ingress Shaping Overhead** list, select the number of CoS shaping overhead bytes to add to the packets on the ingress side of the L2TP tunnel to determine the shaped session packet length.  
   Range: 0 through 255  
6. From the **Egress Shaping Overhead** list, select the number of CoS shaping overhead bytes to add to the packets on the egress interface.  
   Range: 0 through 255  
7. From the **Mode** list, select the mode of shaping. |
| Configure the amount of bandwidth for tunnel services. | 1. Click **Add new entry** next to Fpc.  
2. Click **Pic** next to fpc.  
3. Click **Add new entry** next to Pic.  
4. Click **Tunnel Service** next to pic.  
5. From the **Bandwidth** list, select the bandwidth of 1 Gbps or 10Gbps on the Packet Forwarding Engine connected to a Gigabit Ethernet 40-port DPC. |
| Configure port-mirroring instances for FPC. | 1. Click **Add new entry** next to Fpc.  
2. Click **Port Mirror Instance** next to fpc and perform the following:  
   • **Add**—Adds the selected port-mirroring instances from the Non member list to the Members list.  
   • **Remove**—Removes the selected port-mirroring instances from the Members list.  
   • **Add All**—Adds all the port-mirroring instances from the Non-members list to the Members list.  
   • **Remove All**—Removes all the port-mirroring instances from the Members list. |
### 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 (SFM s), System and Switch Boards (SSBs), Forwarding Engine Boards (FEB s), 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 50 on page 110.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.

### Table 50: 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 <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>2. From the <strong>keepalive</strong> 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 <strong>Failover</strong> next to Redundancy.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. Select the type of failover.</td>
</tr>
</tbody>
</table>
Table 50: 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 97
- Configuring a T640 Router on a Routing Matrix (NSM Procedure) on page 105
- Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors (NSM Procedure) on page 111

**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 51 on page 112.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.
Table 51: 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 97
- Configuring a T640 Router on a Routing Matrix (NSM Procedure) on page 105
- Configuring Routing Engine Redundancy (NSM Procedure) on page 110
Configuring Authentication

- Configuring RADIUS Authentication (NSM Procedure) on page 113
- Configuring TACACS+ Authentication (NSM Procedure) on page 114
- Configuring Authentication Order (NSM Procedure) on page 115
- Configuring User Access (NSM Procedure) on page 116
- Configuring Template Accounts (NSM Procedure) on page 117

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 52 on page 113.
5. Click one:
   - New—Adds a new RADIUS server.
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

Table 52: 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>
</tbody>
</table>

Copyright © 2010, Juniper Networks, Inc.
Table 52: RADIUS 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 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 114
- Configuring Authentication Order (NSM Procedure) on page 115
- Configuring User Access (NSM Procedure) on page 116

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 53 on page 114.
5. Click one:
   - New—Adds a new TACACS+ server.
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

Table 53: 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 53: 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 113
- Configuring Authentication Order (NSM Procedure) on page 115
- Configuring User Access (NSM Procedure) on page 116

Configuring Authentication Order (NSM Procedure)

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

To configure authentication order:

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

Related Topics

- Configuring RADIUS Authentication (NSM Procedure) on page 113
- Configuring TACACS+ Authentication (NSM Procedure) on page 114
- Configuring User Access (NSM Procedure) on page 116
Configuring User Access (NSM Procedure)

This section includes the following topics:

- Configuring Login Classes on page 116
- Configuring User Accounts on page 117

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 54 on page 116.
5. Click one:
   - New—Adds a new login class.
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 54: 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, &quot;request system reboot&quot;.</td>
</tr>
<tr>
<td>Login &gt; Class &gt; Permissions</td>
<td>Confi£ues 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 55 on page 117.
5. Click one:
   - New—Adds a new user account.
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 55: User Authentication Configuration Details

<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>
<tr>
<td>Login &gt; User &gt; Authentication</td>
<td>Plain Text Password Value</td>
<td>Specifies the user’s password. Enter the plain text password for the user.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring RADIUS Authentication (NSM Procedure) on page 113
- Configuring TACACS+ Authentication (NSM Procedure) on page 114
- Configuring Authentication Order (NSM Procedure) on page 115

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 118
• Creating a Local Template Account on page 119

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 56 on page 118.
5. Click one:
   • New—Creates a new remote template account.
   • OK—Saves the changes.
   • Cancel—Cancels the modifications.

Table 56: 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.</td>
<td>Enter the user name. For example, type remote.</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 operator.</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 57 on page 119.
5. Click one:
   - **New**—Creates a new local template account.
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 57: 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. Enter the user name. For example, type admin.</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 superuser.</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

- Configuring RADIUS Authentication (NSM Procedure) on page 113
- Configuring TACACS+ Authentication (NSM Procedure) on page 114
- Configuring Authentication Order (NSM Procedure) on page 115
CHAPTER 13

Configuring Class of Service Features

- Configuring CoS Classifiers (NSM Procedure) on page 122
- Configuring CoS Code Point Aliases (NSM Procedure) on page 124
- Configuring CoS Drop Profile (NSM Procedure) on page 125
- Configuring CoS Forwarding Classes (NSM Procedure) on page 127
- Configuring CoS Forwarding Policy (NSM Procedure) on page 129
- Configuring CoS Fragmentation Maps (NSM Procedure) on page 130
- Configuring CoS Host Outbound Traffic (NSM Procedure) on page 131
- Configuring CoS Interfaces (NSM Procedure) on page 132
- Configuring CoS Routing Instances (NSM Procedure) on page 138
- Configuring CoS Schedulers (NSM Procedure) on page 139
- Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 141
- Configuring CoS Restricted Queues (NSM Procedure) on page 142
- Configuring Tracing Operations (NSM Procedure) on page 143
- Configuring CoS Traffic Control Profiles (NSM Procedure) on page 144
- Configuring CoS Translation Table (NSM Procedure) on page 145
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 122.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See 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>
</table>
| Configure behavior aggregate classifiers for DiffServ CoS. | 1. Click Add new entry next to Dscp.  
2. In the Name box, type the name of the behavior aggregate classifier—for example, ba-classifier.  
3. In the Import box, type the name of the default DSCP map. |
### Table 58: Configuring and Applying Behavior Aggregate Classifiers (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a best-effort 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 best-effort forwarding class—for example, <strong>be-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 best-effort traffic—for example, <strong>00001</strong>.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>OK</strong> three times.</td>
</tr>
<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>
<tr>
<td>Configure an assured 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 assured forwarding—for example, <strong>class-af-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 assured forwarding traffic—for example, <strong>001100</strong>.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>OK</strong> three times.</td>
</tr>
<tr>
<td>Apply the behavior aggregate classifier to an interface.</td>
<td>1. Click <strong>Add new entry</strong> next to Interfaces.</td>
</tr>
<tr>
<td></td>
<td>2. In the Interface name box, type the name of the interface—for example, <strong>ge-0/0/0</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add new entry</strong> next to Unit.</td>
</tr>
<tr>
<td></td>
<td>4. In the Unit number box, type the logical interface unit number—for example, <strong>0</strong>.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Configure</strong> next to Classifiers.</td>
</tr>
<tr>
<td></td>
<td>6. In the Classifiers box, under Dscp, type the name of the previously configured behavior aggregate classifier—for example, <strong>ba-classifier</strong>.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>
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 125
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 122
- Configuring CoS Drop Profile (NSM Procedure) on page 125
- Configuring CoS Forwarding Classes (NSM Procedure) on page 127
- Configuring CoS Interfaces (NSM Procedure) on page 132
- Configuring CoS Rewrite Rules (NSM Procedure)
- Configuring CoS Schedulers (NSM Procedure) on page 139
- Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 141

**Configuring CoS Drop Profile (NSM Procedure)**

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

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

To configure drop profiles in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure drop profiles.
3. Click the Configuration tab. In the configuration tree expand Class of Service.
4. Select Drop Profiles.
5. Add or modify the drop profiles as specified in Table 60 on page 126.
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 60: Drop Profile Configuration Fields

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

**Related Topics**
- Configuring CoS Classifiers (NSM Procedure) on page 122
- Configuring CoS Code Point Aliases (NSM Procedure) on page 124
- Configuring CoS Forwarding Classes (NSM Procedure) on page 127
- Configuring CoS Interfaces (NSM Procedure) on page 132
- Configuring CoS Rewrite Rules (NSM Procedure)
- Configuring CoS Schedulers (NSM Procedure) on page 139
- Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 141

**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 128.
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>
| **Assign best-effort traffic to queue 0.** | 1. Select *Queue* and click *Add new entry.*  
2. In the Queue num box, type 0.  
3. In the Class name box, type the previously configured name of the best-effort class—for example, *be-class.*  
4. Click *OK.* |
| **Assign expedited forwarding traffic to queue 1.** | 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 122
- Configuring CoS Code Point Aliases (NSM Procedure) on page 124
- Configuring CoS Drop Profile (NSM Procedure) on page 125
- Configuring CoS Interfaces (NSM Procedure) on page 132
- Configuring CoS Rewrite Rules (NSM Procedure) on page 139
- Configuring CoS Schedulers (NSM Procedure) on page 141
- Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 141
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 129.
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. |
Table 62: Forwarding Policy Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the map for CoS forwarding routes.</td>
<td>1. Click <strong>Add new entry</strong> next to Next Hop Map.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Name</strong> box, enter the map that defines next-hop routes.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Forwarding Class</strong> next to next-hop-map.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Add new entry</strong> next to Forwarding Class.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Name</strong> box, enter the name of the forwarding class.</td>
</tr>
<tr>
<td></td>
<td>6. Select the <strong>Non LSP Next Hop</strong> check box to use a non-LSP next hop for traffic sent to the forwarding class next-hop map of the forwarding policy.</td>
</tr>
<tr>
<td></td>
<td>7. Select the <strong>Discard</strong> check box to discard the traffic sent to the forwarding class for the next-hop map referenced by the forwarding policy.</td>
</tr>
<tr>
<td></td>
<td>8. Click <strong>Lsp Next Hop</strong> next to forwarding-class.</td>
</tr>
<tr>
<td></td>
<td>9. Click <strong>New</strong> button next to Lsp Next Hop.</td>
</tr>
<tr>
<td></td>
<td>10. In the <strong>New Lsp-next-hop</strong> dialog box, enter the LSP regular expression to which to map the forwarded traffic.</td>
</tr>
<tr>
<td></td>
<td>11. Click <strong>Next Hop</strong> next to forwarding-class.</td>
</tr>
<tr>
<td></td>
<td>12. In the <strong>New next-hop</strong> dialog box, enter the next-hop name or address to which to map forwarded traffic.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Configuring CoS Classifiers (NSM Procedure) on page 122
- Configuring CoS Routing Instances (NSM Procedure) on page 138
- Configuring Tracing Operations (NSM Procedure) on page 143

**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 131.
6. Click one:
• OK—Saves the changes.
• Cancel—Cancels the modifications.

Table 63: Fragmentation Maps Configuration Details

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

| Set the fragmentation threshold for an individual forwarding class for only AS PIC link services IQ interfaces (lsq). | 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 129
• Configuring CoS Schedulers (NSM Procedure) on page 139
• Configuring CoS Traffic Control Profiles (NSM Procedure) on page 144

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 132.
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 <strong>Forwarding Class</strong> box, enter the name for the forwarding class.</td>
</tr>
<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 <strong>Dscp Code Point</strong> list, select the DSCP code point value.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Configuring CoS Forwarding Classes (NSM Procedure) on page 127
- Configuring CoS Fragmentation Maps (NSM Procedure) on page 130
- Configuring CoS Traffic Control Profiles (NSM Procedure) on page 144
- Configuring CoS Interfaces (NSM Procedure) on page 132

### 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 133.
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>1. Expand the Interfaces tree and select Interface.</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 Interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the interface name in the Name box.</td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the interface name.</td>
<td>1. Expand the Interfaces tree and select Interface.</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 Interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the interface name in the Name box.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for the interface.</td>
<td>1. Expand the Interfaces tree and select Interface.</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 Interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the comment for the interface in the Comment box.</td>
</tr>
<tr>
<td>Scheduler Map</td>
<td>Specifies the scheduler configuration mapped to the forwarding class.</td>
<td>1. Expand the Interfaces tree and select Interface.</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 Interface.</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 Interfaces tree and select Interface.</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 Interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Select the scheduler map chassis from the list.</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</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 Interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Expand the Interface tree and select <strong>Input Traffic Control Profile</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the comment and the profile name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click <strong>Ok</strong>.</td>
</tr>
<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 <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in Interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Expand the Interface tree and select <strong>Input Traffic Control Profile Remaining</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify a comment and a profile name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click <strong>Ok</strong>.</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 <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in Interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Expand the Interface tree and select <strong>Output Traffic Control Profile</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify a comment and a profile name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click <strong>Ok</strong>.</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 <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in Interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Expand the Interface tree and select <strong>Output Traffic Control Profile Remaining</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify a comment and a profile name.</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>
</table>
| Shaping Rate | Shapes the output of the physical interface, so that the interface transmits less traffic than it is physically capable of carrying. | 1. Click the New button or select an interface and click the Edit button in Interface.  
2. Expand Interface tree and select Shaping Rate.  
3. Specify the comment and the rate  
4. Click Ok. |
| Unit       | Sets the units that need to be allocated to the specific forwarding class and scheduling map. | 1. Click the New button or select an interface and click the Edit button in Interface.  
2. Expand Interface tree and select Unit.  
3. Specify the Unit, Classifiers, Output Traffic Control Profile and Shaping Rate.  
4. Click Ok. |
| Interface Set |                                                                 | 1. Expand the Interfaces tree and select Interface Set.  
2. Click the New button or select an interface set and click the Edit button.  
3. Select the name from the list. |
| Name       | Specifies the interface set name.                                          | 1. Expand the Interfaces tree and select Interface Set.  
2. Click the New button or select an interface set and click the Edit button.  
3. Select the name from the list. |
| Comment    | Specifies the comment for the interface.                                  | 1. Expand the Interfaces tree and select Interface Set.  
2. Click the New button or select an interface set and click the Edit button.  
3. Enter the comment. |
### Table 65: Interfaces Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Internal Node         | Sets the scheduler node as internal, allowing resource scheduling to be applied equally to interface sets that include child nodes and those that do not include child nodes. | 1. Expand the **Interfaces** tree and select **Interface Set**.  
2. Click the **New** button or select an interface set and click the **Edit** button.  
3. Set the internal node.                                                                 |
| Excess Bandwidth Share| Sets the excess 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 **Excess Bandwidth Share**.  
4. Specify the comment and proportion.  
5. Click **Ok**.                                                                                          |
| 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**.                                                                                          |
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</td>
<td>Applies an input traffic scheduling and shaping profile for remaining traffic to the logical interface.</td>
<td>1. Expand the Interfaces tree and select Interface Set.</td>
</tr>
<tr>
<td>Remaining</td>
<td></td>
<td>2. Click the New button or select an interface set and click the Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Expand interface—set tree and select Input Traffic Control Profile Remaining.</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 Ok.</td>
</tr>
</tbody>
</table>

Output Traffic Control Profile

1. Expand the Interfaces tree and select Interface Set.
2. Click the New button or select an interface set and click the Edit button.
4. Specify the comment and profile name.
5. Click Ok.

Output Traffic Control Profile Remaining

1. Expand the Interfaces tree and select Interface Set.
2. Click the New button or select an interface set and click the Edit button.
3. Expand interface—set tree and select Output Traffic Control Profile Remaining.
4. Specify the comment and profile name.
5. Click Ok.

Related Topics
- Configuring CoS Classifiers (NSM Procedure) on page 122
- Configuring CoS Code Point Aliases (NSM Procedure) on page 124
- Configuring CoS Drop Profile (NSM Procedure) on page 125
You can apply a custom MPLS EXP classifier to the routing instance with VPN routing and forwarding (VRF) table labels enabled using this option. The default MPLS EXP classifier or one that is previously defined can be applied for routing instance.

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

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Class of Service.
4. Select Routing Instances.
5. Add or modify settings as specified in Table 66 on page 138.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

**Table 66: Routing Instances Configuration Details**

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Apply a custom MPLS EXP classifier to the routing instance for routing instances with VRF table labels enabled. | 1. Click **Add new entry** next to Routing Instances.  
2. In the **Name** box, enter the name of the routing instance. |
| Specify the classifier name. | 1. Click **Classifiers** next to routing-instances.  
2. Click **Dscp** next to Classifiers.  
3. In the **Comment** box, enter the comment.  
4. From the **Classifier name** list, select the classifier name.  
5. Click **Dscp ipv6** next to Classifiers.  
6. In the **Comment** box, enter the comment.  
7. From the **Classifier name** list, select the classifier name.  
8. Click **Exp** next to Classifiers.  
9. From the **Classifier Name** list, select the classifier name.  
10. Click **ieee 802.1** next to Classifiers.  
11. In the **Comment** box, enter the comment.  
12. From the **Classifier name** list, select the classifier name.  
13. From the **Vlan tag** list, select the VLAN tag. |
Table 66: Routing Instances Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify a rewrite-rules mapping for the traffic that passes through all queues on the interface. | 1. Click Rewrite Rules next to routing-instances.  
2. In the Comment box, enter the comment.  
4. Click IEEE 802.1 next to Rewrite Rules.  
5. Select one of the following:  
  • IEEE–802.1d—To apply an IEEE-802.1 rewrite rule  
  • IEEE–802.1ad—To apply an IEEE-802.1ad rewrite rule  
6. In the Comment box, enter the comment.  
7. From the Rewrite Rule Name list, select the name of a rewrite-rules mapping.  
8. From the Vlan tag list, select the VLAN tag. |

Related Topics

- Configuring CoS Classifiers (NSM Procedure) on page 122
- Configuring CoS Forwarding Policy (NSM Procedure) on page 129
- Configuring CoS Restricted Queues (NSM Procedure) on page 142
- Configuring Tracing Operations (NSM Procedure) on page 143

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 140.
6. Click one:  
  • OK—Saves the changes.  
  • Cancel—Cancels the modifications.

NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the Network and Security Manager Administration Guide for more information.
Table 67: Configuring Schedulers

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the buffer size.</td>
<td>1.</td>
</tr>
<tr>
<td></td>
<td>Click the <strong>Add New</strong> icon.</td>
</tr>
<tr>
<td></td>
<td>2.</td>
</tr>
<tr>
<td></td>
<td>Expand <strong>BufferSize</strong>.</td>
</tr>
<tr>
<td></td>
<td>3.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>Percent</strong>.</td>
</tr>
<tr>
<td></td>
<td>4.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Configure drop profile map.</td>
<td>1.</td>
</tr>
<tr>
<td></td>
<td>Click the <strong>Add New</strong> icon.</td>
</tr>
<tr>
<td></td>
<td>2.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>drop-profile-map</strong>.</td>
</tr>
<tr>
<td></td>
<td>3.</td>
</tr>
<tr>
<td></td>
<td>In the Loss Priority box, select the required loss priority—for example, <strong>high</strong>.</td>
</tr>
<tr>
<td></td>
<td>4.</td>
</tr>
<tr>
<td></td>
<td>In the Protocol box, select the type of protocol—for example, <strong>any</strong>.</td>
</tr>
<tr>
<td></td>
<td>5.</td>
</tr>
<tr>
<td></td>
<td>In the Drop Profile box, select the previously configured drop profile.</td>
</tr>
<tr>
<td></td>
<td>6.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Specify the transmit rate.</td>
<td>1.</td>
</tr>
<tr>
<td></td>
<td>Click the <strong>Add New</strong> icon.</td>
</tr>
<tr>
<td></td>
<td>2.</td>
</tr>
<tr>
<td></td>
<td>Expand <strong>Transmit Rate</strong>.</td>
</tr>
<tr>
<td></td>
<td>3.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>Rate</strong>.</td>
</tr>
<tr>
<td></td>
<td>4.</td>
</tr>
<tr>
<td></td>
<td>Under Rate, select the appropriate option:</td>
</tr>
<tr>
<td></td>
<td>• To not specify transmit rate, select <strong>None</strong>.</td>
</tr>
<tr>
<td></td>
<td>• To enforce a specific transmission rate, select <strong>rate</strong> and type the transmission rate that you want to enforce.</td>
</tr>
<tr>
<td></td>
<td>• To specify a percentage of transmission capacity, select <strong>percent</strong> and type an integer from 1 through 100.</td>
</tr>
<tr>
<td></td>
<td>• To specify the remaining transmission capacity, select <strong>remainder</strong>.</td>
</tr>
<tr>
<td></td>
<td>5.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Configuring CoS Classifiers (NSM Procedure) on page 122
- Configuring CoS Code Point Aliases (NSM Procedure) on page 124
- Configuring CoS Drop Profile (NSM Procedure) on page 125
- Configuring CoS Forwarding Classes (NSM Procedure) on page 127
- Configuring CoS Interfaces (NSM Procedure) on page 132
- Configuring CoS Rewrite Rules (NSM Procedure)
- Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 141
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 141.
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 68: Assigning Forwarding Classes to Output Queues

<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. |
| 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. |
### Table 68: Assigning Forwarding Classes to Output Queues (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
</table>
| 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 122
- Configuring CoS Code Point Aliases (NSM Procedure) on page 124
- Configuring CoS Drop Profile (NSM Procedure) on page 125
- Configuring CoS Forwarding Classes (NSM Procedure) on page 127
- Configuring CoS Interfaces (NSM Procedure) on page 132
- Configuring CoS Rewrite Rules (NSM Procedure)
- Configuring CoS Schedulers (NSM Procedure) on page 139

### Configuring CoS Restricted Queues (NSM Procedure)

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

To configure Class of Service restricted queues in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Class of Service**.
4. Select **Restricted Queue**.
5. Add or modify settings as specified in Table 69 on page 143.
6. Click one:
   - **OK**—Saves the changes.
Cancel— Cancels the modifications.

Table 69: Restricted Queue Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map forwarding classes to restricted queues.</td>
<td>In the Comment box, enter the comment.</td>
</tr>
</tbody>
</table>
| Specify the name of the forwarding class and queue number. | 1. In the Name box, enter the name of the forwarding class.  
2. In the Comment box, enter the comment for the forwarding class.  
3. From the Rqueue Num list, select the output queue number. Range: 0 through 3 |

Related Topics
- Configuring CoS Classifiers (NSM Procedure) on page 122
- Configuring CoS Forwarding Policy (NSM Procedure) on page 129
- Configuring CoS Translation Table (NSM Procedure) on page 145
- Configuring Tracing Operations (NSM Procedure) on page 143

Configuring Tracing Operations (NSM Procedure)

You can configure tracing operations using this option.

To configure tracing operations in NSM:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Class Of Service.
4. Select Traceoptions.
5. Add or modify settings as specified in Table 70 on page 143.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

Table 70: Traceoptions Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure tracing operations. | 1. In the Comment box, enter the comment for the traceoptions.  
2. Select the No Remote Trace check box to disable remote tracing globally or for a specific tracing operation. |
Table 70: Traceoptions Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specifies the name of the file to receive the output of the tracing operation and specifies the maximum number of trace files. | 1. Click File next to Traceoptions.  
2. In the Comment box, enter the comment for the file.  
3. In the Filename box, enter the name of the file to receive the output of the tracing operation.  
4. In the Size box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).  
5. From the Files list, select the maximum number of trace files. Range: 2 through 1000.  
6. Select world-readable to enable unrestricted file access.  
7. Select no-world-readable to restrict file access to owner. This is the default setting.  
8. In the Match box, enter the regular expression. |

| Specifies the tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. | 1. Click Flag next to Traceoptions.  
2. Click Add new entry next to Flag.  
3. From the Name list, select the flag.  
4. In the Comment box, enter the comment for the flag. |

**Related Topics**
- Configuring CoS Rewrite Rules (NSM Procedure)
- Configuring CoS Routing Instances (NSM Procedure) on page 138
- Configuring CoS Restricted Queues (NSM Procedure) on page 142
- Configuring CoS Traffic Control Profiles (NSM Procedure) on page 144

**Configuring CoS Traffic Control Profiles (NSM Procedure)**

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

To configure CoS Traffic Control Profiles in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device for which you want to configure CoS Restricted Queues.
3. Click the Configuration tab. In the configuration tree, expand Class of Service.
5. Add or modify settings as specified in Table 71 on page 145.
6. Click one:  
   - OK—Saves the changes.  
   - Cancel—Cancels the modifications.
Table 71: Traffic Control profile Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure traffic shaping and scheduling profiles for Gigabit Ethernet IQ, Channelized IQ PICs, and AS PIC FRF:16 LSQ interfaces. | 1. In the Name box, enter the name of the traffic-control profile.  
2. Select the scheduler map.  
3. Expand traffic-control-profiles.  
4. Select the following:  
  - Select Delay Buffer Rate as default value and set the delay buffer rate.  
  - Select Guaranteed Rate if you do not configure delay buffer rate. The delay buffer rate calculation is based on the guaranteed rate.  
  - Select Shaping Rate if you do not configure delay buffer rate or guaranteed rate. The delay buffer rate calculation is based on the shaping rate.  

NOTE: On LSQ interfaces, you can configure the guaranteed rate as a percentage from 1 through 100.  
On IQ and IQ2 interfaces, you can configure the guaranteed rate as an absolute rate from 1000 through 160,000,000,000 bits per second.  

Related Topics  
- Configuring CoS Drop Profile (NSM Procedure) on page 125  
- Configuring CoS Host Outbound Traffic (NSM Procedure) on page 131  
- Configuring CoS Routing Instances (NSM Procedure) on page 138  
- Configuring CoS Translation Table (NSM Procedure) on page 145

Configuring CoS Translation Table (NSM Procedure)

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

To configure CoS Translation Table in NSM:
1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Class of Service**.
4. Select **Translation Table**.
5. Add or modify settings as specified in Table 72 on page 146.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

**Table 72: Translation Table Configuration Details**

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Translate incoming IPv4 DSCP values to new values. | 1. Click **To Dscp From Dscp** next to Translation Table.  
2. Click **Add new entry** next to To Dscp From Dscp.  
3. In the **Name** box, enter the IPv4 DSCP values.  
4. In the **Comment** box, enter the comment.  
5. Click **To Code Point** next to to-dscp-from-dscp.  
6. Click **Add new entry** next to to-dscp-from-dscp.  
7. From the **Name** list, select the DSCP.  
8. In the **Comment** box, enter the comment.  
9. Click **From Code Points** next to to-code-point and perform the following:  
   - **Add**—Adds the selected code points from the Non member list to the Members list.  
   - **Remove**—Removes the selected code points from the Members list.  
   - **Add All**—Adds all the code points from the Non-members list to the Members list.  
   - **Remove All**—Removes all the code points from the Members list. |
### Table 72: Translation Table Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Translate incoming IPv6 DSCP values to new values. | 1. Click **To Dscp ipv6 From Dscp ipv6** next to Translation Table.  
2. Click **Add new entry** next to To Dscp ipv6 From Dscp ipv6.  
3. In the **Name** box, enter the IPv6 DSCP values  
4. In the **Comment** box, enter the comment.  
5. Click **To Code Point** next to to-dscp-ipv6-from-dscp-ipv6.  
6. Click **Add new entry** next to to-dscp-ipv6-from-dscp-ipv6  
7. From the **Name** list, select the DSCP.  
8. In the **Comment** box, enter the comment.  
9. Click **From Code Points** next to to-code-point and perform the following:  
  - **Add**—Adds the selected code points from the Non member list to the Members list.  
  - **Remove**—Removes the selected code points from the Members list.  
  - **Add All**—Adds all the code points from the Non-members list to the Members list.  
  - **Remove All**—Removes all the code points from the Members list. |
Table 72: Translation Table Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Translate incoming MPLS EXP values to new values. | 1. Click **To Exp From Exp** next to Translation Table.  
2. Click **Add new entry** next to To Exp From Exp.  
3. In the **Name** box, enter the MPLS EXP values.  
4. In the **Comment** box, enter the comment.  
5. Click **To Code Point** next to to-exp-from-exp.  
6. Click **Add new entry** next to to-exp-from-exp.  
7. From the **Name** list, select the EXP code point.  
8. In the **Comment** box, enter the comment.  
9. Click **From Code Points** next to to-code-point and perform the following:  
   • **Add**—Adds the selected code points from the Non member list to the Members list.  
   • **Remove**—Removes the selected code points from the Members list.  
   • **Add All**—Adds all the code points from the Non-members list to the Members list.  
   • **Remove All**—Removes all the code points from the Members list. |
### Table 72: Translation Table Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Translate incoming Inet precedence values to new values. | 1. Click **To Inet Precedence From Inet Precedence** next to Translation Table.  
2. Click **Add new entry** next to To Inet Precedence From Inet Precedence.  
3. In the Name box, enter the Inet precedence values.  
4. In the Comment box, enter the comment.  
5. Click **To Code Point** next to to-inet-precedence-from-inet-precedence.  
6. Click **Add new entry** next to to-inet-precedence-from-inet-precedence.  
7. From the Name list, select the INET precedence code point.  
8. In the Comment box, enter the comment.  
9. Click **From Code Points** next to to-code-point and perform the following:  
   • **Add**—Adds the selected code points from the Non member list to the Members list.  
   • **Remove**—Removes the selected code points from the Members list.  
   • **Add All**—Adds all the code points from the Non-members list to the Members list.  
   • **Remove All**—Removes all the code points from the Members list. |

**Related Topics**  
- Configuring CoS Rewrite Rules (NSM Procedure)  
- Configuring CoS Routing Instances (NSM Procedure) on page 138  
- Configuring Tracing Operations (NSM Procedure) on page 143  
- Configuring CoS Traffic Control Profiles (NSM Procedure) on page 144
CHAPTER 14

Configuring Event Options

• Configuring Destinations for File Archiving (NSM Procedure) on page 151
• Configuring Event Script (NSM Procedure) on page 152
• Generating Internal Events (NSM Procedure) on page 154
• Configuring Event Policy (NSM Procedure) on page 154
• Configuring Event Policy Tracing Operations (NSM Procedure) on page 157

Configuring Destinations for File Archiving (NSM Procedure)

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

To configure destinations for file archiving in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Event Options.
4. Select Destination.
5. Add or modify settings as specified in Table 73 on page 151.
6. Click one:
   • OK—Saves the changes.
   • Cancel—Cancels the modifications.

Table 73: Destination 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 destination.</td>
<td>Enter the name for the destination.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for the destination.</td>
<td>Enter the comment for the destination.</td>
</tr>
</tbody>
</table>
## Table 73: Destination Configuration Details *(continued)*

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer Delay</td>
<td>Specifies the number of seconds the event process (eventd) waits before beginning to upload a file or multiple files.</td>
<td>Select the duration of the delay.</td>
</tr>
</tbody>
</table>

### Destination > Archive Sites

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies an archive site to which files are transferred. If you specify more than one archive site, the router attempts to transfer to the first archive site in the list, moving to the next site only if the transfer fails.</td>
<td>Enter the archive destination.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for the archive sites.</td>
<td>Enter the comment for the archive site.</td>
</tr>
<tr>
<td>Password</td>
<td>Defines a plain-text password for login into the archive site.</td>
<td>Enter the password.</td>
</tr>
</tbody>
</table>

### Related Topics
- Configuring Event Script (NSM Procedure) on page 152
- Generating Internal Events (NSM Procedure) on page 154
- Configuring Event Policy (NSM Procedure) on page 154
- Configuring Event Policy Tracing Operations (NSM Procedure) on page 157

## Configuring Event Script (NSM Procedure)

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

To configure event scripting in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Event Options > Event Script.
4. Select Event Script.
5. Add or modify settings as specified in Table 74 on page 153.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
Table 74: Event Script Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the name of an Extensible Stylesheet Language Transformations (XSLT) or Stylesheet Language Alternative Syntax (SLAX) file containing an event script.</td>
<td>1. Click <strong>File</strong> next to Event Script.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to File.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the filename.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td>Calculate the checksum.</td>
<td>1. Click <strong>Checksum</strong> next to file.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Md5</strong> box, enter the MD5 checksum.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Sha1</strong> box, enter the SHA-1 checksum.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Sha 256</strong> box, enter the SHA-256 checksum.</td>
</tr>
<tr>
<td>Configure the username and passphrase for a remote machine.</td>
<td>1. Click <strong>Remote Execution</strong> next to file.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Remote Execution.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the filename.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Username</strong> box, enter the username for the remote machine.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Passphrase</strong> box, enter the passphrase for the remote machine.</td>
</tr>
<tr>
<td>Define tracing operations for event scripts.</td>
<td>1. Click <strong>Traceoptions</strong> next to Event Script.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. Expand <strong>traceoptions</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>File</strong> next to Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Filename</strong> box, enter the name of the file to receive the output of the tracing operation.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Size</strong> box, enter the maximum trace file size.</td>
</tr>
<tr>
<td></td>
<td>8. From the <strong>Files</strong> list, select the maximum number of trace files.</td>
</tr>
<tr>
<td></td>
<td>9. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>no-world-readable</strong>—To restrict the file access to owner.</td>
</tr>
<tr>
<td></td>
<td>• <strong>world-readable</strong>—To enable unrestricted access.</td>
</tr>
<tr>
<td></td>
<td>10. Click <strong>Flag</strong> next to traceoptions.</td>
</tr>
<tr>
<td></td>
<td>11. Click <strong>Add new entry</strong> next to Flag.</td>
</tr>
<tr>
<td></td>
<td>12. From the <strong>Name</strong> list, select the flag to perform the trace operation.</td>
</tr>
<tr>
<td></td>
<td>13. In the <strong>Comment</strong> box, enter the comment for the flag.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Configuring Destinations for File Archiving (NSM Procedure) on page 151
- Generating Internal Events (NSM Procedure) on page 154
- Configuring Event Policy (NSM Procedure) on page 154
- Configuring Event Policy Tracing Operations (NSM Procedure) on page 157
Generating Internal Events (NSM Procedure)

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

To generate internal events in NSM:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Event Options.
4. Select Generate Event.
5. Add or modify settings as specified in Table 75 on page 154.
6. Click one:
   • OK—Saves the changes.
   • Cancel—Cancels the modifications.

Table 75: Generate Event Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate an internal event, based on a time interval or the time of day.</td>
<td>1. In the Name box, enter the name of an internally generated event 2. In the Comment box, enter the comment for the generate event. 3. Click Time of Day next to generate-event and select one of the following: • time-of-day—To configure a time of day at which to generate a particular event. • time-interval—To configure a frequency at which to generate a particular event.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring Destinations for File Archiving (NSM Procedure) on page 151
- Configuring Event Script (NSM Procedure) on page 152
- Configuring Event Policy (NSM Procedure) on page 154
- Configuring Event Policy Tracing Operations (NSM Procedure) on page 157

Configuring Event Policy (NSM Procedure)

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

To configure an event policy in NSM:
1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Event Options**.
4. Select **Policy**.
5. Add or modify settings as specified in Table 76 on page 155.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

### Table 76: Configure Event Policy Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 1. Define an event policy to be processed by the event process (eventd) process. | 1. Click **Add new entry** next to Policy.  
2. In the **Name** box, enter the policy name.  
3. In the **Comment** box, enter the comment for the policy. |
| 2. Execute the policy only if the attributes of two events are correlated or if the attribute of one event matches a regular expression. | 1. Click **Add new entry** next to Attributes Match.  
2. In the **From Event Attribute** box, enter the first attribute to compare.  
3. From the **Condition** list, select the match condition for the attributes.  
4. In the **To Event Attribute Value** box, enter another attribute.  
5. In the **Comment** box, enter the comment for the attributes-match. |
| 3. Create a list of events that trigger this policy. If one or more of the listed events occurs, the policy is executed. | 1. Click **Add new entry** next to Events.  
2. In the **New events** dialog box, enter the name of the event. |
| 4. Define actions to take if an event occurs. For each policy, you can configure multiple actions. | 1. Click **Then** next to policy.  
2. In the **comment** box, enter the comment.  
3. Select the **Ignore** check box to define a policy that ignores particular events.  
4. Select the **Raise Trap** check box to define a policy that raises a Simple Network Management Protocol (SNMP) trap in response to an event. |

Copyright © 2010, Juniper Networks, Inc.
### Table 76: Configure Event Policy Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify operational mode commands to be issued, the format of the   | 1. Expand **Then** and select Event Script.  
| command output, and a name and destination for the output file.     | 2. Click **Add new entry** next to Event Script.  
                                                                 | 3. In the **Name** box, enter the filename.  
                                                                 | 4. In the **comment** box, enter the comment for the event script.  
                                                                 | 5. From the **Username** list, select the user associated with an action in an event policy.  
                                                                 | 6. In the **Output Filename** box, enter the filename to which to write command or script output for the specified commands or script.  
                                                                 | 7. From the **Output Format** list, select the format for the output of the specified commands.  
| Include command-line arguments to the script for JUNOS op scripts    | 1. Expand **event-script**.  
| and assign a location to which to upload command or script output   | 2. Click **Arguments** next to event-script.  
| for the specified policy.                                            | 3. Click **Add new entry** next to Arguments.  
                                                                 | 4. In the **Name** box, enter the arguments to the script as name.  
                                                                 | 5. In the **comment** box, enter the comment.  
                                                                 | 6. In the **Value** box, enter the variables in the argument values to allow data from the triggering event to be automatically included in the argument.  
                                                                 | 7. Click **Destination** next to event-script.  
                                                                 | 8. From the **Name** list, select the location to which to upload command or script output for the specified policy.  
                                                                 | 9. In the **Comment** box, enter the comment.  
                                                                 | 10. From the **Transfer Delay** list, select the delay in seconds before transferring files.  
                                                                 | 11. Expand **Destinations** and select **Retry Count** next to it.  
                                                                 | 12. In the **Comment** box, enter the comment for the retry count.  
                                                                 | 13. From the **Retry** list, select the number of retries.  
                                                                 | 14. From the **Retry Interval** list, select the length of time to wait between retries.  
| Specify operational mode commands to be issued, the format of the   | 1. Expand **Execute Commands**.  
| command output, and a name and destination for the output file on   | 2. Click **Commands**.  
| receipt of an event.                                                | 3. In the **Name** box, enter the command.  
                                                                 | 4. Click **Destination** next to Execute Commands.  
                                                                 | 5. See                                                                                                                                                                                                 |
| Specify a file to be uploaded to a destination on receipt of an     | 1. Click **Upload** next to Event Script.  
| event.                                                             | 2. In the **Filename** box, enter the name of the file to be uploaded.  
                                                                 | 3. From the **Destination** list, select the name of a destination.  
                                                                 | 4. From the **User Name** list, select the username.  
                                                                 | 5. From the **transfer relay** list, select the delay before transferring files.  |
Table 76: Configure Event Policy Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Create a list of events that must (or must not) occur within a specified time interval for the policy to be triggered. | 1. Click **Add new entry** next to **Within**.  
2. Expand **Within**.  
3. From the **Name** list, select the interval between events.  
4. Click **Events** next to **within**.  
5. Click **Add new entry** next to **Events**.  
6. In the **New events** dialog box, enter the events that trigger this policy.  
7. Expand **Not**.  
8. Click **Events** next to **Not**.  
9. In the **New events** dialog box, enter the events that trigger this policy.  
10. Click **Trigger** next to **Not**.  
11. In the **Comment** box, enter the comment.  
12. Select one of the following:  
   a. **until**—if the policy is to be executed each time a matching event is received and stops being executed when the number of matching events received equals number.  
   b. **on**—if the policy is executed when the number of matching events received equals number.  
   c. **after**—if the policy is executed when the number of matching events received equals number + 1.  
13. From the **Count** list, select the number of times an event or set of events should occur within a specified time period. |

**Related Topics**
- Configuring Destinations for File Archiving (NSM Procedure) on page 151
- Configuring Event Script (NSM Procedure) on page 152
- Generating Internal Events (NSM Procedure) on page 154
- Configuring Event Policy Tracing Operations (NSM Procedure) on page 157

**Configuring Event Policy Tracing Operations (NSM Procedure)**

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

To configure event policy tracing operations in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Event Options**.
4. Select **Traceoptions**.
5. Add or modify settings as specified in Table 77 on page 158.

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

Table 77: Event Options Traceoptions Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define tracing operations for event policy.</td>
<td>1. In the Comment box, enter the comment for the traceoptions.</td>
</tr>
<tr>
<td></td>
<td>2. Select the No Remote Trace check box to disable remote tracing globally or for a specific tracing operation.</td>
</tr>
<tr>
<td>Specify the name of the file to receive the output of the tracing operation and the maximum number of trace files.</td>
<td>1. Click File next to Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>2. In the Comment box, enter the comment for the file.</td>
</tr>
<tr>
<td></td>
<td>3. In the Filename box, enter the name of the file to receive the output of the tracing operation.</td>
</tr>
<tr>
<td></td>
<td>4. In the Size box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).</td>
</tr>
<tr>
<td></td>
<td>5. From the Files list, select the maximum number of trace files. Range: 2 through 1000.</td>
</tr>
<tr>
<td></td>
<td>6. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• world-readable—To enable unrestricted file access.</td>
</tr>
<tr>
<td></td>
<td>• no-world-readable—To restrict file access to owner. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>7. In the Match box, enter the regular expression.</td>
</tr>
<tr>
<td>Specify the tracing operation to perform.</td>
<td>1. Click Flag next to Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>2. Click Add new entry next to Flag.</td>
</tr>
<tr>
<td></td>
<td>3. From the Name list, select the flag.</td>
</tr>
<tr>
<td></td>
<td>4. In the Comment box, enter the comment for the flag.</td>
</tr>
</tbody>
</table>

Related Topics

- Configuring Destinations for File Archiving (NSM Procedure) on page 151
- Configuring Event Script (NSM Procedure) on page 152
- Generating Internal Events (NSM Procedure) on page 154
- Configuring Event Policy (NSM Procedure) on page 154
CHAPTER 15

Configuring Firewall

- Configuring the Firewall Filter for Any Family Type (NSM Procedure) on page 159
- Configuring the Firewall Filter for Bridge Family Type (NSM Procedure) on page 161
- Configuring the Firewall Filter for Ccc Family Type (NSM Procedure) on page 163
- Configuring Filters for inet Family Type (NSM Procedure) on page 165
- Configuring Filters for inet6 Family Type (NSM Procedure) on page 170
- Configuring the Firewall Filter for MPLS Family Type (NSM Procedure) on page 174
- Configuring the Firewall Filter for VPLS Family Type (NSM Procedure) on page 177
- Configuring a Policer for a Firewall Filter on page 180

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

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

To configure firewall filter in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Firewall > Family > Any.
4. Add or modify settings as specified in Table 78 on page 160.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
Table 78: Firewall Filter Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure firewall filters for protocol-independent match conditions.</td>
<td>1. Expand Any.</td>
</tr>
<tr>
<td></td>
<td>2. In the Comment box, enter the comment for Any.</td>
</tr>
<tr>
<td></td>
<td>3. Click Filter next to Any.</td>
</tr>
<tr>
<td></td>
<td>4. Click Add new entry next to Filter.</td>
</tr>
<tr>
<td></td>
<td>5. In the name box, enter the name that identifies the filter.</td>
</tr>
<tr>
<td></td>
<td>6. In the Comment box, enter the comment for the filter.</td>
</tr>
<tr>
<td></td>
<td>7. Expand Filter.</td>
</tr>
<tr>
<td></td>
<td>8. Click Term next to Filter.</td>
</tr>
<tr>
<td></td>
<td>9. Click Add new entry next to Term.</td>
</tr>
<tr>
<td></td>
<td>10. Expand Term.</td>
</tr>
<tr>
<td></td>
<td>11. In the Name box, enter the name that identifies the term.</td>
</tr>
<tr>
<td></td>
<td>12. In the Comment box, enter the comment for the term.</td>
</tr>
<tr>
<td></td>
<td>13. Expand From.</td>
</tr>
<tr>
<td></td>
<td>14. From the listed protocol-independent match conditions, select the filters defined for the any family type.</td>
</tr>
<tr>
<td></td>
<td>The protocol-independent match conditions are Forwarding Class, Interface, Interface Set, Loss Priority, and Packet Length.</td>
</tr>
<tr>
<td></td>
<td>15. Expand Then.</td>
</tr>
<tr>
<td></td>
<td>16. In the Comment box, enter the comment for then.</td>
</tr>
<tr>
<td></td>
<td>17. In the Count box, enter the number of packets.</td>
</tr>
<tr>
<td></td>
<td>18. From the Loss Priority list, set the packet loss priority (PLP) to low, medium-low, medium-high, or high.</td>
</tr>
<tr>
<td></td>
<td>19. In the Forwarding Class box, enter the packet forwarding class name.</td>
</tr>
<tr>
<td></td>
<td>20. Click Accept next to Then.</td>
</tr>
<tr>
<td></td>
<td>21. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Accept—To accept a packet.</td>
</tr>
<tr>
<td></td>
<td>• Discard—To discard a packet silently, without sending an ICMP message.</td>
</tr>
<tr>
<td></td>
<td>• Next—To evaluate the next term in the firewall filter.</td>
</tr>
<tr>
<td></td>
<td>22. Click Policer next to Then.</td>
</tr>
<tr>
<td></td>
<td>23. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• policer—To configure a new policer for each filter and select the policer name.</td>
</tr>
<tr>
<td></td>
<td>• three-color-policer—To configure a tricolor marking policer.</td>
</tr>
<tr>
<td></td>
<td>a. Expand Three Color Policer.</td>
</tr>
<tr>
<td></td>
<td>b. Click Single Rate next to Three Color Policer.</td>
</tr>
<tr>
<td></td>
<td>c. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• single-rate—if the named tricolor policer is a single-rate policer.</td>
</tr>
<tr>
<td></td>
<td>• two-rate—if the named tricolor policer is a two-rate policer.</td>
</tr>
</tbody>
</table>

Related Topics  • Configuring the Firewall Filter for Bridge Family Type (NSM Procedure) on page 161
Configuring the Firewall Filter for Bridge Family Type (NSM Procedure)

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

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Firewall > Family > Bridge.
4. Add or modify settings as specified in Table 79 on page 161.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 79: Bridge Filter Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure firewall filters for Layer 2 packets that are part of bridging domain for MX series routers. | 1. Click Filter next to Bridge.  
2. Click Add new entry next to Filter.  
3. Expand Filter.  
4. In the name box, enter the name that identifies the filter.  
5. In the Comment box, enter the comment.  
6. Select Interface Specific to configure interface-specific names for firewall counters. |
| Configure accounting for firewall filter. | 1. Click Accounting Profile next to filter.  
2. In the New accounting-profile window, enter the name to be assigned to the accounting profile. |
Table 79: Bridge Filter Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Define a firewall filter term. | 1. Click **Add new entry** next to Term. 2. Expand **Term**. 3. In the **Name** box, enter the name that identifies the term. 4. In the **Comment** box, enter the comment for the term. 5. From the **Filter** list, select the name that identifies the filter. 6. Expand **From**. 7. In the **Comment** box, enter the comment. 8. In the **Tcp Flags** box, enter the Tcp flags. 9. From the listed protocol-independent match conditions, select the filters defined for the Bridge family type.  
   The protocol-independent match conditions are Destination Mac Address, Destination port, DSCP, Ether Type, Forwarding Class, ICMP Code, ICMP Type, Interface Group, Ip Address, Ip Destination Address, Ip Precedence, Ip Protocol, Ip Source Address, Learn Vlan 1p Priority, Learn Vlan Id, Loss priority, Port, Source Mac Address, Source Port, Traffic Type, User Vlan 1p Priority, User Vlan Id, and Vlan Ether Type. 10. Expand **Then**. 11. In the **Comment** box, enter the comment for then. 12. In the **Count** box, enter the number of packets. 13. From the **Loss Priority** list, set the packet loss priority (PLP) to low, medium-low, medium-high, or high. 14. In the **Forwarding Class** box, enter the packet forwarding class name. 15. Select **Port Mirror** check box to port mirror the packets. 16. Click **Accept** next to **Then**.  
   • Select **Accept** to accept a packet.  
   • Select **Discard** to discard a packet silently, without sending an ICMP message.  
   • Select **Next** to evaluate the next term in the firewall filter. 17. Click **Policer** next to **Then**. 18. Select one of the following:  
   • **Policer**—To configure a new policer for each filter and select the policer name.  
   • **three-color-policer**—To configure a tricolor marking policer,  
     a. Expand **Three Color Policer**.  
     b. Click **Single Rate** next to Three Color Policer.  
     c. Select one of the following:  
       • single-rate—if the named tricolor policer is a single-rate policer.  
       • two-rate—if the named tricolor policer is a two-rate policer. |

Related Topics  
- Configuring the Firewall Filter for Any Family Type (NSM Procedure) on page 159  
- Configuring the Firewall Filter for Ccc Family Type (NSM Procedure) on page 163
On the MX Series router, you can filter Layer 2 packets in a bridging environment using this option.

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Firewall > Family > Ccc**.
4. Add or modify settings as specified in Table 80 on page 163.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.

### Table 80: Ccc Filter Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure firewall filters for Layer 2 switching cross-connects. | 1. Click **Filter** next to Ccc.  
2. Click **Add new entry** next to Filter.  
3. Expand **Filter**.  
4. In the **name** box, enter the name that identifies the filter.  
5. In the **Comment** box, enter the comment.  
6. Select the **Interface Specific** check box to configure interface-specific names for firewall counters. |
| Configure accounting for firewall filter. | 1. Click **Accounting Profile** next to filter.  
2. Click **Add new entry** next to Accounting Profile.  
3. In the **New accounting-profile** window, enter the name to be assigned to the accounting profile. |
### Table 80: Ccc Filter Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Define a firewall filter term. | 1. Click **Term** next to Accounting Profile.  
2. Click **Add new entry** next to Term.  
3. Expand **Term**.  
4. In the **Name** box, enter the name that identifies the term.  
5. In the **Comment** box, enter the comment for the term.  
6. From the **Filter** list, select the name that identifies the filter.  
7. Expand **From**.  
8. In the **Comment** box, enter the comment.  
9. From the listed protocol-independent match conditions, select the filters defined for the Ccc family type. The protocol-independent match conditions are Forwarding Class, Interface Group, Vlan 1p property, Loss Priority, and User Vlan-1p Priority.  
10. Expand **Then**.  
11. In the **Comment** box, enter the comment for then.  
12. In the **Count** box, enter the number of packets.  
13. From the **Loss Priority** list, set the packet loss priority (PLP) to low, medium-low, medium-high, or high.  
14. In the **Forwarding Class** box, enter the packet forwarding class name.  
15. Click **Accept** next to Then.  
16. Select one of the following:  
   • **Accept**—To accept a packet.  
   • **Discard**—To discard a packet silently, without sending an ICMP message.  
   • **Next**—To evaluate the next term in the firewall filter.  
17. Click **Policer** next to Then.  
18. Select one of the following:  
   • **Policer**—To configure a new policer for each filter and select the policer name.  
   • **three-color-policer**—To configure a tricolor marking policer,  
     a. Expand **Three Color Policer**.  
     b. Click **Single Rate** next to Three Color Policer.  
     c. Select one of the following:  
        • **single-rate**—If the named tricolor policer is a single-rate policer.  
        • **two-rate**—If the named tricolor policer is a two-rate policer.  

**Related Topics**  
- Configuring the Firewall Filter for Bridge Family Type (NSM Procedure) on page 161  
- Configuring the Firewall Filter for MPLS Family Type (NSM Procedure) on page 174  
- Configuring the Firewall Filter for VPLS Family Type (NSM Procedure) on page 177
Configuring Filters for inet Family Type (NSM Procedure)

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

- Configuring Firewall Filter for inet Family Type (NSM Procedure) on page 165
- Configuring Prefix-specific Actions (NSM Procedure) on page 167
- Configuring Service Filters (NSM Procedure) on page 168
- Configuring Simple Filters (NSM Procedure) on page 169

Configuring Firewall Filter for inet Family Type (NSM Procedure)

You can configure a firewall filter for inet family type.

To configure the firewall filter in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Firewall > Family > Inet.
4. Select Filter.
5. Add or modify settings as specified in Table 81 on page 165.
6. Click one:
   1. OK—Saves the changes.
   2. Cancel— Cancels the modifications.

Table 81: Firewall Filter Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure a firewall filter to filter IPv4 packets. | 1. Expand Inet.  
  2. Click Filter next to Inet.  
  3. Click Add new entry next to Filter.  
  4. Expand Filter.  
  5. In the name box, enter the name that identifies the filter.  
  6. In the Comment box, enter the comment.  
  7. Select the Interface Specific check box to configure interface-specific names for firewall counters. |
| Configure accounting for firewall filters. | 1. Click Accounting Profile next to filter.  
  2. Click Add new entry next to Accounting Profile.  
  3. In the New accounting-profile window, enter the name to be assigned to the accounting profile. |
Table 81: Firewall Filter Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define firewall filter term.</td>
<td>1. Click <strong>Term</strong> next to Accounting Profile.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Term.</td>
</tr>
<tr>
<td></td>
<td>3. Expand <strong>Term</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Name</strong> box, enter the name that identifies the term.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment for the term.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Filter</strong> list, select the name that identifies the filter.</td>
</tr>
<tr>
<td></td>
<td>7. Expand <strong>From</strong>.</td>
</tr>
<tr>
<td></td>
<td>8. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>9. Select the <strong>Is Fragment</strong> check box if the packet is a trailing fragment.</td>
</tr>
<tr>
<td></td>
<td>10. Select the <strong>First Fragment</strong> check box if it matches the first fragment of a fragmented packet.</td>
</tr>
<tr>
<td></td>
<td>11. In the <strong>Fragment Flags</strong> box, enter the IP fragmentation flags.</td>
</tr>
<tr>
<td></td>
<td>12. Select the <strong>Tcp initial</strong> check box if it matches the first TCP packet of a connection.</td>
</tr>
<tr>
<td></td>
<td>13. Select the <strong>Tcp established</strong> check box if it matches the TCP packets other than the first packet of a connection.</td>
</tr>
<tr>
<td></td>
<td>14. In the <strong>Tcp Flags</strong> box, enter the TCP flags.</td>
</tr>
<tr>
<td></td>
<td>15. From the listed protocol-independent match conditions, select the filters defined for the Inet family type. The protocol-independent match conditions are Address, Ah Spi, Destination Address, Destination Class, Destination port, Destination prefix List, Dscp, Esp Spi, Forwarding Class, Fragment offset, Icmp Code, Icmp Type, Interface, Interface Group, Interface Set, Ip Options, Loss Priority, Packet Length, Port, Precedence, prefix List, Protocol, Source Address, Source Port, Source Prefix List and Ttl.</td>
</tr>
<tr>
<td></td>
<td>16. Expand <strong>Then</strong>.</td>
</tr>
<tr>
<td></td>
<td>17. In the <strong>Comment</strong> box, enter the comment for then.</td>
</tr>
<tr>
<td></td>
<td>18. In the <strong>Count</strong> box, enter the number of packets.</td>
</tr>
<tr>
<td></td>
<td>19. Select the <strong>Log</strong> check box to store the header information of a packet on the Routing Engine.</td>
</tr>
<tr>
<td></td>
<td>20. Select <strong>Syslog</strong> to log an alert for the packet.</td>
</tr>
<tr>
<td></td>
<td>21. Select the <strong>Sample</strong> check box to sample the packet traffic.</td>
</tr>
<tr>
<td></td>
<td>22. Select the <strong>Port Mirror</strong> check box to port-mirror the packets.</td>
</tr>
<tr>
<td></td>
<td>23. From the <strong>Loss Priority</strong> list, set the packet loss priority (PLP) to low, medium-low, medium-high, or high.</td>
</tr>
<tr>
<td></td>
<td>24. In the <strong>Forwarding Class</strong> box, enter the packet forwarding class name.</td>
</tr>
<tr>
<td></td>
<td>25. From the <strong>Prefix Action</strong> list, select the prefix specific action.</td>
</tr>
</tbody>
</table>
Table 81: Firewall Filter Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>26.</td>
<td>Click <strong>Accept</strong> next to Then.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Accept</strong> to accept a packet.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Discard</strong> to discard a packet silently, without sending an ICMP message.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Next</strong> to evaluate the next term in the firewall filter.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Routing instance</strong> to specify a routing table to which packets are forwarded.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>IPsec Sa</strong> to specify an IP Security (IPsec) security association (SA) for the packet.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Reject</strong> to discard a packet, and send an ICMP destination unreachable message.</td>
</tr>
<tr>
<td>27.</td>
<td>Click <strong>Policer</strong> next to Then.</td>
</tr>
<tr>
<td>28.</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Policer</strong> to configure a new policer for each filter and select the policer name.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>three-color-policer</strong> to configure a tricolor marking policer,</td>
</tr>
<tr>
<td></td>
<td>a. Expand <strong>Three Color Policer</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. Click <strong>Single Rate</strong> next to Three Color Policer.</td>
</tr>
<tr>
<td></td>
<td>c. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>single-rate</strong>—If the named tricolor policer is a single-rate policer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>two-rate</strong>—If the named tricolor policer is a two-rate policer.</td>
</tr>
</tbody>
</table>

Configuring Prefix-specific Actions (NSM Procedure)

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

To configure the prefix-specific actions in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Firewall > Family > Inet**.
4. Click **Prefix Action**.
5. Add or modify settings as specified in Table 82 on page 168.
6. Click one:
   • **OK**—Saves the changes.
   • **Cancel**—Cancels the modifications.
Table 82: Prefix Actions Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure prefix-specific actions.</td>
<td>1. Click <strong>Prefix Action</strong> next to Inet.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Name</strong> box, enter the action name.</td>
</tr>
<tr>
<td></td>
<td>3. From the <strong>Policer</strong> list, select the actions to be taken.</td>
</tr>
<tr>
<td></td>
<td>4. Select the <strong>Count</strong> check box to include count as the action modifier.</td>
</tr>
<tr>
<td></td>
<td>5. Select the <strong>Filter Specific</strong> check box to configure a policer to act as a filter-specific policer.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Subnet Prefix Length</strong> list, select the subnet prefix length.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 to 32</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>Source Prefix Length</strong> next to prefix-action.</td>
</tr>
<tr>
<td></td>
<td>8. Select <strong>source-prefix-length</strong> to configure the source address range specified for a prefix-specific policer or counter and select the source prefix length.</td>
</tr>
<tr>
<td></td>
<td>9. Select <strong>destination-prefix-length</strong> to configure the destination address range specified for a prefix-specific policer or counter and select the destination prefix length.</td>
</tr>
</tbody>
</table>

Configuring Service Filters (NSM Procedure)

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

To configure the service filters for inet in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Firewall > Family > Inet**.
4. Click **Prefix Action**.
5. Add or modify settings as specified in Table 83 on page 168.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 83: Service Filter Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure service filter.</td>
<td>1. Click <strong>Service Filter</strong> next to Inet.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Service Filter.</td>
</tr>
<tr>
<td></td>
<td>3. Expand <strong>service-filter</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Name</strong> box, enter the name that identifies the service filter.</td>
</tr>
</tbody>
</table>
Table 83: Service Filter Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Define firewall filter term. | 1. Click Term next to service-filter.  
2. Click Add new entry next to Term.  
3. Expand Term.  
4. In the Name box, enter the name that identifies the term.  
5. In the Comment box, enter the comment for the term.  
6. Expand From.  
7. In the Comment box, enter the comment.  
8. Check the Is Fragment check box if the packet is a trailing fragment.  
9. Check the First Fragment check box if it matches the first fragment of a fragmented packet.  
10. In the Fragment Flags box, enter the IP fragmentation flags.  
11. From the listed protocol-independent match conditions, select the filters defined for the Inet family type.  
The protocol-independent match conditions are Address, Ah Spi, Destination Address, Destination port, Destination prefix List, Esp Spi, Fragment offset, Interface Group, , Ip Options, Loss Priority, Port, Prefix List, Protocol, Source Address, Source Port, and Source Prefix List.  
12. Click Then next to From.  
13. In the Comment box, enter the comment for then.  
14. In the Count box, enter the number of packets.  
15. Select the Log check box to store the header information of a packet on the Routing Engine.  
16. Select the Sample check box to sample the packet traffic.  
17. Select the Port Mirror check box to port-mirror the packets.  
18. Select Service to direct packets for stateful-firewall service.  
19. Select Skip to let packets bypass stateful-firewall service. |

Configuring Simple Filters (NSM Procedure)

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

- The next-term action is not supported.
- The except and protocol-except match conditions are not supported.
- Noncontiguous masks are not supported.
- Only one source-address and one destination-address prefix are allowed for each filter term.
To configure the simple filters for inet in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Firewall > Family > Inet**.
4. Select **Simple Filters**.
5. Add or modify settings as specified in Table 84 on page 170.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

### Table 84: Simple Filter Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure simple filter.</td>
<td>1. Click <strong>Simple Filter</strong> next to Inet.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Simple Filter.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the name that identifies the simple filter.</td>
</tr>
<tr>
<td>Define a term.</td>
<td>1. Click <strong>Term</strong> next to simple-filter.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Term.</td>
</tr>
<tr>
<td></td>
<td>3. Expand <strong>Term</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Name</strong> box, enter the name that identifies the term.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. Expand <strong>From</strong>.</td>
</tr>
<tr>
<td></td>
<td>7. From the listed protocol-independent match conditions, select the filters defined for the Inet family type.</td>
</tr>
<tr>
<td></td>
<td>The protocol-independent match conditions are Destination Address, Destination port, Forwarding Class, Protocol, Source Address, and Source Port.</td>
</tr>
<tr>
<td></td>
<td>8. Click <strong>Then</strong> next to From.</td>
</tr>
<tr>
<td></td>
<td>9. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>10. From the <strong>Loss Priority</strong> list, select the packet loss priority (PLP) level to set it as low, medium-low, medium-high, or high.</td>
</tr>
<tr>
<td></td>
<td>11. In the <strong>Forwarding Class</strong> box, enter the packet forwarding class name.</td>
</tr>
</tbody>
</table>

### Configuring Filters for inet6 Family Type (NSM Procedure)

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

- Configuring Firewall Filter for inet6 Family Type (NSM Procedure) on page 171
- Configuring Service Filters for inet6 (NSM Procedure) on page 173
Configuring Firewall Filter for inet6 Family Type (NSM Procedure)

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

To configure the firewall filter in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Firewall > Family > Inet6.
4. Add or modify settings as specified in Table 85 on page 171.
5. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

Table 85: Inet6 Firewall Filter Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure firewall filter to</td>
<td>1. Click Filter next to Inet6.</td>
</tr>
<tr>
<td>filter IPv6 packets.</td>
<td>2. Click Add new entry next to Filter.</td>
</tr>
<tr>
<td></td>
<td>3. Expand Filter.</td>
</tr>
<tr>
<td></td>
<td>4. In the Name box, enter the name that identifies the filter.</td>
</tr>
<tr>
<td></td>
<td>5. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. Select the Interface Specific check box to configure</td>
</tr>
<tr>
<td></td>
<td>interface-specific names for firewall counters.</td>
</tr>
</tbody>
</table>

| Configure accounting for     | 1. Click Accounting Profile next to filter.                                 |
| firewall filters.            | 2. Click Add new entry next to Accounting Profile.                         |
|                               | 3. In the New accounting-profile window, enter the name to be assigned to  |
|                               | the accounting profile.                                                    |
Table 85: Inet6 Firewall Filter Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define firewall filter term.</td>
<td>1. Click Term next to Accounting Profile.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>2. Click Add new entry next to Term.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>3. Expand Term.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>4. In the Name box, enter the name that identifies the term.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>5. In the Comment box, enter the comment for the term.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>6. From the Filter list, select the name that identifies the filter.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>7. Expand From.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>8. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>9. Select the Tcp initial check box if it matches the first TCP packet of a connection.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>10. Select the Tcp established check box if it matches the TCP packets other than the first packet of a connection.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>11. In the Tcp Flags box, enter the TCP flags.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>12. From the listed protocol-independent match conditions, select the filters defined for the inet family type.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>The protocol-independent match conditions are Address, Destination Address, Destination Class, Destination port, Destination prefix List, Dscp, Forwarding Class, Fragment offset, Icmp Code, Icmp Type, Interface, Interface Group, Interface Set, Ip Options, Loss Priority, Packet Length, Port, prefix List, Protocol, Source Address, Source Port, Source Prefix List, and traffic list.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>13. Expand Then.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>14. In the Comment box, enter the comment for then.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>15. In the Count box, enter the number of packets.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>16. Select the Log check box to store the header information of a packet on the Routing Engine.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>17. Select the Syslog check box to log an alert for the packet.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>18. Select the Sample check box to sample the packet traffic.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>19. Select the Port Mirror check box to port-mirror the packets.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>20. From the Loss Priority list, set the packet loss priority (PLP) to low, medium-low, medium-high, or high.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>21. In the Forwarding Class box, enter the packet forwarding class name.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>22. From the Prefix Action list, select the prefix specific action.</td>
</tr>
</tbody>
</table>
Table 85: Inet6 Firewall Filter Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>23.</td>
<td>Click <strong>Accept</strong> next to Then.</td>
</tr>
<tr>
<td>24.</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Accept</strong>—To accept a packet.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Discard</strong>—To discard a packet silently, without sending an ICMP message.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Next</strong>—To evaluate the next term in the firewall filter.</td>
</tr>
<tr>
<td>25.</td>
<td>Click <strong>Policer</strong> next to Then.</td>
</tr>
<tr>
<td>26.</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>policer</strong>—To configure a new policer for each filter and select the policer name.</td>
</tr>
<tr>
<td></td>
<td>• <strong>three-color-policer</strong>—To configure a tricolor marking policer,</td>
</tr>
<tr>
<td></td>
<td>a.  Expand <strong>Three Color Policer</strong>.</td>
</tr>
<tr>
<td></td>
<td>b.  Click <strong>Single Rate</strong> next to Three Color Policer.</td>
</tr>
<tr>
<td></td>
<td>c.  Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>single-rate</strong> if the named tricolor policer is a single-rate policer.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>two-rate</strong> if the named tricolor policer is a two-rate policer.</td>
</tr>
</tbody>
</table>

Configuring Service Filters for inet6 (NSM Procedure)

To configure the service filters for inet6 in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.  
2. Click the **Device Tree** tab, and then double-click the device to select it.  
3. Click the **Configuration** tab. In the configuration tree, expand **Firewall > Family > Inet6**.  
4. Add or modify settings as specified in Table 86 on page 173.  
5. Click one:  
   • **OK**—Saves the changes.  
   • **Cancel**—Cancels the modifications.  

Table 86: inet6 Service Filter Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure service filter.</td>
<td>1. Click <strong>Service Filter</strong> next to inet.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Service Filter.</td>
</tr>
<tr>
<td></td>
<td>3. Expand <strong>service-filter</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Name</strong> box, enter the name that identifies the service filter.</td>
</tr>
</tbody>
</table>
Table 86: inet6 Service Filter Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define term.</td>
<td>1. Click Term next to service-filter.</td>
</tr>
<tr>
<td></td>
<td>2. Click Add new entry next to Term.</td>
</tr>
<tr>
<td></td>
<td>3. Expand Term.</td>
</tr>
<tr>
<td></td>
<td>4. In the Name box, enter the name that identifies the term.</td>
</tr>
<tr>
<td></td>
<td>5. In the Comment box, enter the comment for the term.</td>
</tr>
<tr>
<td></td>
<td>6. Expand From.</td>
</tr>
<tr>
<td></td>
<td>7. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>8. From the listed protocol-independent match conditions, select the filters defined for the inet6 family type.</td>
</tr>
<tr>
<td></td>
<td>The protocol-independent match conditions are Address, Ah Spi, Destination Address, Destination port, Destination prefix List, interface Group, Next Header, Interface Set, Ip Options, Loss Priority, Port, Prefix List, Protocol, Source Address, Source Port, Source Prefix List, and Esp spi.</td>
</tr>
<tr>
<td></td>
<td>9. Click Then next to From.</td>
</tr>
<tr>
<td></td>
<td>10. In the Comment box, enter the comment for then.</td>
</tr>
<tr>
<td></td>
<td>11. In the Count box, enter the number of packets.</td>
</tr>
<tr>
<td></td>
<td>12. Select the Log check box to store the header information of a packet on the Routing Engine.</td>
</tr>
<tr>
<td></td>
<td>13. Select the Sample check box to sample the packet traffic.</td>
</tr>
<tr>
<td></td>
<td>14. Select the Port Mirror check box to port-mirror the packets.</td>
</tr>
<tr>
<td></td>
<td>15. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• service—To direct packets for stateful-firewall service.</td>
</tr>
<tr>
<td></td>
<td>• skip—To let packets bypass stateful-firewall service.</td>
</tr>
</tbody>
</table>

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

You can configure firewall filters to filter MPLS packets.

To configure the MPLS firewall filter in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Firewall > Family > MPLS.
4. Add or modify settings as specified in Table 87 on page 175.
5. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.
Table 87: MPLS Firewall Filter Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure a firewall filter to filter MPLS packets. | 1. Click **Filter** next to MPLS.  
2. Click **Add new entry** next to Filter.  
3. Expand **Filter**.  
4. In the **Name** box, enter the name that identifies the filter.  
5. In the **Comment** box, enter the comment.  
6. Select the **Interface Specific** check box to configure interface-specific names for firewall counters. |
| Configure accounting for firewall filters. | 1. Click **Accounting Profile** next to filter.  
2. Click **Add new entry** next to Accounting Profile.  
3. In the **New accounting-profile** window, enter the name to be assigned to the accounting profile. |
Table 87: MPLS Firewall Filter Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Define a firewall filter term. | 1. Click Term next to Accounting Profile.  
2. Click Add new entry next to Term.  
3. Expand Term.  
4. In the Name box, enter the name that identifies the term.  
5. In the Comment box, enter the comment for the term.  
6. From the Filter list, select the name that identifies the filter.  
7. Expand From.  
8. In the Comment box, enter the comment.  
9. From the listed protocol-independent match conditions, select the filters defined for the MPLS family type.  
   The protocol-independent match conditions are Exp, Forwarding Class, Interface, Interface Set, and Loss Priority.  
10. Expand Then.  
11. In the Comment box, enter the comment for then.  
12. In the Count box, enter the number of packets.  
13. Select the Sample check box to sample the packet traffic.  
14. From the Loss Priority list, set the packet loss priority (PLP) to low, medium-low, medium-high, or high.  
15. In the Forwarding Class box, enter the packet forwarding class name.  
16. Click Accept next to Then.  
17. Select one of the following:  
   • Select Accept to accept a packet.  
   • Select Discard to discard a packet silently, without sending an ICMP message.  
   • Select Next to evaluate the next term in the firewall filter.  
18. Click Policer next to Then.  
19. Select one of the following:  
   • Policer—To configure a new policer for each filter and select the policer name.  
   • Select three-color-policer—To configure a tricolor marking policer,  
     a. Expand Three Color Policer.  
     b. Click Single Rate next to Three Color Policer.  
     c. Select one of the following:  
        • single-rate—If the named tricolor policer is a single-rate policer.  
        • two-rate—If the named tricolor policer is a two-rate policer.

Related Topics  
• Configuring the Firewall Filter for Any Family Type (NSM Procedure) on page 159  
• Configuring Filters for inet Family Type (NSM Procedure) on page 165  
• Configuring Filters for inet6 Family Type (NSM Procedure) on page 170
Configuring the Firewall Filter for VPLS Family Type (NSM Procedure)

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

To configure the vpls firewall filter in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Firewall > Family > VPLS.
4. Add or modify settings as specified in Table 88 on page 178.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
Configure a firewall filter to filter VPLS packets.

1. Click **Filter** next to VPLS.
2. Click **Add new entry** next to Filter.
3. Expand **Filter**.
4. In the **Name** box, enter the name that identifies the filter.
5. In the **Comment** box, enter the comment.
6. Select the **Interface Specific** check box to configure interface-specific names for firewall counters.

Configure accounting for firewall filters.

1. Click **Accounting Profile** next to filter.
2. Click **Add new entry** next to Accounting Profile.
3. In the **New accounting-profile** window, enter the name to be assigned to the accounting profile.

---

**Table 88: VPLS Firewall Filter Configuration Details**

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a firewall filter to filter VPLS packets.</td>
<td>1. Click <strong>Filter</strong> next to VPLS.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Filter.</td>
</tr>
<tr>
<td></td>
<td>3. Expand <strong>Filter</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Name</strong> box, enter the name that identifies the filter.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. Select the <strong>Interface Specific</strong> check box to configure interface-specific names for firewall counters.</td>
</tr>
<tr>
<td>Configure accounting for firewall filters.</td>
<td>1. Click <strong>Accounting Profile</strong> next to filter.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Accounting Profile.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>New accounting-profile</strong> window, enter the name to be assigned to the accounting profile.</td>
</tr>
</tbody>
</table>
Table 88: VPLS Firewall Filter Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Define a firewall filter term. | 1. Click **Term** next to Accounting Profile.  
2. Click **Add new entry** next to Term.  
3. Expand **Term**.  
4. In the **Name** box, enter the name that identifies the term.  
5. In the **Comment** box, enter the comment for the term.  
6. From the **Filter** list, select the name that identifies the filter.  
7. Expand **From**.  
8. In the **Comment** box, enter the comment.  
9. From the listed protocol-independent match conditions, select the filters defined for the VPLS family type.  
The protocol-independent match conditions are: Destination Mac Address, Destination Port, Dscp, Ether Type, Forwarding Class, Icmp Code, Icmp Type, Interface Group, Ip Adress, Ip Destination Address, Ip Precedence, Ip Protocol, Ip Source Address, Learn Vlan, Ip Priority, Learn Vlan id, Loss Priority, Port, Source Mac Address, Source Port, Traffic Type, User Vlan 1p priority, User Vlan id, Vlan Ether Type.  
10. Expand **Then**.  
11. In the **Comment** box, enter the comment for then.  
12. In the **Count** box, enter the number of packets.  
13. Select the **Sample** check box to sample the packet traffic.  
14. From the **LossPriority** list, set the packet loss priority (PLP) to low, medium-low, medium-high, or high.  
15. In the **Forwarding Class** box, enter the packet forwarding class name.  
16. Select the **Port Mirror** check box to configure port mirroring for VPLS traffic.  
17. Click **Accept** next to Then.  
18. Select one of the following:  
   - **Accept**—To accept a packet.  
   - **Discard**—To discard a packet silently, without sending an ICMP message.  
   - **Next**—To evaluate the next term in the firewall filter.  
19. Click **Policer** next to Then.  
20. Select one of the following:  
   - **Policer**—To configure a new policer for each filter and select the policer name.  
   - **three-color-policer**—To configure a tricolor marking policer,  
a. Expand **Three Color Policer**.  
b. Click **Single Rate** next to Three Color Policer.  
c. Select one of the following:  
   - **single-rate**—If the named tricolor policer is a single-rate policer.  
   - **two-rate**—If the named tricolor policer is a two-rate policer.
You can configure policers to rate limit traffic on a device. After you configure a policer, you can include it in an ingress firewall filter configuration.

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

The following policer limits apply on the switch:

- A maximum of 512 policers can be configured for port firewall filters.
- A maximum of 512 policers can be configured for VLAN and Layer 3 firewall filters.

1. In the navigation tree, select Device Manager > Devices. In Device Manager, select the device for which you want to configure a policer.
2. In the configuration tree, expand Firewall.
3. Perform the configuration tasks as described in Table 89 on page 180.

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

### Table 89: Configuring a Policer for a Firewall Filter

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

Related Topics

- Configuring the Firewall Filter for Any Family Type (NSM Procedure) on page 159
- Configuring the Firewall Filter for Ccc Family Type (NSM Procedure) on page 163
- Configuring the Firewall Filter for MPLS Family Type (NSM Procedure) on page 174
Table 89: Configuring a Policer for a Firewall Filter (continued)

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

1. Select Then.
2. In the Comment field, enter high.
3. Click OK.
CHAPTER 16

Configuring Forwarding Options

- Configuring Accounting Options (NSM Procedure) on page 183
- Configuring the Extended DHCP Agent (NSM Procedure) on page 185
- Specifying Address Family for Filters (NSM Procedure) on page 193
- Configuring Load Balancing Using Hash Key (NSM Procedure) on page 194
- Configuring Helpers (NSM Procedure) on page 195
- Configuring Per-Flow and Per-Prefix Load Balancing (NSM Procedure) on page 203
- Configuring Port Mirroring (NSM Procedure) on page 204

Configuring Accounting Options (NSM Procedure)

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

To configure an accounting group in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Forwarding Options.
4. Select Accounting.
5. Add or modify the settings as specified in Table 90 on page 183.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 90: Accounting Options Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure an accounting group.</td>
<td>1. Click Add new entry next to Accounting.</td>
</tr>
</tbody>
</table>
Table 90: Accounting Options Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure flow output.                    | 1. Expand Output.  
2. In the Comment box, enter the comment for the output.  
3. From the Aggregate export interval list, select the time.  
4. From the Flow Inactive Timeout list, select the interval before a flow is considered inactive.  
5. From the Flow Active Timeout list, select the interval before exporting an active flow. |
| Configure flow aggregation.              | 1. Click Add new entry next to cflowd.  
2. In the Name box, Enter the IP address or identifier of the host system (the workstation running the cflowd utility).  
3. From the Port list, select the UDP port number on the cflowd host system.  
4. From the Version list, select the version format of the aggregated flows exported to a cflowd server.  
5. From the Autonomous System Type, select the type of AS numbers that cflowd exports.  
   • origin—Export origin AS numbers of the packet source address in the Source Autonomous System cflowd field.  
   • peer—Export peer AS numbers through which the packet passed in the Source Autonomous System cflowd field. Default: origin  
6. Click Aggregation next to cflowd.  
7. Select Autonomous System check box to aggregate by autonomous system (AS) type.  
8. Select the Protocol Port check box to aggregate by protocol and port number.  
9. Select the Source Prefix check box to aggregate by source prefix.  
10. Select the Destination Prefix check box to aggregate by destination prefix.  
11. Expand Aggregation.  
12. Click Source Destination Prefix next to Aggregation.  
13. Select the Caida Compliant check box to record source and destination mask length values in compliance with the Version 2.1b1 release of the cflowd application from the Cooperative Association for Internet Data Analysis (CAIDA). |
| Configure the output interface.           | 1. Expand Output.  
2. Click Interface next to Output.  
3. Click Add new entry next to Interface.  
4. In the Name box, enter the name of the accounting interfaces.  
5. In the Comment box, enter the comment for the interface.  
6. From the Engine Id list, select the identity of the accounting interface.  
7. From the Engine Type list, select the type of this accounting interface.  
8. In the Source Address box, enter the address used for generating packets. |
Configuring the Extended DHCP Agent (NSM Procedure)

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

- Configuring Authentication Support for the DHCP Relay Agent (NSM Procedure) on page 185
- Configuring Group (NSM Procedure) on page 186
- Overriding the Default Configuration Settings for the Extended DHCP Relay Agent (NSM Procedure) on page 187
- Configuring Relay Option 60 Information for Forwarding Client Traffic to Specific DHCP Servers (NSM Procedure) on page 189
- Configuring Relay Option 82 for a DHCP Server (NSM Procedure) on page 190
- Specifying the Name of a Group of DHCP Server Addresses for Use by the Extended DHCP Relay Agent (NSM Procedure) on page 191
- Configuring Operations for Extended DHCP Relay Agent Processes (NSM Procedure) on page 192

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

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

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Forwarding Options > DHCP Relay.
4. Select Authentication.
5. Add or modify Authentication settings as specified in Table 91 on page 186.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.
### Table 91: Authentication Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the password</td>
<td>1. Expand Authentication.</td>
</tr>
<tr>
<td></td>
<td>2. In the Comment box, enter the comment for authentication.</td>
</tr>
<tr>
<td></td>
<td>3. In the Password box, enter the password to be sent to the external AAA authentication server for subscriber authentication.</td>
</tr>
<tr>
<td>Configure the username</td>
<td>1. Click Username Include next to Authentication.</td>
</tr>
<tr>
<td></td>
<td>2. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. In the Delimiter box, enter the character used as the delimiter between the concatenated components of the username. You cannot use the semicolon (;) as a delimiter.</td>
</tr>
<tr>
<td></td>
<td>4. In the Domain Name box, enter the domain name that is concatenated with the username during the subscriber authentication process.</td>
</tr>
<tr>
<td></td>
<td>5. In the User prefix box, enter the user prefix concatenated with the username during the subscriber authentication process.</td>
</tr>
<tr>
<td></td>
<td>• Select Mac Address check box if the MAC address from the client PDU be concatenated with the username during the subscriber authentication process.</td>
</tr>
<tr>
<td></td>
<td>• Select Logical System Name check box if the logical system name be concatenated with the username during the subscriber authentication process.</td>
</tr>
<tr>
<td></td>
<td>• Select Routing Instance Name check box if the routing instance name be concatenated with the username during the subscriber authentication process.</td>
</tr>
<tr>
<td></td>
<td>• Select Option 60 check box if the payload of the Option 60 (Vendor Class Identifier) from the client PDU be concatenated with the username during the subscriber authentication process.</td>
</tr>
<tr>
<td></td>
<td>• Select Circuit Type check box if the circuit type be concatenated with the username during the subscriber authentication process.</td>
</tr>
<tr>
<td></td>
<td>6. Click Option 82 next to Username Include.</td>
</tr>
<tr>
<td></td>
<td>7. Select the Circuit-id or remote id check box to select the string for the agent circuit ID suboption.</td>
</tr>
</tbody>
</table>

### Configuring Group (NSM Procedure)

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

To configure group of interfaces:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Forwarding Options > DHCP Relay.
5. Add or modify settings as specified in Table 92 on page 187.

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

### Table 92: Group Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring authentication support for the DHCP relay agent.</td>
<td>See “Configuring Authentication Support for the DHCP Relay Agent (NSM Procedure)” on page 185</td>
</tr>
<tr>
<td>Specify one or more interfaces, or a range of interfaces, that are</td>
<td>1. Click Add new entry next to Group.</td>
</tr>
<tr>
<td>within a specified group on which the DHCP local server is enabled.</td>
<td>2. Expand Group.</td>
</tr>
<tr>
<td>3. Click Interface next to group.</td>
<td>4. Click Add new entry next to Interface.</td>
</tr>
<tr>
<td>4. From the Name list, select the name of the interface.</td>
<td>5. From the Name list, select the name of the interface.</td>
</tr>
<tr>
<td>5. In the Comment box, enter the comment.</td>
<td>6. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td>6. From the Upto list, select the upper end of the range of</td>
<td>7. From the Upto list, select the upper end of the range of interfaces.</td>
</tr>
<tr>
<td>interfaces.</td>
<td>8. Select the Exclude check box to exclude an interface or a range of interfaces from the group.</td>
</tr>
</tbody>
</table>

Overriding the default configuration settings for the extended DHCP relay agent.
See “Overriding the Default Configuration Settings for the Extended DHCP Relay Agent (NSM Procedure)” on page 187.

Configuring relay option 60 Information for forwarding client traffic to specific DHCP servers.
See “Configuring Relay Option 60 Information for Forwarding Client Traffic to Specific DHCP Servers (NSM Procedure)” on page 189.

Configuring relay option 82 for a DHCP server.
See “Configuring Relay Option 82 for a DHCP Server (NSM Procedure)” on page 190.

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

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

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, select Forwarding Options > DHCP Relay.
4. Select Overrides.
5. Add or modify settings as specified in Table 93 on page 188.

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

Table 93: Overrides Configuration Details

<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 override.</td>
<td>In the Comment box, enter the comment.</td>
</tr>
<tr>
<td>always-write-giaddr</td>
<td>Overwrites the gateway IP address (giaddr) of every DHCP packet with the gateway IP address of the DHCP relay agent before forwarding the packet to the DHCP server.</td>
<td>Select the Always Write Giaddr check box.</td>
</tr>
<tr>
<td>always-write-option-82</td>
<td>Overrides the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server.</td>
<td>Select the Always Write Option 82 check box.</td>
</tr>
<tr>
<td>layer2-unicast-replies</td>
<td>Overrides the setting of the broadcast bit in DHCP request packets and instead use the Layer 2 unicast transmission method to transmit DHCP Offer reply packets and DHCP ACK reply packets from the DHCP server to DHCP clients during the discovery process.</td>
<td>Select the Layer2 Unicast Replies check box.</td>
</tr>
<tr>
<td>trust-option-82</td>
<td>Enables processing of DHCP client packets that have a gateway IP address (giaddr) of 0 (zero) and contain option 82 information.</td>
<td>Select the Trust Option 82 check box.</td>
</tr>
<tr>
<td>disable-relay</td>
<td>Disables DHCP relay on specific interfaces in a group.</td>
<td>Select the disable-relay check box.</td>
</tr>
<tr>
<td>Interface client limit</td>
<td>Specifies the interface client limit.</td>
<td>From the Interface Client Limit list, select the interface client limit.</td>
</tr>
<tr>
<td>No Arp</td>
<td>Disable Address Resolution Protocol entry for this client.</td>
<td>Select the No Arp check box to drop the unwanted ARP requests.</td>
</tr>
</tbody>
</table>
Configuring Relay Option 60 Information for Forwarding Client Traffic to Specific DHCP Servers (NSM Procedure)

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

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the tree, expand **Forwarding Options > DHCP Relay**.
4. Select **Relay Option 60**.
5. Add or modify settings as specified in Table 94 on page 189.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

### Table 94: Relay Option 60 Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure the match criteria when you use the DHCP vendor class identifier option (option 60) in DHCP client packets to forward client traffic to specific DHCP servers. | 1. In the **Comment** box, enter the comment for the relay option 60.  
2. Click **Vendor Option** next to Relay Option 60.  
3. In the **Comment** box, enter the comment for Vendor Option.  
4. Click **Default Relay Server Group** next to Vendor Option and select the name of the default DHCP relay server group.  
   - Select **Drop** to drop DHCP client packets that contain an option 60 string that matches the ASCII or hexadecimal match string and match criteria. |
Table 94: Relay Option 60 Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure the match string using the Equals and Starts With options. | 1. Expand **Equals** and **Starts With** next to Default Relay Server Group.  
2. Click **Add new entry** next to Equals and Starts With.  
3. Expand ascii.  
4. In the **name** box, enter the ASCII match string of 1 through 255 alphanumeric characters.  
5. Click **Relay Server Group** next to ascii.  
6. In the **Comment** box, enter the comment for the ASCII.  
7. Select the name of the extended DHCP local server group and enter the group name in the box.  
   - Select **Drop** to drop DHCP client packets that contain an option 60 string that matches the ASCII or hexadecimal match string and match criteria.  
8. Click **Hexadecimal** next to ascii.  
9. Click **Add new entry** next to Hexadecimal.  
10. Expand hexadecimal.  
11. In the **Name** box, enter the Hexadecimal match string.  
12. Click **Relay Server Group** next to ascii.  
13. In the **Comment** box, enter the comment for the ASCII.  
14. Select the name of the extended DHCP local server group and enter the group name in the box.  
   - Select **Drop** to drop DHCP client packets that contain an option 60 string that matches the ASCII or hexadecimal match string and match criteria. |

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

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

1. In the NSM navigation tree, select **Device Manager > Devices**.  
2. Click the **Device Tree** tab, and then double-click the device to select it.  
3. Click the **Configuration** tab. In the configuration tree, expand **Forwarding Options > DHCP Relay**.  
4. Select **Relay Option 82**.  
5. Add or modify settings as specified in Table 95 on page 191.  
6. Click one:  
   - **OK**—Saves the changes.  
   - **Cancel**—Cancels the modifications.
Table 95: Relay option 82 Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Enable or disable the insertion of the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server | 1. Expand Relay Option 82.  
2. In the Comment box, enter the comment for the relay option 82.  
3. Click Circuit Id next to Relay Option 82.  
4. In the Comment box, enter the comment.  
5. Click Prefix next to Circuit Id.  
6. In the Comment box, enter the comment.  
7. Select the prefix to be added to the base option 82 agent circuit ID information in DHCP packets destined for a DHCP server. The prefix can consist of any combination of the hostname, logical system name, and routing instance name. |

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

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

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Forwarding Options > DHCP Relay.
5. Add or modify settings as specified in Table 96 on page 192.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
### Table 96: Sever Group Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify the name of a group of DHCP server addresses for use by the extended DHCP relay agent. | 1. Expand Server Group.  
2. In the Comment box, enter the comment for the server group.  
3. Click Server Group next to Server Group.  
4. Click Add new entry next to Server Group.  
5. Expand Server-Group.  
6. In the Name box, enter the name of the group of DHCP server addresses.  
7. In the Comment box, enter the comment for the server group.  
8. Click Address next to Server-Group.  
9. Click Add new entry next to Address.  
10. In the Name box, enter the IP address of the DHCP server belonging to this named server group. You can configure a maximum of five IP addresses per named server group. |

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

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

To configure tracing operations for DHCP relay agent in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Forwarding Options > DHCP Relay.
4. Select Traceoptions.
5. Add or modify settings as specified in Table 97 on page 192.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

### Table 97: DHCP Relay Traceoptions Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure tracing operations for extended DHCP relay agent processes. | 1. In the Comment box, enter the comment for the traceoptions.  
2. Select the No Remote Trace check box to disable remote tracing globally or for a specific tracing operation. |
Table 97: DHCP Relay Traceoptions Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify the name of the file to receive the output of the tracing operation and specifies the maximum number of trace files. | 1. Click **File** next to Traceoptions.  
2. In the **Comment** box, enter the comment for the file.  
3. In the **Filename** box, enter the name of the file to receive the output of the tracing operation.  
4. In the **Size** box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).  
5. From the **Files** list, select the maximum number of trace files. Range: 2 through 1000.  
6. Select one of the following:  
   - **world-readable**—To enable unrestricted file access  
   - **no-world-readable**—To restrict file access to owner  
7. In the **Match** box, enter the regular expression. |
| Specify the tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. | 1. Click **Flag** next to Traceoptions.  
2. Click **Add new entry** next to Flag.  
3. From the **Name** list, select the flag.  
4. In the **Comment** box, enter the comment for the flag. |

Specifying Address Family for Filters (NSM Procedure)

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

To specify the address family for filters in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Forwarding Options > Family**.
4. Add or modify settings as specified in Table 98 on page 193.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 98: Address Family Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Apply a forwarding table filter to a forwarding table. | 1. Click **Inet**, **Inet6**, or **Mpls**.  
2. Click **Filter** next to Inet, Inet6, or Mpls.  
3. In the **Comment** box, enter the comment.  
4. From the **Input** list, select the name of the applied filter.  
5. From the **Output** list, select the name of the applied filter. |
Table 98: Address Family Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Apply a forwarding table filter for VPLS. | 1. Click Vplsl next to Family.  
2. Expand Vpls.  
3. Click Filter next to Vpls.  
4. In the Comment box, enter the comment.  
5. From the Input list, select the name of the applied filter.  
6. Click Flood next to Vpls.  
7. In the Comment box, enter the comment.  
8. From the Input list, select the name of the applied filter. |

Related Topics
- Configuring the Extended DHCP Agent (NSM Procedure) on page 185
- Configuring Per-Flow and Per-Prefix Load Balancing (NSM Procedure) on page 203
- Configuring Port Mirroring (NSM Procedure) on page 204

Configuring Load Balancing Using Hash Key (NSM Procedure)

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

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

To configure load balancing in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Forwarding Options > Hash Key.
4. Add or modify settings as specified in Table 99 on page 195.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
Table 99: Load Balance Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure layer information for the load-balancing specification. Only the IPv4 protocol is supported.</td>
<td>1. Click <strong>Inet</strong> next to Family.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Layer 3</strong> next to Inet.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. Select the <strong>Destination Address</strong> check box to include the destination-address MAC information in the hash key.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Layer 4</strong> next to Inet.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td>Configure load balancing based on MPLS labels. Only the IPv4 protocol is supported.</td>
<td>1. Click <strong>Mpls</strong> next to Family.</td>
</tr>
<tr>
<td></td>
<td>2. Expand <strong>Mpls</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Payload</strong> next to Mpls.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Ip</strong> next to Payload.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>7. Expand <strong>Ip</strong>.</td>
</tr>
<tr>
<td></td>
<td>8. Click <strong>Layer 3 Only</strong> next to Ip.</td>
</tr>
<tr>
<td></td>
<td>9. Select <strong>layer-3-only</strong> to include only Layer 3 IP information.</td>
</tr>
<tr>
<td></td>
<td>10. Select <strong>port-data</strong> to include only Layer 3 IP information.</td>
</tr>
<tr>
<td></td>
<td>a. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>b. Select <strong>Source Msb</strong> to include the most significant byte of the source port.</td>
</tr>
<tr>
<td></td>
<td>c. Select <strong>Source Lsb</strong> to include the least significant byte of the source port.</td>
</tr>
<tr>
<td></td>
<td>d. Select <strong>Destination Msb</strong> to include the most significant byte of the destination port.</td>
</tr>
<tr>
<td></td>
<td>e. Select <strong>Destination Lsb</strong> to include the least significant byte of the destination port.</td>
</tr>
<tr>
<td>Configure load balancing based on Layer 2 media access control information.</td>
<td>1. Click <strong>Multiservice</strong> next to Mpls.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. Select <strong>Source Mac</strong> to include the source-address MAC information in the hash key.</td>
</tr>
<tr>
<td></td>
<td>4. Select <strong>Destination Mac</strong> to include the destination-address MAC information in the hash key.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Configuring Accounting Options (NSM Procedure) on page 183
- Configuring Helpers (NSM Procedure) on page 195
- Configuring Per-Flow and Per-Prefix Load Balancing (NSM Procedure) on page 203

**Configuring Helpers (NSM Procedure)**

You can enable Trivial File Transfer Protocol (TFTP) or Domain Name System (DNS) request packet forwarding, or configure the router or interface to act as a Dynamic Host...
Configuration Protocol (DHCP) or Bootstrap Protocol (BOOTP) relay agent. You use only one server address per interface or global configuration. See the following topics:

- Configuring a Router or Interface to Act as a Bootstrap Protocol Relay Agent on page 196
- Enabling DNS Request Packet Forwarding on page 199
- Configuring a Port for a DHCP or BOOTP Relay Agent on page 201
- Configuring Tracing Operations for BOOTP, DNS, and TFTP Packet Forwarding on page 202

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

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

To configure a BOOTP relay agent in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Forwarding Options > Helpers > BOOTP.
4. Add or modify settings as specified in Table 100 on page 196.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 100: BOOTP Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configures a router or interface to act as a DHCP or BOOTP relay agent. | 1. In the Comment box, enter the comment.  
  2. Select the Relay Agent check box to configure router as a BOOTP relay agent.  
  3. From the Maximum Hop Count list, select the maximum number of hops allowed.  
     Default: 4 hops  
  4. From the Minimum Wait Time list, select the minimum time allowed.  
     Default: 3 seconds  
  5. From the Client Response TTL list, select the IP time-to-live (TTL) value in DHCP response packets sent to a DHCP client. |
Table 100: BOOTP Configuration Details (continued)

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify the interface for a DHCP and BOOTP relay agent. | 1. Click **Interface** next to BOOTP.  
2. Click **Add new entry** next to Interface.  
3. Expand **Interface**.  
4. In the **Name** box, enter the interface for a DHCP and BOOTP relay agent.  
5. In the **Comment** box, enter the comment.  
6. Select the **No Listen** check box to disable recognition of DNS requests or stop packets from being forwarded on a logical interface, a group of logical interfaces, or a router.  
7. Select the **Broadcast** check box to issue the DHCP or BOOTP request as a broadcast message.  
8. In the **Descriptions** box, enter the description of BOOTP, DHCP, Domain Name System (DNS), or Trivial File Transfer Protocol (TFTP) service, or of an interface that is configured for the service.  
9. From the **Maximum Hop Count** list, select the maximum number of hops allowed.  
   Default: 4 hops  
10. From the **Minimum Wait Time** list, select the minimum time allowed.  
   Default: 3 seconds  
11. From the **Client Response Ttl** list, select the IPv4 time-to-live (TTL) value in DHCP response packets sent to a DHCP client.  

Table 100: BOOTP Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure the router to act as a DHCP and BOOTP relay agent. | 1. Click **Server** next to Interface.  
  2. Click **Add new entry** next to Server.  
  3. Expand **Server**.  
  4. In the **Name** box, enter the server identifier.  
  5. In the **Comment** box, enter the comment.  
  6. Click **Logical System** next to Server.  
  7. Click **Add new entry** next to Logical System.  
  8. Expand **logical-system**.  
  9. In the **Name** box, enter the logical system name.  
  10. In the **Comment** box, enter the comment.  
  11. Click **Routing Instance** next to logical-system.  
  12. Click **Add new entry** next to Routing Instance.  
  13. In the **New routing-instance** window, enter the routing instance name.  
  14. Click **Routing instance** next to server.  
  15. Click **Add new entry** next to Routing Instance.  
  16. In the **New routing-instance** window, enter the routing instance name.  
  17. Click **Server** next to BOOTP.  
  18. Click **Add new entry** next to Server.  
  19. Expand **Server**.  
  20. Click **Logical System** next to Server.  
  21. Click **Add new entry** next to Logical System.  
  22. In the **Name** box, enter the logical system name.  
  23. In the **Comment** box, enter the comment.  
  24. Click **Routing Instance** next to logical-system.  
  25. Click **Add new entry** next to Routing Instance.  
  26. In the **New routing-instance window** enter the routing instance name.  
  27. Click **Routing Instance** next to server.  
  28. Click **Add new entry** next to Routing Instance.  
  29. In the **New routing-instance window** enter the routing instance name. |

### Enabling DNS Request Packet Forwarding

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

To enable DNS request packet forwarding in NSM:

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

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

4. Add or modify settings as specified in Table 101 on page 200.

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

### Table 101: DNS and TFTP Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify the interface for monitoring and forwarding DNS or TFTP requests. | 1. In the **Comment** box, enter the comment.  
2. In the **Description** box, enter the description of BOOTP, DHCP, Domain Name System (DNS), or Trivial File Transfer Protocol (TFTP) service, or of an interface that is configured for the service.  
3. Click **Interface** next to Domain.  
4. Click **Add new entry** next to Interface.  
5. Expand **Interface**.  
6. In the **Name** box, enter the interface for a DHCP and BOOTP relay agent.  
7. In the **Comment** box, enter the comment.  
8. Select the **No Listen** check box to disable recognition of DNS requests or stop packets from being forwarded on a logical interface, a group of logical interfaces, or a router.  
9. Select the **Broadcast** check box to issue the DHCP or BOOTP request as a broadcast message.  
10. In the **Descriptions** box, enter the description of BOOTP, DHCP, Domain Name System (DNS), or Trivial File Transfer Protocol (TFTP) service, or of an interface that is configured for the service.  
11. Click **Server** next to Interface.  
12. In the **Comment** box, enter the comment.  
13. In the **Address** box, enter the address of the server.  
14. Expand **Server**.  
15. Click **Logical System** next to Server.  
16. Select **logical-system** or **routing-instance**.  
17. Click **Server** next to Domain.  
18. In the **Comment** box, enter the comment.  
19. In the **Address** box, enter the address of the server.  
20. Expand **Server**.  
21. Click **Logical System** next to Server.  
22. Select **logical-system** or **routing-instance**. |
Configuring a Port for a DHCP or BOOTP Relay Agent

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

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

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Forwarding Options > Helpers.
4. Select Port.
5. Add or modify settings as specified in Table 102 on page 202.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.
Table 102: Port Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring a Port.</td>
<td>1. From the Name list, select the port number.</td>
</tr>
<tr>
<td></td>
<td>2. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. In the Description box, enter the description of BOOTP, DHCP, Domain</td>
</tr>
<tr>
<td></td>
<td>Name System (DNS), or Trivial File Transfer Protocol (TFTP) service, or</td>
</tr>
<tr>
<td></td>
<td>of an interface that is configured for the service.</td>
</tr>
<tr>
<td></td>
<td>4. Expand Port.</td>
</tr>
<tr>
<td></td>
<td>5. Click Interface next to Domain.</td>
</tr>
<tr>
<td></td>
<td>6. Click Add new entry next to Interface.</td>
</tr>
<tr>
<td></td>
<td>7. Expand Interface.</td>
</tr>
<tr>
<td></td>
<td>8. In the Name box, enter the interface for a DHCP and BOOTP relay agent.</td>
</tr>
<tr>
<td></td>
<td>9. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>10. Select the No Listen check box to disable recognition of DNS requests</td>
</tr>
<tr>
<td></td>
<td>or stop packets from being forwarded on a logical interface, a group of</td>
</tr>
<tr>
<td></td>
<td>logical interfaces, or a router.</td>
</tr>
<tr>
<td></td>
<td>11. Select the Broadcast check box to issue the DHCP or BOOTP request as</td>
</tr>
<tr>
<td></td>
<td>a broadcast message.</td>
</tr>
<tr>
<td></td>
<td>12. In the Descriptions box, enter the description of BOOTP, DHCP, Domain</td>
</tr>
<tr>
<td></td>
<td>Name System (DNS), or Trivial File Transfer Protocol (TFTP) service, or</td>
</tr>
<tr>
<td></td>
<td>of an interface that is configured for the service.</td>
</tr>
<tr>
<td></td>
<td>13. Click Server next to Interface.</td>
</tr>
<tr>
<td></td>
<td>15. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>16. In the Address box, enter the address of the server.</td>
</tr>
<tr>
<td></td>
<td>17. Click Logical System next to Server.</td>
</tr>
<tr>
<td></td>
<td>18. Select the corresponding logical system.</td>
</tr>
<tr>
<td></td>
<td>19. Click Server next to Port.</td>
</tr>
<tr>
<td></td>
<td>20. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>21. In the Address box, enter the address of the server.</td>
</tr>
<tr>
<td></td>
<td>22. Click Logical System next to Server.</td>
</tr>
<tr>
<td></td>
<td>23. Select the corresponding logical system.</td>
</tr>
</tbody>
</table>

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

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

To configure tracing operations in NSM:

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

5. Add or modify settings as specified in Table 103 on page 203.

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

<table>
<thead>
<tr>
<th>Table 103: Traceoptions Configuration Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task</td>
</tr>
<tr>
<td>Define tracing operations for event policy.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Specify the name of the file to receive the output of the tracing operation and the maximum number of trace files.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Specify the tracing operation to perform</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

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

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

To configure load balancing in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Forwarding Options > Load Balance.
4. Add or modify settings as specified in Table 104 on page 204.
5. Click one:
• OK—Saves the changes.
• Cancel—Cancels the modifications.

Table 104: Load Balancing Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Enable per-flow load balancing based on hash values. | 1. In the Comment box, enter the comment.  
2. Select the Indexed Next Hop check box to generate a permuted index of next-hop entries for unicast and aggregate next hops.  
3. Click Per Flow next to Load Balance.  
4. In the Comment box, enter the comment for per-flow.  
5. Select the Hash Seed check box to configure based on the hash value. |
| Configure the hash parameter for per-prefix load balancing. | 1. Click Per Prefix next to Load Balance.  
2. In the Comment box, enter the comment for per prefix.  
3. From the Hash Seed list, select the hash value.  
   Range: 0 through 65,535  
   Default: 0 |

Related Topics

• Configuring Port Mirroring (NSM Procedure) on page 204
• Configuring Helpers (NSM Procedure) on page 195
• Configuring Load Balancing Using Hash Key (NSM Procedure) on page 194

Configuring Port Mirroring (NSM Procedure)

On all M Series, T Series, and MX Series routers, you can send a copy of an IPv4 or IPv6 packet from the routers to an external host address or a packet analyzer for analysis. This is known as port mirroring. In addition, on the M7i, M10i, M120, M320 and MX Series routers only, you can configure port mirroring for VPLS traffic. VPLS port mirroring is supported only on M7i and M10i routers with Enhanced CFEB (CFEB-E). In addition, on M320 routers, VPLS port mirroring is supported only on Enhanced III Flexible PIC Concentrators (FPCs).

To configure port mirroring in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Forwarding Options > Port Mirroring.
4. Add or modify settings as specified in Table 105 on page 205.
5. Click one:
   • OK—Saves the changes.
• Cancel— Cancels the modifications.

Table 105: Port Mirroring Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure the address type family to sample for port mirroring. | 1. In the **Comment** box, enter the comment for the port mirroring.  
2. Select the **Mirror Once** check box to configure the router to mirror packets only once.  
3. Click **Family** next to Port Mirroring.  
4. Expand **Family**.  
5. Click **Inet** or **Inet6** next to Family.  
6. Click **Output**.  
7. In the **Comment** box, enter the comment.  
8. Select the **No Filter Check** check box to disable filter checking on the port-mirroring interface.  
9. Click **Interface** next to Output.  
10. Click **Add new entry** next to Interface.  
11. Expand **Interface**.  
12. In the **Name** box, enter the name of the interface.  
13. In the **Comment** box, enter the comment.  
14. Click **Next Hop** next to interface.  
15. Click **Add new entry** next to Next Hop.  
16. In the **Name** box, enter the IP address of the next-hop router.  
17. In the **Comment** box, enter the comment.  
18. Click **Vpls** next to Family.  
19. In the **Comment** box, enter the comment.  
20. Click **Output** next to Vpls.  
21. In the **Comment** box, enter the comment.  
22. In the **Interface** box, enter the name of the interface.  
23. Select the **No Filter Check** check box to disable filter checking on the port-mirroring interface.  

Configure input packet properties for port mirroring. | 1. In the **Comment** box, enter the comment for input.  
2. From the **Rate** list, select the ratio of the number of packets to be sampled. For example, if you specify a rate of 10, every tenth packet (1 packet out of 10) is sampled.  
Range: 1 through 65,535  
3. From the **Run Length** list, select the number of samples following the initial trigger event. This allows you to sample packets following those already being sampled.  
Range: 0 through 20  
Default: 0 |
Table 105: Port Mirroring Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a port-mirroring instance.</td>
<td>1. Click <strong>Instance</strong> next to Port Mirroring.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Instance.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the name of the port-mirroring instance.</td>
</tr>
<tr>
<td></td>
<td>4. To configure the address type family to sample for port mirroring, refer Table 105 on page 205.</td>
</tr>
<tr>
<td></td>
<td>5. To configure input packet properties for port mirroring, refer Table 105 on page 205.</td>
</tr>
<tr>
<td>Configure traffic sampling tracing operations.</td>
<td>1. In the <strong>Comment</strong> box, enter the comment for traceoptions.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>File</strong> next to Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Comment</strong> box, enter the comment for the file.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Filename</strong> box, enter the name of the file containing the trace information. Default: /var/log/sampled</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Size</strong> box, enter the maximum size of each traffic sampling file or trace log file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). Syntax: xk to specify KB, xm to specify MB, or xg to specify GB Range: 10 KB through the maximum file size supported on your router Default: 1 MB for sampling data; 128 KB for log information</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Files</strong> list, select the maximum number of traffic sampling or trace log files. Range: 1 through 100 files Default: 5 files for sampling output; 10 files for trace log information</td>
</tr>
<tr>
<td></td>
<td>7. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>world-readable</strong>—To enable unrestricted file access.</td>
</tr>
<tr>
<td></td>
<td>• <strong>no-world-readable</strong>—To restrict file access to owner.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Configuring Per-Flow and Per-Prefix Load Balancing (NSM Procedure) on page 203
- Configuring Load Balancing Using Hash Key (NSM Procedure) on page 194
- Specifying Address Family for Filters (NSM Procedure) on page 193
CHAPTER 17

Configuring Interfaces

- Configuring Interfaces on the Routing Platform (NSM Procedure) on page 207
- Configuring Interface set on the Routing Platform (NSM Procedure) on page 234
- Configuring Trace Options on the Routing Platform (NSM Procedure) on page 235

Configuring Interfaces on the Routing Platform (NSM Procedure)

You can configure the interfaces on the router using this option. See the following topics:

- Configuring Interface Properties (NSM Procedure) on page 207
- Damping Interface Transitions (NSM Procedure) on page 208
- Configuring Receive Bucket Properties on Interfaces (NSM Procedure) on page 209
- Configuring Tracing Operations of an Individual Router Interface (NSM Procedure) on page 210
- Configuring Transmit Leaky Bucket Properties (NSM Procedure) on page 211
- Configuring Logical Interface Properties (NSM Procedure) on page 212
- Configuring Protocol Family Information for the Logical Interface (NSM Procedure) on page 215
- Configuring the Traffic Shaping Profile (NSM Procedure) on page 232

Configuring Interface Properties (NSM Procedure)

You can configure interfaces on the router using this option. The management and internal Ethernet interfaces are automatically configured. You must configure all other interfaces.

To configure interfaces in NSM:

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

NOTE: You can also configure interfaces through the Quick Configuration tab. Also, you can configure interfaces in a Config group and apply them to the interface node.
5. Add or modify settings as specified in Table 106 on page 208.

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

Table 106: Interface Properties Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Interfaces.</td>
<td>1. Click <strong>Add Interface</strong> next to Interface.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Add Interface Dialog</strong> box, enter the interface name.</td>
</tr>
<tr>
<td></td>
<td>3. From the <strong>Name</strong> list, select the interface name.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Description</strong> box, enter the text to describe the interface.</td>
</tr>
<tr>
<td></td>
<td>If the text includes spaces, enclose the entire text in quotation marks.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Accounting Profile</strong> list, select the name of the accounting profile.</td>
</tr>
<tr>
<td></td>
<td>7. Select <strong>per-unit-scheduler</strong> to enable association of scheduler map names with logical interfaces.</td>
</tr>
<tr>
<td></td>
<td>8. Select <strong>Hierarchical-scheduler</strong> to enable the use of hierarchical scheduler.</td>
</tr>
<tr>
<td></td>
<td>9. From the <strong>Native Vlan Id</strong> list, select the VLAN ID number.</td>
</tr>
<tr>
<td></td>
<td>10. From the <strong>Speed</strong> list, select the speed.</td>
</tr>
<tr>
<td></td>
<td>11. From the <strong>Mtu</strong> list, select the maximum transmission unit (MTU) size for the media or protocol.</td>
</tr>
<tr>
<td></td>
<td>12. From the <strong>Encapsulation</strong> list, select the encapsulation type.</td>
</tr>
<tr>
<td></td>
<td>13. In the <strong>Bandwidth</strong> box, enter the peak rate.</td>
</tr>
<tr>
<td></td>
<td>14. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• traps—to enable the sending of Simple Network Management Protocol (SNMP) notifications when the state of the connection changes.</td>
</tr>
<tr>
<td></td>
<td>• no-traps—to disable the sending of Simple Network Management Protocol (SNMP) notifications when the state of the connection changes.</td>
</tr>
<tr>
<td></td>
<td>15. From the <strong>Accounting Profile</strong> list, select the accounting profile.</td>
</tr>
</tbody>
</table>

Damping Interface Transitions (NSM Procedure)

When an interface changes from being up to being down, or from down to up, this transition is advertised immediately to the hardware and the JUNOS Software. In some situations you might want to damp interface transitions. This means not advertising the interface’s transition until a certain period of time called the hold time has passed. When you have damped interface transitions and the interface goes from up to down, the interface is not advertised to the rest of the system as being down until it has remained down for the hold-time period. Similarly when an interface goes from down to up, it is not advertised as being up until it has remained up for the hold-time period.

To configure hold time value to use to damp interface transitions:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Interfaces.
4. Select Interface.
5. Add or modify settings as specified in Table 107 on page 209.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

**Table 107: Hold Time Configuration Details**

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure hold-time value to use to damp interface transitions.      | 1. Click Add Interface next to Interface.  
|                                                                      | 2. In the Add Interface Dialog box, enter the interface name.  
|                                                                      | 3. Click Hold Time next to interface.  
|                                                                      | 4. In the Comment box, enter the comment.  
|                                                                      | 5. From the Up list, select the hold time to use when an interface transitions from down to up.  
|                                                                      | Range: 0 through 4,294,967,295 milliseconds  
|                                                                      | Default: 0 milliseconds  
|                                                                      | 6. From the Down list, select the hold time to use when an interface transitions from up to down  
|                                                                      | Range: 0 through 4,294,967,295 milliseconds  
|                                                                      | Default: 0 milliseconds |

**Configuring Receive Bucket Properties on Interfaces (NSM Procedure)**

For all interface types except ATM, Fast Ethernet, Gigabit Ethernet, and channelized IQ and IQE, you can configure leaky bucket properties, which allow you to limit the amount of traffic received on a particular interface. You effectively specify what percentage of the interface’s total capacity can be used to receive packets. You might want to set leaky bucket properties to limit the traffic flow from a link that is known to transmit a high volume of traffic.

To configure receive bucket properties in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Interfaces.
4. Select Interface.
5. Add or modify settings as specified in Table 108 on page 210.
6. Click one:
   - OK—Saves the changes.
- Cancel—Cancels the modifications.

Table 108: Receive Bucket Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure receive bucket</td>
<td>1. Click <strong>Add Interface</strong> next to Interface.</td>
</tr>
<tr>
<td>properties.</td>
<td>2. In the <strong>Add Interface Dialog</strong> box, enter the interface name.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Receive Bucket</strong> next to interface.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. From the <strong>Overflow</strong> list, select how to handle packets that exceed the</td>
</tr>
<tr>
<td></td>
<td>threshold for the receive leaky bucket.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>tag</strong> to tag, count, and process received packets that</td>
</tr>
<tr>
<td></td>
<td>exceed the threshold.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>discard</strong> to discard received packets that exceed the</td>
</tr>
<tr>
<td></td>
<td>threshold.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Rate</strong> list, select the percentage of the interface line rate</td>
</tr>
<tr>
<td></td>
<td>that is available to receive or transmit packets.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 100</td>
</tr>
<tr>
<td></td>
<td>7. From the <strong>Threshold</strong> list, select the maximum size, in bytes, for traffic</td>
</tr>
<tr>
<td></td>
<td>bursts.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 65,535 bytes</td>
</tr>
</tbody>
</table>

Configuring Tracing Operations of an Individual Router Interface (NSM Procedure)

You can define tracing operations for individual interfaces using this option. To specify more than one tracing operation, include multiple flag statements.

To configure tracing operations of an router interface in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in Table 109 on page 211.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.
Table 109: Trace Options Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define tracing operations</td>
<td>1. Click <strong>Add Interface</strong> next to Interface.</td>
</tr>
<tr>
<td>for individual interfaces.</td>
<td>2. In the <strong>Add Interface Dialog</strong> box, enter the interface name.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Traceoptions</strong> next to interface.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. Expand <strong>Traceoptions</strong>.</td>
</tr>
<tr>
<td></td>
<td>6. Click <strong>Flag</strong> next to Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>Add new entry</strong> next to Flag.</td>
</tr>
<tr>
<td></td>
<td>8. From the <strong>Name</strong> list, select the tracing operation to perform.</td>
</tr>
<tr>
<td></td>
<td>9. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
</tbody>
</table>

Configuring Transmit Leaky Bucket Properties (NSM Procedure)

For all interface types except ATM, channelized E1, E1, Fast Ethernet, Gigabit Ethernet, and channelized IQ, you can configure leaky bucket properties, which allow you to limit the amount of traffic transmitted by a particular interface. You effectively specify what percentage of the interface’s total capacity can be used to transmit packets. You might want to set leaky bucket properties to limit the traffic flow from a link that is known to transmit a high volume of traffic.

To configure transmit leaky bucket properties in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Interfaces.
4. Select Interface.
5. Add or modify settings as specified in Table 110 on page 212.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
Table 110: Transmit Bucket Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure transmit bucket properties.</td>
<td>1. Click <strong>Add Interface</strong> next to Interface.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Add Interface Dialog</strong> box, enter the interface name.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Transmit Bucket</strong> next to interface.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. From the <strong>Overflow</strong> list, select how to handle packets that exceed the threshold for the transmit leaky bucket.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>discard</strong> to discard packets that exceed the threshold for the transmit leaky bucket.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Rate</strong> list, select the percentage of the interface line rate that is available to receive or transmit packets.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 100</td>
</tr>
<tr>
<td></td>
<td>7. From the <strong>Threshold</strong> list, select the maximum size, in bytes, for traffic bursts.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 65,535 bytes</td>
</tr>
</tbody>
</table>

Configuring Logical Interface Properties (NSM Procedure)

The following sections describes the configuration of logical interface properties:

- Configuring Logical Unit Properties (NSM Procedure) on page 212
- Configuring an IP Demux Underlying Interface (NSM Procedure) on page 213
- Configuring the Logical Demux Source Family Type on the IP Demux Underlying Interface (NSM Procedure) on page 214
- Configuring Epd Threshold for the Logical Interface (NSM Procedure) on page 214

**Configuring Logical Unit Properties (NSM Procedure)**

To configure logical unit properties in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in Table 111 on page 213.
6. Click one:
   • OK—Saves the changes.
   • Cancel— Cancels the modifications.
Table 111: Logical Unit Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure logical unit properties.</td>
<td>1. Click <strong>Add Interface</strong> next to Interface.</td>
</tr>
<tr>
<td>2. In the <strong>Add Interface Dialog</strong> box,</td>
<td>enter the interface name.</td>
</tr>
<tr>
<td>3. Click <strong>Unit</strong> next to interface.</td>
<td></td>
</tr>
<tr>
<td>4. Click <strong>Add new entry</strong> next to Unit.</td>
<td></td>
</tr>
<tr>
<td>5. From the <strong>Name</strong> list, select the</td>
<td>interface name.</td>
</tr>
<tr>
<td>6. In the <strong>Comment</strong> check box, enter</td>
<td>the comment.</td>
</tr>
<tr>
<td>7. Select the <strong>Disable</strong> check box to</td>
<td>disable a physical or a logical interface, effectively unconfiguring it.</td>
</tr>
<tr>
<td>8. Select the <strong>Reassemble Packets</strong></td>
<td>check box to enable reassembly of fragmented tunnel packets on generic</td>
</tr>
<tr>
<td>9. In the <strong>Description</strong> box, enter the</td>
<td>routing encapsulation (GRE) tunnel interfaces.</td>
</tr>
<tr>
<td>10. From the <strong>Encapsulation</strong> list,</td>
<td>select the encapsulation type.</td>
</tr>
<tr>
<td>11. In the <strong>Bandwidth</strong> box, enter the</td>
<td>peak rate.</td>
</tr>
<tr>
<td>12. Select one of the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>traps</strong>—To enable the sending of Simple Network Management Protocol</td>
</tr>
<tr>
<td></td>
<td>(SNMP) notifications when the state of the connection changes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>no-traps</strong>—To disable the sending of Simple Network Management Protocol</td>
</tr>
<tr>
<td></td>
<td>(SNMP) notifications when the state of the connection changes.</td>
</tr>
<tr>
<td></td>
<td>13. From the <strong>Accounting Profile</strong> list, select the accounting profile.</td>
</tr>
</tbody>
</table>

**Configuring an IP Demux Underlying Interface (NSM Procedure)**

You can configure the logical demultiplexing (demux) destination family type on the IP demux underlying interface.

To configure an IP demux underlying interface in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in Table 112 on page 214.
6. Click one:
   • **OK**—Saves the changes.
   • **Cancel**— Cancels the modifications.
### Configuring the Logical Demux Source Family Type on the IP Demux Underlying Interface (NSM Procedure)

You can configure the logical demultiplexing (demux) source family type on the IP demux underlying interface using this option.

To configure logical demux source family type in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in Table 113 on page 214.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.

### Table 113: IP Demux Source Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure the logical demultiplexing (demux) source family type on the IP demux underlying interface. | 1. Click **Add Interface** next to Interface.  
2. In the **Add Interface Dialog** box, enter the interface name.  
3. Click **Unit** next to interface.  
4. Click **Add new entry** next to Unit.  
5. Click **Demux Source** next to Unit.  
6. Click **Add new entry** next to Demux Source.  
7. From the **New demux-destination** window, select the family type. |

### Configuring Epd Threshold for the Logical Interface (NSM Procedure)

To configure Epd threshold for the logical interface in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in Table 114 on page 215.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

### Table 114: Epd Threshold Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Define the EPD threshold on a virtual circuit (VC). | 1. Click **Add Interface** next to Interface.  
2. In the **Add Interface Dialog** box, enter the interface name.  
3. Click **Unit** next to interface.  
4. Click **Add new entry** next to Unit.  
5. Click **Epd Threshold** next to Unit.  
6. In the **Comment** box, enter the comment.  
7. In the **Epd Threshold plo0** box, enter the early packet discard threshold value.  
8. In the **Plp1** box, enter the maximum number of cells.  
   Range: For 1-port and 2-port OC12 interfaces, 1 through 425,984 cells |

### Configuring Protocol Family Information for the Logical Interface (NSM Procedure)

You can configure the family information for the logical interface for different protocols using the following options:

1. Configuring Protocol Family (Ccc) Information for the Logical Interface (NSM Procedure) on page 215
2. Configuring Protocol Family (Inet) Information for the Logical Interface (NSM Procedure) on page 217
3. Configuring Protocol Family (Inet6) Information for the Logical Interface (NSM Procedure) on page 223
4. Configuring Protocol Family (ISO) Information for the Logical Interface (NSM Procedure) on page 229
5. Configuring Protocol Family (MPLS) Information for the Logical Interface (NSM Procedure) on page 230
6. Configuring Protocol Family (TCC) Information for the Logical Interface (NSM Procedure) on page 232

**Configuring Protocol Family (Ccc) Information for the Logical Interface (NSM Procedure)**

To configure ccc family information in NSM:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Interfaces.
4. Select Interface.
5. Add or modify settings as specified in Table 115 on page 216.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

### Table 115: Ccc Family Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Apply a filter to an interface.</strong></td>
<td>1. Click Add Interface next to Interface.</td>
</tr>
<tr>
<td></td>
<td>2. In the Add Interface Dialog box, enter the interface name.</td>
</tr>
<tr>
<td></td>
<td>3. Click Unit next to interface.</td>
</tr>
<tr>
<td></td>
<td>4. Click Add new entry next to Unit.</td>
</tr>
<tr>
<td></td>
<td>5. Click Family next to Unit.</td>
</tr>
<tr>
<td></td>
<td>6. Expand Family.</td>
</tr>
<tr>
<td></td>
<td>7. Click Ccc next to Family.</td>
</tr>
<tr>
<td></td>
<td>8. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>9. Click Filter next to Ccc.</td>
</tr>
<tr>
<td></td>
<td>10. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>11. From the Group list, select the filter group number.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 255</td>
</tr>
</tbody>
</table>

#### Configure input filter.

1. Click Input next to Filter.
2. Select one of the following:
   - Input—To configure name of one filter to evaluate when packets are received on the interface. Enter the input filter name.
   - Input-list—To apply a group of filters to evaluate when packets are received on an interface.
     a. Click Add new entry next to input-list.
     b. In the New input-list window, enter the filter names. Up to 16 filters can be included in a filter input list.

#### Configure output filter.

1. Click Output next to Filter.
2. Select one of the following:
   - output—To configure name of one filter to evaluate when packets are transmitted on the interface. Enter the output filter name.
   - output-list—To apply a group of filters to evaluate when packets are transmitted on an interface.
     a. Click Add new entry next to output-list.
     b. In the New output-list window, enter the filter names. Up to 16 filters can be included in a filter input list.
Table 115: Ccc Family Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply a policer to an interface.</td>
<td>1. Click <strong>Policer</strong> next to Filter.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Input</strong> box, enter the name of one policer to evaluate when packets are received on the interface.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Output</strong> box, enter the name of one policer to evaluate when packets are transmitted on the interface.</td>
</tr>
</tbody>
</table>

Configuring Protocol Family (Inet) Information for the Logical Interface (NSM Procedure)

To configure inet family information in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in Table 116 on page 218.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.
Table 116: Inet Family Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Inet information.</td>
<td>1. Click <strong>Add Interface</strong> next to Interface.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Add Interface Dialog</strong> box, enter the interface name.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Unit</strong> next to interface.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Add new entry</strong> next to Unit.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Family</strong> next to Unit.</td>
</tr>
<tr>
<td></td>
<td>6. Expand <strong>Family</strong>.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>Inet</strong> next to Family.</td>
</tr>
<tr>
<td></td>
<td>8. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>9. From the <strong>Mac Validate</strong> list, select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>strict</strong>—Forwards incoming packets when both the IP source address and the MAC source address match one of the trusted address tuples. Drops packets when the MAC address does not match the tuple’s MAC source address, or when IP source address of the incoming packet does not match any of the trusted IP addresses.</td>
</tr>
<tr>
<td></td>
<td>• <strong>loose</strong>—Forwards incoming packets when both the IP source address and the MAC source address match one of the trusted address tuples. Drops packets when the IP source address matches one of the trusted tuples, but the MAC address does not match the MAC address of the tuple. Continues to forward incoming packets when the source address of the incoming packet does not match any of the trusted IP addresses.</td>
</tr>
<tr>
<td></td>
<td>10. From the <strong>Mtu</strong> list, select the MTU size.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 4294967295</td>
</tr>
<tr>
<td></td>
<td>11. Select the <strong>No Redirects</strong> check box to disable the sending of protocol redirect messages for the entire routing platform.</td>
</tr>
<tr>
<td></td>
<td>12. Select the <strong>No Arp Learn</strong> check box to disable ARP mappings.</td>
</tr>
<tr>
<td></td>
<td>13. Select the <strong>Primary</strong> check box to configure the address to be the primary address of the protocol on the interface.</td>
</tr>
<tr>
<td>Enable IP packet counters on an interface.</td>
<td>1. Click <strong>Accounting</strong> next to Inet.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. Select the <strong>Destination Class Usage</strong> check box to enable packet counters on an interface that count packets that arrive from specific customers and are destined for specific prefixes on the provider core router.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Source Class Usage</strong> next to Accounting.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. Select the <strong>Input</strong> check box to configure at least one expected ingress point.</td>
</tr>
<tr>
<td></td>
<td>7. Select the <strong>Output</strong> check box to configure at least one expected egress point.</td>
</tr>
</tbody>
</table>
Table 116: Inet Family Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the interface address.</td>
<td>1. Click <strong>Address</strong> next to Inet.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Address.</td>
</tr>
<tr>
<td></td>
<td>3. Expand <strong>address</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Name</strong> box, enter the interface name.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. Select the <strong>Primary</strong> check box to configure this address to be the primary address of the protocol on the interface. If the logical unit has more than one address, the primary address is used by default as the source address when packets originate from the interface and the destination does not indicate the subnet.</td>
</tr>
<tr>
<td></td>
<td>7. Select the <strong>Preferred</strong> check box to configure this address to be the preferred address on the interface. If you configure more than one address on the same subnet, the preferred source address is chosen by default as the source address when you originate packets to destinations on the subnet.</td>
</tr>
</tbody>
</table>

| Configure VRRP IPv4 group. | 1. Click **Vrrp Group** next to address.                                        |
|                           | 2. Click **Add new entry** next to Vrrp Group.                                |
|                           | 3. In the **Name** box, enter the interface name.                             |
|                           | 4. In the **Comment** box, enter the comment.                                |
|                           | 5. In the **Virtual Link Local Address** box, enter the virtual link local address. |
|                           | 6. From the **priority** list, select the router’s priority for being elected to be the master router in the VRRP group. A larger value indicates a higher priority for being elected. Range: 1 through 255 Default: 100 (for backup routers) |
|                           | 7. Select one of the following:                                               |
|                           |   • **accept-data**—To enable the interface to accept packets destined for the virtual IP address. |
|                           |   • **no-accept-data**—To prevent the interface from accepting packets destined for the virtual IP address. |
|                           | 8. From the **Authentication Type** list, select the authentication type.     |
|                           | 9. In the **Authentication Key** box, enter the authentication password.      |
|                           | 10. Select **Advertise-Interval** next to vrrp-group.                         |
|                           | 11. Select one of the following:                                              |
|                           |   • **advertise-interval**—To configure the interval between Virtual Router Redundancy Protocol (VRRP) IPv4 advertisement packets. Range: 1 through 255 seconds |
|                           |   • **fast-interval**—To configure the interval, in milliseconds, between Virtual Router Redundancy Protocol (VRRP) advertisement packets. Range: 100 through 999 milliseconds |
|                           |   • **inet6-advertise-interval**—To configure the interval between Virtual Router Redundancy Protocol (VRRP) IPv6 advertisement packets Range: 100 to 40,950 milliseconds (ms) |
Table 116: Inet Family Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure a backup router to preempt the master router | 1. Click **Preempt** next to vrrp-group.  
2. Select **preempt** to allow the master router to be preempted.  
   a. In the **Comment** box, enter the comment.  
   b. From the **Hold Time** list, select the hold time before a higher-priority backup router preempts the master router.  
3. Select **no-preempt** to prohibit the preemption of the master router.  
4. Click **Track** next to vrrp-group.  
5. In the **Comment** box, enter the comment.  
6. From the **Priority Hold Time** list, select the minimum length of time that must elapse between dynamic priority changes.  
   Range: 1 through 3600 seconds  
7. Click **Interface** next to Track.  
8. Click **Add new entry** next to Interface.  
9. In the **Name** box, enter the interface name.  
10. In the **Comment** box, enter the comment.  
11. From the **Priority Cost** list, select the VRRP routers’ priority cost for becoming the master default router. The router with the highest priority within the group becomes the master.  
   Range: 1 through 254 |
Table 116: Inet Family Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the bandwidth threshold for VRRP.</td>
<td>1. Click <strong>Bandwidth Threshold</strong> next to interface.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Bandwidth Threshold.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the interface name.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. From the <strong>Priority Cost</strong> list, select the VRRP router’s priority cost for</td>
</tr>
<tr>
<td></td>
<td>becoming the master default router. The router with the highest priority</td>
</tr>
<tr>
<td></td>
<td>within the group becomes the master.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 254</td>
</tr>
<tr>
<td></td>
<td>6. Click <strong>Route</strong> next to Track.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Route_address</strong> box, enter the address.</td>
</tr>
<tr>
<td></td>
<td>8. In the <strong>Routing Instances</strong> box, enter the routing instance in which the</td>
</tr>
<tr>
<td></td>
<td>route is to be tracked</td>
</tr>
<tr>
<td></td>
<td>9. From the <strong>Priority Cost</strong> list, select the VRRP router’s priority cost for</td>
</tr>
<tr>
<td></td>
<td>becoming the master default router. The router with the highest priority</td>
</tr>
<tr>
<td></td>
<td>within the group becomes the master.</td>
</tr>
<tr>
<td></td>
<td>10. Click <strong>Virtual Address</strong> next to vrrp-group.</td>
</tr>
<tr>
<td></td>
<td>11. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>virtual-address</strong>—To configure the addresses of the virtual routers in</td>
</tr>
<tr>
<td></td>
<td>a Virtual Router Redundancy Protocol (VRRP) IPv4 group. You can configure up</td>
</tr>
<tr>
<td></td>
<td>to eight addresses.</td>
</tr>
<tr>
<td></td>
<td>a. Click <strong>Add new entry</strong> and in the New virtual-address window, enter</td>
</tr>
<tr>
<td></td>
<td>the addresses of one or more virtual routers.</td>
</tr>
<tr>
<td></td>
<td>b. In the New virtual-address window, enter the addresses of one or more</td>
</tr>
<tr>
<td></td>
<td>virtual routers.</td>
</tr>
<tr>
<td></td>
<td>• <strong>virtual-inet6-address</strong>—To configure the addresses of the virtual routers</td>
</tr>
<tr>
<td></td>
<td>a Virtual Router Redundancy Protocol (VRRP) IPv6 group. You can configure up</td>
</tr>
<tr>
<td></td>
<td>to eight addresses.</td>
</tr>
<tr>
<td></td>
<td>a. Click <strong>Add new entry</strong></td>
</tr>
<tr>
<td></td>
<td>b. In the New virtual-address window, enter the addresses of one or more</td>
</tr>
<tr>
<td></td>
<td>virtual routers.</td>
</tr>
</tbody>
</table>

Configure input filter.

1. Click **Input** next to Filter.
2. Select one of the following:
   - **input**—To configure name of one filter to evaluate when packets are received on the interface. Enter the input filter name.
   - **input-list**—To apply a group of filters to evaluate when packets are received on an interface.
     a. Click **Add new entry** next to input-list.
     b. In the New **input-list** window, enter the filter names. Up to 16 filters can be included in a filter input list.
Table 116: Inet Family Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure output filter. | 1. Click **Output** next to Filter.  
2. Select one of the following:  
   • **output**—To configure name of one filter to evaluate when packets are transmitted on the interface. Enter the output filter name.  
   • **output–list**—To apply a group of filters to evaluate when packets are transmitted on an interface.  
     a. Click **Add new entry** next to output-list.  
     b. In the **New output-list** window, enter the filter names. Up to 16 filters can be included in a filter input list. |
| Apply a policer to an interface. | 1. Click **Policer** next to Filter.  
2. In the **Comment** box, enter the comment.  
3. In the **Input** box, enter the name of one policer to evaluate when packets are received on the interface.  
4. In the **Output** box, enter the name of one policer to evaluate when packets are transmitted on the interface. |
| Check whether traffic is arriving on an expected path. | 1. Click **Rpf Check** next to **Inet**.  
2. In the **Comment** box, enter the comment.  
3. In the **Fail Filter** box, enter the filter name to evaluate when packets are received on the interface.  
4. Click **Mode** next to Rpf Check.  
5. In the **Comment** box, enter the comment.  
6. Select the **loose** check box to check whether the packet has a source address with a corresponding prefix in the routing table. |
| Configure the direction of traffic to be sampled. | 1. In the **Comment** box, enter the comment.  
2. Select the **Input** check box to configure at least one expected ingress point.  
3. Select the **Output** check box to configure at least one expected egress point. |
Table 116: Inet Family Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Define one or more service sets to be applied to an interface.       | 1. Click Service next to Inet.  
|                                                                      | 2. In the Comment box, enter the comment.                                   |
|                                                                      | 3. Click Input next to Service.                                             |
|                                                                      | 4. In the Comment box, enter the comment.                                   |
|                                                                      | 5. In the Post Service Filter box, enter the filter to be applied to traffic after service processing. |
|                                                                      | 7. Click Service Set next to Input.                                         |
|                                                                      | 8. Click Add new entry next to Service Set.                                 |
|                                                                      | 9. From the Name list, select the service set name.                        |
|                                                                      | 10. In the Comment box, enter the comment.                                  |
|                                                                      | 11. In the Service Filter box, enter the filter name.                      |
|                                                                      | 12. Click Output next to Service.                                           |
|                                                                      | 13. In the Comment box, enter the comment.                                  |
|                                                                      | 15. Click Service Set next to Output.                                       |
|                                                                      | 16. Click Add new entry next to Service Set.                                |
|                                                                      | 17. From the Name list, select the service set name.                       |
|                                                                      | 18. In the Comment box, enter the comment.                                 |
|                                                                      | 19. In the Service Filter box, enter the filter name.                      |
| Configure an Ethernet or demultiplexing interface to be unnumbered. | 1. Click Unnumbered Address next to Inet.                                  |
|                                                                      | 2. In the Comment box, enter the comment.                                  |
|                                                                      | 3. In the Source box, enter the secondary IP address of the donor loopback interface. |

Configuring Protocol Family (Inet6) Information for the Logical Interface (NSM Procedure)

To configure inet6 family information in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Interfaces.
4. Select Interface.
5. Add or modify settings as specified in Table 117 on page 224.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
### Table 117: Inet6 Family Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure Inet6 information.</strong></td>
<td>1. Click <strong>Add Interface</strong> next to Interface.  &lt;br&gt; 2. In the <strong>Add Interface Dialog</strong> box, enter the interface name.  &lt;br&gt; 3. Click <strong>Unit</strong> next to interface.  &lt;br&gt; 4. Click <strong>Add new entry</strong> next to Unit.  &lt;br&gt; 5. Click <strong>Family</strong> next to Unit.  &lt;br&gt; 6. Expand <strong>Family</strong>.  &lt;br&gt; 7. Click <strong>inet</strong> next to Family.  &lt;br&gt; 8. In the <strong>Comment</strong> box, enter the comment.  &lt;br&gt; 9. From the <strong>Mac Validate</strong> list, select one of the following:  &lt;br&gt;     • <strong>strict</strong>—Forwards incoming packets when both the IP source address and the MAC source address match one of the trusted address tuples. Drops packets when the MAC address does not match the tuple's MAC source address, or when IP source address of the incoming packet does not match any of the trusted IP addresses.  &lt;br&gt;     • <strong>loose</strong>—Forwards incoming packets when both the IP source address and the MAC source address match one of the trusted address tuples. Drops packets when the IP source address matches one of the trusted tuples, but the MAC address does not match the MAC address of the tuple. Continues to forward incoming packets when the source address of the incoming packet does not match any of the trusted IP addresses.  &lt;br&gt; 10. From the <strong>Mtu</strong> list, select the MTU size.  &lt;br&gt;    Range: 0 through 4294967295  &lt;br&gt; 11. Select the <strong>No Redirects</strong> check box to disable the sending of protocol redirect messages for the entire routing platform.  &lt;br&gt; 12. Select the <strong>No Arp Learn</strong> check box to disable arp.  &lt;br&gt; 13. Select the <strong>Primary</strong> check box to configure the address to be the primary address of the protocol on the interface.</td>
</tr>
<tr>
<td><strong>Enable IP packet counters on an interface.</strong></td>
<td>1. Click <strong>Accounting</strong> next to Inet.  &lt;br&gt; 2. In the <strong>Comment</strong> box, enter the comment.  &lt;br&gt; 3. Select <strong>Destination Class Usage</strong> check box to enable packet counters on an interface that count packets that arrive from specific customers and are destined for specific prefixes on the provider core router.  &lt;br&gt; 4. Click <strong>Source Class Usage</strong> next to Accounting.  &lt;br&gt; 5. In the <strong>Comment</strong> box, enter the comment.  &lt;br&gt; 6. Select the <strong>Input</strong> check box to configure at least one expected ingress point.  &lt;br&gt; 7. Select the <strong>Output</strong> check box to configure at least one expected egress point.</td>
</tr>
</tbody>
</table>
Table 117: Inet6 Family Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure the interface address. | 1. Click **Address** next to Inet.  
2. Click **Add new entry** next to Address.  
3. Expand **address**.  
4. In the **Name** box, enter the interface name.  
5. In the **Comment** box, enter the comment.  
6. Select the **Primary** check box to configure this address to be the primary address of the protocol on the interface. If the logical unit has more than one address, the primary address is used by default as the source address when packets originate from the interface and the destination does not indicate the subnet.  
7. Select the **Preferred** check box to configure this address to be the preferred address on the interface. If you configure more than one address on the same subnet, the preferred source address is chosen by default as the source address when you originate packets to destinations on the subnet. |

| Configure VRRP IPV6 Group. | 1. Click **Vrrp Group** next to address.  
2. Click **Add new entry** next to Vrrp Group.  
3. In the **Name** box, enter the interface name.  
4. In the **Comment** box, enter the comment.  
5. In the **Virtual Link Local Address** box, enter the virtual link local address.  
6. From the **priority** list, select the router’s priority for being elected to be the master router in the VRRP group. A larger value indicates a higher priority for being elected.  
Range: 1 through 255  
Default: 100 (for backup routers)  
7. Select one of the following:  
   - **accept-data**—To enable the interface to accept packets destined for the virtual IP address.  
   - **no-accept-data**—To prevent the interface from accepting packets destined for the virtual IP address.  
8. From the **Authentication Type** list, select the authentication type.  
9. In the **Authentication Key** box, enter the authentication password.  
10. Select **Advertise-interval** next to vrrp-group.  
11. Select one of the following:  
   - **advertise-interval**—To configure the interval between Virtual Router Redundancy Protocol (VRRP) IPv4 advertisement packets.  
     Range: 1 through 255 seconds  
   - **fast-interval**—To configure the interval, in milliseconds, between Virtual Router Redundancy Protocol (VRRP) advertisement packets.  
     Range: 100 through 999 milliseconds  
   - **inet6-advertise-interval**—To configure the interval between Virtual Router Redundancy Protocol (VRRP) IPv6 advertisement packets  
     Range: 100 to 40,950 milliseconds (ms) |
### Table 117: Inet6 Family Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure a backup router to preempt the master router. | 1. Click **Preempt** next to vrrp-group.  
2. Select one of the following:  
   - **preempt**—To allow the master router to be preempted.  
     a. In the **Comment** box, enter the comment.  
     b. From the **Hold Time list**, select the hold time before a higher-priority backup router preempts the master router.  
       Range: 0 through 3600  
   - **no-preempt**—To prohibit the preemption of the master router.  
3. Click **Track** next to vrrp-group.  
4. In the **Comment** box, enter the comment.  
5. From the **Priority Hold Time** list, select the minimum length of time that must elapse between dynamic priority changes.  
   Range: 1 through 3600 seconds  
6. Click **Interface** next to Track.  
7. Click **Add new entry** next to Interface.  
8. In the **Name** box, enter the interface name.  
9. In the **Comment** box, enter the comment.  
10. From the **Priority Cost** list, select the VRRP router's priority cost for becoming the master default router. The router with the highest priority within the group becomes the master.  
   Range: 1 through 254 |
Table 117: Inet6 Family Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify the bandwidth threshold for VRRP. | 1. Click **Bandwidth Threshold** next to interface.  
2. Click **Add new entry** next to Bandwidth Threshold.  
3. In the **Name** box, enter the interface name.  
4. In the **Comment** box, enter the comment.  
5. From the **Priority Cost** list, select the VRRP router's priority cost for becoming the master default router. The router with the highest priority within the group becomes the master. Range: 1 through 254 |
| | 6. Click **Route** next to Track.  
7. In the **Route address** box, enter the address.  
8. In the **Routing Instances** box, enter the routing instance in which the route is to be tracked.  
9. From the **Priority Cost** list, select the VRRP router's priority cost for becoming the master default router. The router with the highest priority within the group becomes the master. |
| | 10. Click **Virtual Address** next to vrrp-group.  
11. Select one of the following:  
   • **virtual-address**—To configure the addresses of the virtual routers in a Virtual Router Redundancy Protocol (VRRP) IPv4 group. You can configure up to eight addresses.  
     a. Click **Add new entry** and in the **New virtual-address** window, enter the addresses of one or more virtual routers.  
   • **virtual-inet6-address**—To configure the addresses of the virtual routers in a Virtual Router Redundancy Protocol (VRRP) IPv6 group. You can configure up to eight addresses.  
     a. Click **Add new entry** and in the **New virtual-inet6-address** window, enter the addresses of one or more virtual routers. |
| Configure input filter. | 1. Click **Input** next to Filter.  
2. Select one of the following:  
   • Select **input** to configure name of one filter to evaluate when packets are received on the interface. Enter the input filter name.  
   • Select **input-list** to apply a group of filters to evaluate when packets are received on an interface.  
     a. Click **Add new entry** next to input-list.  
     b. In the **New input-list** window, enter the filter names. Up to 16 filters can be included in a filter input list. |
Table 117: Inet6 Family Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure output filter.    | 1. Click **Output** next to Filter.  
2. Select one of the following:  
   • Select **output** to configure name of one filter to evaluate when packets are transmitted on the interface. Enter the output filter name.  
     a. Enter the output filter name.  
   • Select **output-list** to apply a group of filters to evaluate when packets are transmitted on an interface.  
     a. Click **Add new entry** next to output-list.  
     b. In the **New output-list** window, enter the filter names. Up to 16 filters can be included in a filter input list. |
| Apply a policer to an interface. | 1. Click **Policer** next to Filter.  
2. In the **Comment** box, enter the comment.  
3. In the **Input** box, enter the name of one policer to evaluate when packets are received on the interface.  
4. In the **Output** box, enter the name of one policer to evaluate when packets are transmitted on the interface. |
| Check whether traffic is arriving on an expected path. | 1. Click **Rpf Check** next to Inet.  
2. In the **Comment** box, enter the comment.  
3. In the **Fail Filter** box, enter the filter name to evaluate when packets are received on the interface.  
4. Click **Mode** next to Rpf Check.  
5. In the **Comment** box, enter the comment.  
6. Select the **loose** check box to check whether the packet has a source address with a corresponding prefix in the routing table. |
| Configure the direction of traffic to be sampled. | 1. In the **Comment** box, enter the comment.  
2. Select the **Input** check box to configure at least one expected ingress point.  
3. Select the **Output** check box to configure at least one expected egress point. |
Table 117: Inet6 Family Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define one or more service sets to be applied to an interface.</td>
<td>1. Click Service next to Inet.&lt;br&gt;2. In the Comment box, enter the comment.&lt;br&gt;3. Click Input next to Service.&lt;br&gt;4. In the Comment box, enter the comment.&lt;br&gt;5. In the Post Service Filter box, enter the filter to be applied to traffic after service processing.&lt;br&gt;6. Expand Input.&lt;br&gt;7. Click Service Set next to Input.&lt;br&gt;8. Click Add new entry next to Service Set.&lt;br&gt;9. From the Name list, select the service set name.&lt;br&gt;10. In the Comment box, enter the comment.&lt;br&gt;11. In the Service Filter box, enter the filter name.&lt;br&gt;12. Click Output next to Service.&lt;br&gt;13. In the Comment box, enter the comment.&lt;br&gt;14. Expand Output.&lt;br&gt;15. Click Service Set next to Output.&lt;br&gt;16. Click Add new entry next to Service Set.&lt;br&gt;17. From the Name list, select the service set name.&lt;br&gt;18. In the Comment box, enter the comment.&lt;br&gt;19. In the Service Filter box, enter the filter name.</td>
</tr>
</tbody>
</table>

Configuring Protocol Family (ISO) Information for the Logical Interface (NSM Procedure)

To configure iso family information in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Interfaces.
4. Select Interface.
5. Add or modify settings as specified in Table 118 on page 230.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.
Table 118: Iso Family Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Iso information.</td>
<td>1. Click <strong>Add Interface</strong> next to Interface.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Add Interface Dialog</strong> box, enter the interface name.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Unit</strong> next to interface.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Add new entry</strong> next to Unit.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Family</strong> next to Unit.</td>
</tr>
<tr>
<td></td>
<td>6. Expand <strong>Family</strong>.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>Iso</strong> next to <strong>Family</strong>.</td>
</tr>
<tr>
<td></td>
<td>8. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>9. From the <strong>Mtu</strong> list, select the MTU size.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 4294967295</td>
</tr>
<tr>
<td>Configure the interface address.</td>
<td>1. Click <strong>Address</strong> next to <strong>Inet</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to <strong>Address</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Expand <strong>address</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Name</strong> box, enter the interface name.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
</tbody>
</table>

Configuring Protocol Family (MPLS) Information for the Logical Interface (NSM Procedure)

To configure mpls family information in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in Table 119 on page 231.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.
Table 119: MPLS Family Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure MPLS information.</td>
<td>1. Click Add Interface next to Interface.</td>
</tr>
<tr>
<td></td>
<td>2. In the Add Interface Dialog box, enter the interface name.</td>
</tr>
<tr>
<td></td>
<td>3. Click Unit next to interface.</td>
</tr>
<tr>
<td></td>
<td>4. Click Add new entry next to Unit.</td>
</tr>
<tr>
<td></td>
<td>5. Click Family next to Unit.</td>
</tr>
<tr>
<td></td>
<td>6. Expand Family.</td>
</tr>
<tr>
<td></td>
<td>7. Click MPLS next to Family.</td>
</tr>
<tr>
<td></td>
<td>8. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>9. From the Mtu list, select the MTU size.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 4294967295</td>
</tr>
<tr>
<td>Configure input filter.</td>
<td>1. Click Input next to Filter.</td>
</tr>
<tr>
<td></td>
<td>2. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• input—To configure name of one filter to evaluate when packets are received on the interface. Enter the input filter name.</td>
</tr>
<tr>
<td></td>
<td>• input-list—To apply a group of filters to evaluate when packets are received on an interface.</td>
</tr>
<tr>
<td></td>
<td>a. Click Add new entry next to input-list.</td>
</tr>
<tr>
<td></td>
<td>b. In the New input-list window, enter the filter names. Up to 16 filters can be included in a filter input list.</td>
</tr>
<tr>
<td>Configure output filter.</td>
<td>1. Click Output next to Filter.</td>
</tr>
<tr>
<td></td>
<td>2. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• output—To configure name of one filter to evaluate when packets are transmitted on the interface. Enter the output filter name.</td>
</tr>
<tr>
<td></td>
<td>• output-list—To apply a group of filters to evaluate when packets are transmitted on an interface.</td>
</tr>
<tr>
<td></td>
<td>a. Click Add new entry next to output-list.</td>
</tr>
<tr>
<td></td>
<td>b. In the New output-list window, enter the filter names. Up to 16 filters can be included in a filter input list.</td>
</tr>
<tr>
<td>Apply a policer to an interface.</td>
<td>1. Click Policer next to Filter.</td>
</tr>
<tr>
<td></td>
<td>2. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. In the Input box, enter the name of one policer to evaluate when packets are received on the interface.</td>
</tr>
<tr>
<td></td>
<td>4. In the Output box, enter the name of one policer to evaluate when packets are transmitted on the interface.</td>
</tr>
</tbody>
</table>
Configuring Protocol Family (TCC) Information for the Logical Interface (NSM Procedure)

To configure tcc family information in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Interfaces.
4. Select Interface.
5. Add or modify settings as specified in Table 120 on page 232.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 120: TCC Family Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure tcc information.</td>
<td>1. Click Add Interface next to Interface.</td>
</tr>
<tr>
<td></td>
<td>2. In the Add Interface Dialog box, enter the interface name.</td>
</tr>
<tr>
<td></td>
<td>3. Click Unit next to interface.</td>
</tr>
<tr>
<td></td>
<td>4. Click Add new entry next to Unit.</td>
</tr>
<tr>
<td></td>
<td>5. Click Family next to Unit.</td>
</tr>
<tr>
<td></td>
<td>6. Expand Family.</td>
</tr>
<tr>
<td></td>
<td>7. Click Tcc next to Family.</td>
</tr>
<tr>
<td></td>
<td>8. In the Comment box, enter the comment.</td>
</tr>
</tbody>
</table>

| Apply a policer to an interface. | 1. Click Policer next to Tcc.                                               |
|                                  | 2. In the Comment box, enter the comment.                                   |
|                                  | 3. In the Input box, enter the name of one policer to evaluate when packets are received on the interface. |
|                                  | 4. In the Output box, enter the name of one policer to evaluate when packets are transmitted on the interface. |

| Configure Ethernet TCC encapsulation. | 1. Click proxy next to TCC.                                                   |
|                                         | 2. In the Comment box, enter the comment.                                    |
|                                         | 3. Click Remote next to TCC.                                                  |
|                                         | 4. In the Comment box, enter the comment.                                    |

Configuring the Traffic Shaping Profile (NSM Procedure)

When you use an ATM encapsulation on ATM1 and ATM2 IQ interfaces, you can define bandwidth utilization, which consists of either a constant rate or a peak cell rate, with sustained cell rate and burst tolerance.

To configure traffic shaping profile in NSM:
1. In the NSM navigation tree, select **Device Manager > Devices**.

2. Click the **Device Tree** tab, and then double-click the device to select it.

3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.

4. Select **Interface**.

5. Add or modify settings as specified in Table 121 on page 233.

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

### Table 121: Traffic Shaping Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Define the traffic-shaping profile. | 1. Click **Add Interface** next to Interface.  
2. In the **Add Interface Dialog** box, enter the interface name.  
3. Click **Unit** next to interface.  
4. Click **Add new entry** next to Unit.  
5. Click **Shaping** next to Unit.  
6. Expand **Shaping**.  
7. In the **Comment** box, enter the comment.  
8. From the **Queue Length** list, select the maximum number of packets the queue can contain.  
   Range: 1 through 16383 packets  
   Default: 16383 packets  
9. Click **Cbr** next to Shaping.  
10. Select one of the following:  
   a. **cbr**—To define a constant bit rate bandwidth utilization in the traffic-shaping profile for ATM encapsulation.  
      a. In the **Comment** box, enter the comment.  
      b. In the **Cbr Value** box, enter the unspecified bit rate (UBR).  
   b. **vbr**—To define the variable bandwidth utilization in the traffic-shaping profile for ATM encapsulation.  
      a. In the **Comment** box, enter the comment.  
      b. In the **Peak** box, enter the peak rate.  
      c. In the **Sustained** box, enter the sustained rate.  
      d. In the **Burst** box, enter the burst length.  
   c. **rtvbr**—To define the real-time variable bandwidth utilization in the traffic-shaping profile for ATM2 IQ PICs.  
      a. In the **Comment** box, enter the comment.  
      b. In the **Peak** box, enter the peak rate.  
      c. In the **Sustained** box, enter the sustained rate.  
      d. In the **Burst** box, enter the burst length. |
Configuring Interface set on the Routing Platform (NSM Procedure)

You can configure an interface set on the routing platform using this option.

To configure interface set in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Interfaces.
4. Select Interface Set.
5. Add or modify settings as specified in Table 122 on page 234.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

### Table 122: Interface Set Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define the interface set.</td>
<td>1. Click Add new entry next to Interface Set.</td>
</tr>
<tr>
<td></td>
<td>2. Click Interface-set.</td>
</tr>
<tr>
<td></td>
<td>3. In the Name box, enter the name for the interface set.</td>
</tr>
<tr>
<td></td>
<td>4. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td>Apply the interface set to</td>
<td>1. Click interface next to interface-set.</td>
</tr>
<tr>
<td>interfaces.</td>
<td>2. Click Add new entry next to Interface.</td>
</tr>
<tr>
<td></td>
<td>3. In the Name box, enter the interface name.</td>
</tr>
<tr>
<td></td>
<td>4. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. Click Unit next to Interface.</td>
</tr>
<tr>
<td></td>
<td>6. Click Add new entry next to Unit.</td>
</tr>
<tr>
<td></td>
<td>7. From the Name list, select the number of the logical unit. Range: 0 through 16,385</td>
</tr>
<tr>
<td></td>
<td>8. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>9. Click Vlan Tags Outer next to Interface.</td>
</tr>
<tr>
<td></td>
<td>10. Click Add new entry next to Vlan tags Outer.</td>
</tr>
<tr>
<td></td>
<td>11. From the Name list, select the outer VLAN ID.</td>
</tr>
<tr>
<td></td>
<td>12. In the Comment box, enter the comment.</td>
</tr>
</tbody>
</table>

### Related Topics
- Configuring Interfaces on the Routing Platform (NSM Procedure) on page 207
- Configuring Trace Options on the Routing Platform (NSM Procedure) on page 235
Configuring Trace Options on the Routing Platform (NSM Procedure)

You can configure the trace options using this option.

To configure trace options in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Interfaces.
4. Select Trace options.
5. Add or modify settings as specified in Table 123 on page 235.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 123: Traceoption Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Define tracing operations for the interface process. | 1. In the Comment box, enter the comment for the traceoptions.  
2. Select No Remote Trace check box to disable remote tracing.  
3. Click File next to Traceoptions.  
4. In the Comment box, enter the comment for the filename.  
5. In the Filename box, enter the name of the file to receive the output of the tracing operation.  
6. In the Size box, enter the maximum trace file size.  
7. From the Files list, select the maximum number of trace files.  
8. Select one of the following:  
   - no-world-readable—To restrict the file access to owner.  
   - world-readable—To enable unrestricted access.  
9. In the Matchbox, enter the regular expression.  
10. Click Flag next to Traceoptions. |

| Define flag. | 1. Click Add new entry next to Flag.  
2. From the Name list, select the flag to perform the trace operation.  
   - Select kernel to log configuration IPC messages to kernel.  
   - Select change-events to log changes that produce configuration events.  
   - Select kernel-detail to log details of configuration messages to kernel.  
   - Select config-states to log the configuration state machine changes.  
3. Enter the comment for the flag.  
4. Select the Disable check box to disable the tracing operation. |
Related Topics

- Configuring Interfaces on the Routing Platform (NSM Procedure) on page 207
- Configuring Interface set on the Routing Platform (NSM Procedure) on page 234
Multicast snooping is a way for a Layer 2 device to snoop at the Layer 3 packet content to determine which actions are to be taken to process or forward a frame. There are specific forms of snooping, such as IGMP snooping or PIM snooping. In all cases, snooping involves a device configured to function at Layer 2 having access to Layer 3 (packet) information. Snooping makes multicasting more efficient in these devices.

To configure multicast snooping in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double click the device to select it.
3. In the **Configuration** tab, expand **Multicast Snooping Options**.
4. Add or modify the settings as specified in Table 124 on page 238.
5. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.
Table 124: Multicast Snooping Options Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Establish a list of flood group addresses for multicast snooping. | 1. Click **Flood Groups** next to Multicast Snooping Options.  
2. Click Add new entry next to Flood Groups.  
3. In the dialog box, enter the IP addresses. |
| Configure multicast forwarding cache properties. | 1. Click **Forwarding Cache** next to Multicast Snooping Options.  
2. In the **Comment** box, enter the comments.  
3. Expand **Forwarding Cache**.  
4. Click **Threshold** next to Forwarding Cache.  
5. In the **Comment** box, enter the comments.  
6. From the **Suppress** list, select the threshold value for a forwarding cache.  
   Range: 1 through 200,000  
7. From the **Reuse** list, select the reuse value for the threshold.  
   The reuse value must be less than the suppression threshold value.  
   Range: 1 through 200,000 |
| Establish the graceful restart duration for multicast snooping. | 1. Click **Graceful Restart** next to Multicast Snooping Options.  
2. In the **Comment** box, enter the comments.  
3. From the **Restart Duration** list, select the duration for graceful restart.  
   Range: 0 to 300 seconds  
   Default: 180 seconds |
| Establish multicast snooping option values. | 1. Click **Option** next to Multicast Snooping Options.  
2. In the **Comment** box, enter the comments.  
3. Expand **Options**.  
4. Click **Syslog** next to Options.  
5. In the **Comment** box, enter the comments.  
6. From the **Upto** list, select select the level upto which severity the messages to be syslogged.  
7. From the **Mark** list, select the time interval in seconds to mark the trace file.  
   Range: -2147483647 seconds to 2147483647 Seconds  
   Default: 0  
8. Expand **Syslog**.  
9. Click **Level** next to Syslog.  
10. Select the Level of severity to be logged. |
Table 124: Multicast Snooping Options Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure tracing options. | 1. Click Traceoptions next to Multicast Snooping Options.  
2. In the Comment box, enter the comments.  
3. Expand Traceoptions.  
4. Click File next to Trace Options.  
5. In the Comment box, enter the comments.  
6. In the Filename box, enter the name of the file to receive the output of the tracing operation. Enclose the name within quotation marks.  
7. In the Size box, enter the maximum size of each trace file in bytes.  
Range: 10240 to 4294967295 bytes  
8. From the Files list, select the maximum number of files.  
9. Select the world-readable option to enable log file access to all users.  
10. Select the no-world-readable option to prevent all users from reading the log file.  
11. Click Flag next to Trace Options.  
12. Click Add new entry next to flag.  
13. From the Name list, select a tracing operation to perform.  
14. In the Comment box, enter the comments. |
Configuring Policy Options

• Configuring an AS Path in a BGP Routing Policy (NSM Procedure) on page 241
• Configuring an AS Path Group in a BGP Routing Policy (NSM Procedure) on page 242
• Configuring a Community for use in BGP Routing Policy Conditions (NSM Procedure) on page 243
• Configuring a BGP Export Policy Condition (NSM Procedure) on page 244
• Configuring Flap Damping to Reduce the Number of BGP Update Messages (NSM Procedure) on page 245
• Configuring a Routing Policy Statement (NSM Procedure) on page 247
• Configuring Prefix List (NSM Procedure) on page 248

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 125 on page 242.
7. Click one:
   • OK—To save the changes.
- Cancel—To cancel the modifications.
- Apply — To apply the protocol settings.

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

**Table 125: 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 126 on page 243.
7. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.
   - **Apply** — To apply the protocol settings.
NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the Updating Devices section in the Network and Security Manager Administration Guide for more information.

### Table 126: 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 127 on page 244.
7. Click one:  
   - OK—To save the changes.  
   - Cancel—To cancel the modifications.  
   - Apply — To apply the protocol settings.
NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the Updating Devices section in the Network and Security Manager Administration Guide for more information.

**Table 127: 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 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 community expression.</td>
<td>Select the check-box if you want to invert the results. Clear the check-box if you do not want 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 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 128 on page 245.
7. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.
   - **Apply** — To apply the protocol settings.
NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the Updating Devices section in the Network and Security Manager Administration Guide for more information.

Table 128: 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 129 on page 246.

7. Click one:
   - OK—to save the changes.
   - Cancel—to cancel the modifications.
   - Apply—to apply the protocol settings.

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

### Table 129: 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. Select 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 130 on page 247.
7. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
   - Apply — To apply the protocol settings.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Name     | Specifies the name of the policy statement.   | 1. Click the New button or select a policy statement and click Edit button.  
|          |                                               | 2. Select policy-statement.  
|          |                                               | 3. Specify the name.                                                           |
| Comment  | Specifies the comment for the policy statement. | 1. Click the New button or select a policy statement and click Edit button.  
|          |                                               | 2. Select policy-statement.  
|          |                                               | 3. Specify the comment.                                                        |
### Table 130: Configuring Policy Statement Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</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>
</tr>
</tbody>
</table>
|        | 1. Click the New button or select a policy statement and click Edit button.  
|        | 2. Expand `policy-statement` tree and select `From`.  
|        | 3. Enter the `From` criteria.  
|        | 4. Expand `From` tree and specify the match conditions. |
| Term   | Indicates the term to be configured for the routing policy. You can create one or more terms for a routing policy. Each term comprises of match conditions and the corresponding actions. |
|        | 1. Click the New button or select a policy statement and click Edit button.  
|        | 2. Expand `policy-statement` tree and select `Term`.  
|        | 3. Click the New button or select a term and click Edit button.  
|        | 4. Enter the term name, comment and the match conditions and actions. |
| Then   | Enables you to define the action to be taken in the case of a match or mismatch between the packets and From and To conditions. |
|        | 1. Click the New button or select a policy statement and click Edit button.  
|        | 2. Expand `policy-statement` tree and select `Then`.  
|        | 3. Specify the parameters for `Then` criteria.  
|        | 4. Expand `Then` tree and specify the actions for each match condition. |
| To     | Enables you to define the criteria that an outgoing route must match. You can specify one or more match conditions. If you specify more than one, all conditions must match the route for a match to occur. |
|        | 1. Click the New button or select a policy statement and click Edit button.  
|        | 2. Expand `policy-statement` tree and select `To`.  
|        | 3. Enter the `To` criteria.  
|        | 4. Expand `To` tree and specify the match conditions. |

### Configuring Prefix List (NSM Procedure)

A prefix list is a named list of IP addresses. You can specify an exact match with incoming routes and apply a common action to all matching prefixes in the list. This feature enables you to create a named prefix list and include it in a routing policy.

To configure prefix list in NSM:
1. In the navigation tree select **Device Manager** > **Devices** and select the device from the list.

2. In the configuration tree, expand **Policy Options**.

3. Select **Prefix List**.

4. Add/Modify the parameters as specified in Table 131 on page 249.

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 131: Configuring Prefix List Fields**

<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 <strong>prefix-list</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 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 <strong>prefix-list</strong>.</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 by a defined path.</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 <strong>prefix-list</strong>.</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 <strong>prefix-list</strong> tree and select <strong>Prefix List Item</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the name and comment.</td>
</tr>
</tbody>
</table>
CHAPTER 20

Configuring Protocols

- Configuring the BFD Protocol (NSM Procedure) on page 251
- Configuring BGP (NSM Procedure) on page 252
- Configuring the ILMI Protocol (NSM Procedure) on page 255
- Configuring Layer 2 Address Learning and Forwarding Properties (NSM Procedure) on page 256
- Configuring Layer 2 Circuit (NSM Procedure) on page 257
- Configuring Layer 2 Protocol Tunneling and BPDU Protection (NSM Procedure) on page 262
- Configuring Label Distribution Protocol (NSM Procedure) on page 264
- Configuring Link Management Protocol (NSM Procedure) on page 275
- Configuring MPLS Protocol (NSM Procedure) on page 279
- Configuring MSDP Protocol (NSM Procedure) on page 321
- Configuring MSTP (NSM Procedure) on page 329
- Configuring OSPF (NSM Procedure) on page 331
- Configuring RIP (NSM Procedure) on page 335
- Configuring RIPng Protocol (NSM Procedure) on page 337
- Configuring Router Advertisement (NSM Procedure) on page 347
- Configuring ICMP Router Discovery (NSM Procedure) on page 350
- Configuring RSVP (NSM Procedure) on page 351
- Configuring VRRP (NSM Procedure) on page 358
- Configuring VSTP (NSM Procedure) on page 359

Configuring the BFD Protocol (NSM Procedure)

The Bidirectional Forwarding Detection (BFD) protocol is used to detect the failures in a network. The BFD protocol is independent of the underlying transport mechanisms and layers; hence the failure detection timers for BFD have shorter time limits than the failure detection mechanisms of other protocols like OSPF and IS-IS. Each session of the BFD operates in two modes, asynchronous mode and demand mode. In asynchronous mode, both endpoints periodically send Hello packets to each other. If a number of those packets are not received, the session is considered down. In demand mode, no Hello packets are
exchanged after the session is established; it is assumed that the endpoints have another way to verify connectivity to each other.

To configure BFD:

1. In the navigation tree select Device Manager > Devices and select the device from the list.
2. In the configuration tree, expand Protocols.
3. Select Bfd.
4. Add/Modify the parameters under the respective tabs as specified in Table 132 on page 252.
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 132: Configuring Bfd Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Specifies the comment for Bfd.</td>
<td>Enter the comment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traceoptions</td>
<td>Enables you to define tracing operations that track all routing protocol functionality in the device. You can configure the tracing flag, filter, and the tracing policy.</td>
<td>1. Expand the Bfd tree and select Traceoptions. 2. Expand the Traceoptions tree and set up the file and flag parameters.</td>
</tr>
</tbody>
</table>

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 133 on page 253.

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 133: 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></td>
<td></td>
<td>2. Select BGP and select Path Selection tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Set up the path selection parameters and med plus IGP.</td>
</tr>
<tr>
<td>Traceoptions</td>
<td>Defines trace options for IGMP snooping.</td>
<td>1. Expand the Protocol tree.</td>
</tr>
<tr>
<td></td>
<td></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>
</tbody>
</table>
Table 133: BGP Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Multihop    | If an EBGP peer is more than one hop away from the local router, you must specify the next hop to the peer so that the two systems can establish a BGP session. This type of session is called a multihop BGP session. | 1. Expand the Protocol tree.  
2. Select BGP and select Multihop tab.  
3. Set up the comment, Ttl and specify whether the next hop has to be changed. |
| Advertise   | Enables you to specify whether BGP should advertise the best route even if the routing table did not select it to be an active route. | 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. |
Table 133: BGP Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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. |
| 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 the ILMI Protocol (NSM Procedure)

To configure the ILMI protocol in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols > ilmi.
4. Select Traceoptions.
5. Add or modify settings as specified in Table 134 on page 255.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

Table 134: Trace Options Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Define tracing options. | 1. In the Comment box, enter the comment for the traceoptions.  
2. Select the No Remote Trace check box to disable remote tracing globally or for a specific tracing operation. |
Table 134: Trace Options Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify the name of the file to receive the output of the tracing operation and the maximum number of trace files. | 1. Click **File** next to Traceoptions.  
2. In the **Comment** box, enter the comment for the file.  
3. In the **Filename** box, enter the name of the file to receive the output of the tracing operation.  
4. In the **Size** box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). Range: 10240 through 1073741824  
5. From the **Files** list, select the maximum number of trace files. Range: 2 through 1000.  
6. Select one of the following:  
   a. **world-readable**—To enable unrestricted file access.  
   b. **no-world-readable**—To restrict file access to owner. This is the default setting. |
| Specify the tracing operation to perform.                           | 1. Click **Add new entry** next to Flag.  
2. From the **Name** list, select the flag.  
   a. **database**—Trace database events.  
   b. **routing-socket**—Trace Routing socket events.  
   c. **state**—Trace state change events.  
   d. **debug**—Trace debug messages.  
   e. **event**—Trace event handler events.  
   f. **packet**—Trace packet events.  
   g. **all**—Trace all areas of code.  
3. In the **Comment** box, enter the comment for the flag. |

**Related Topics**
- Configuring Link Management Protocol (NSM Procedure) on page 275
- Configuring Layer 2 Address Learning and Forwarding Properties (NSM Procedure) on page 256

**Configuring Layer 2 Address Learning and Forwarding Properties (NSM Procedure)**

On MX Series routers only, you can configure Layer 2 address learning and forwarding properties in support of Layer 2 bridging. The router learns unicast media access control (MAC) addresses to avoid flooding the packets to all the ports in a bridge domain. The router creates a source MAC entry in its source and destination MAC tables for each MAC address learned from packets received on ports that belong to the bridge domain.

To configure Layer 2 address learning in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > L2 Learning**.
4. Add or modify settings as specified in Table 135 on page 257.

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

Table 135: L2 Learning Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure Layer 2 address learning and forwarding properties globally. | 1. In the Comment box, enter the comment.  
2. From the Global Mac Table Aging Time list, select the time elapsed before MAC table entries are timed out and entries are deleted.  
   Range: 10 through 1000000  
3. Select one of the following:  
   - Global No Mac Learning—To disable MAC learning for the entire router  
   - Global Mac Statistics—To enable MAC accounting for the entire router. |

| Limit the number of media access control (MAC) addresses learned from the logical interfaces on the router. | 1. Click Global Mac Limit next to L2 Learning.  
2. In the Comment box, enter the comment.  
3. From the Mac Limit list, select the Number of MAC addresses that can be learned systemwide.  
   Range: 20 through 1,048,575  
4. From the Packet Action list, select drop to specify that packets for new source MAC addresses be dropped after the MAC address limit is reached. |

Related Topics
- Configuring Layer 2 Circuit (NSM Procedure) on page 257
- Configuring Layer 2 Protocol Tunneling and BPDU Protection (NSM Procedure) on page 262

Configuring Layer 2 Circuit (NSM Procedure)

You can enable a Layer 2 circuit using the L2 Circuit option. See the following topics:
- Configuring Local Interface Switching (NSM Procedure) on page 257
- Configuring the Neighbor Interface for the Layer 2 Circuit (NSM Procedure) on page 258
- Tracing Layer 2 Circuit Creation and Changes (NSM Procedure) on page 261

Configuring Local Interface Switching (NSM Procedure)

You can configure a virtual circuit entirely on the local router, terminating the circuit on a local interface. Possible uses for this feature include being able to enable switching between frame relay Data-Link Connection Identifier (DLCI)s.

To configure local interface switching in NSM:
1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > L2 Circuit**.
4. Select **Local Switching**.
5. Add or modify settings as specified in Table 136 on page 258.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

### Table 136: Local Switching Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a local switching interface.</td>
<td>1. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
</tbody>
</table>
| Configure the interface over which Layer 2 circuit traffic travels. | 1. Click **Interface** next to **Local Switching**.  
2. Click **Add new entry** next to **Interface**.  
3. In the **Name** box, enter the name of the interface to be configured.  
4. In the **Protect Interface** box, enter the name of the protect interface to be configured.  
5. In the **Description** box, enter the text description for the Layer 2 circuit. If the text includes one or more spaces, enclose the entire text string in quotation marks (**" **).  
6. Select the **Ignore Mtu Mismatch** check box to ignore the MTU configuration set for the physical interface associated with the local switching interface or with the remote Provider Edge (PE) router. |
| Specify the end interface for a local interface switch. | 1. Click **End Interface** next to interface.  
2. In the **Comment** box, enter the comment.  
3. In the **Interface** box, enter the name of the interface.  
4. In the **Protect Interface** box, enter the name of the protect interface to be configured. |

### Configuring the Neighbor Interface for the Layer 2 Circuit (NSM Procedure)

Each Layer 2 circuit is represented by the logical interface connecting the local provider edge (PE) router to the local customer edge (CE) router. All the Layer 2 circuits using a particular remote PE router designated for remote CE routers are listed under the neighbor statement (neighbor designates the PE router). Each neighbor is identified by its IP address and is usually the end-point destination for the Label Switched Path (LSP) tunnel (transporting the Layer 2 circuit).

To configure a neighbor interface in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand Protocols > L2 Circuit.

4. Select **Neighbor**.

5. Add or modify settings as specified in Table 137 on page 259.

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

### Table 137: Neighbor Interface Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure a neighbor. | 1. In the **Name** box, enter the IP address of a neighboring router.  
2. In the **Comment** box, enter the comment. |
| Configure the interface over which Layer 2 circuit traffic travels. | 1. Click **Interface** next to neighbor.  
2. Click **Add new entry** next to Interface.  
3. In the **Name** box, enter the interface name.  
4. In the **Comment** box, enter the comment.  
5. In the **Psn Tunnel Endpoint** box, enter the address for the tunnel endpoint.  
6. In the **Protect Interface** box, enter the name of the protect interface to be configured.  
7. From the **Virtual Circuit Id** list, select the identifier.  
   Range: 1 through 4,294,967,295  
8. In the **Description** box, enter the text description for the Layer 2 circuit. If the text includes one or more spaces, enclose the entire text string in quotation marks (" ").  
9. Select one of the following:  
   - **control-word**—To enable the use of the control word.  
   - **no-control-word**—To disable the use of the control word.  
10. In the **Community** box, specify the community for the Layer 2 circuit.  
11. From the **MtU** list, select the MTU number to be advertised for the Layer 2 circuit.  
   Range: 512 through 65535  
12. From the **Encapsulation Type** list, select the encapsulation type.  
13. Select the **Ignore Encapsulation Mismatch** check box to allow a Layer 2 circuit to be established even though the encapsulation configured on the CE device interface does not match the encapsulation configured on the Layer 2 circuit interface.  
14. Select the **Ignore MtU Mismatch** check box to ignore the MTU configuration set for the physical interface associated with the local switching interface or with the remote PE router.  
15. From the **Switchover Delay** list, select the time to wait before switching to the backup pseudowire after the primary pseudowire fails.  
   Range: 0 through 180,000 milliseconds  
   Default: 10,000 milliseconds
### Table 137: Neighbor Interface Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| **Configure pseudowire redundancy for Layer 2 circuits and Virtual Private LAN Service (VPLS).** | 1. Click **Interface** next to neighbor.  
2. Click **Add new entry** next to Interface.  
3. Click **Backup Neighbor** next to interface.  
4. Click **Add new entry** next to Backup Neighbor.  
5. In the **Name** box, enter the interface name.  
6. In the **Comment** box, enter the comment.  
7. From the **Virtual Circuit Id** list, select the identifier. Range: 1 through 4,294,967,295  
8. In the **Community** box, specify the community for the Layer 2 circuit.  
9. In the **Psn Tunnel Endpoint** box, enter the address for the tunnel endpoint.  
10. Select the **Standby** check box to configure the pseudowire to the specified backup neighbor as the standby.  
11. Click **Static** next to backup-neighbor.  
12. In the **Comment** box, enter the comment.  
13. From the **Incoming Label** list, select the incoming label for the static pseudowire. Range: 1000000 through 1048575  
14. From the **Outgoing Label** list, select the outgoing label for the static pseudowire. Range: 299776 through 1048575 |
| **Specify bandwidth allocation for a Layer 2 circuit or for the class types of a Layer 2 circuit.** | 1. Click **Interface** next to neighbor.  
2. Click **Add new entry** next to Interface.  
3. Click **Bandwidth** next to interface.  
4. In the **Comment** box, enter the comment.  
5. In the **Per Traffic Class Bandwidth** box, enter the bandwidth in bits per second for a class type on the Layer 2 circuit.  
6. In the **Ctnumber** box, enter the bandwidth in bits per second for a class type on the Layer 2 circuit. You can configure bandwidth for up to 4 class types (ct0, ct1, ct2, ct3) per Layer 2 circuit. If you configure the class types, you must configure them in order, starting with class type ct0. |
| **Configure static Layer 2 circuit pseudowires.** | 1. Click **Interface** next to neighbor.  
2. Click **Add new entry** next to Interface.  
3. Click **Static** next to interface.  
4. In the **Comment** box, enter the comment.  
5. From the **Incoming Label** list, select the incoming label for the static pseudowire. Range: 1000000 through 1048575  
6. From the **Outgoing Label** list, select the outgoing label for the static pseudowire. Range: 299776 through 1048575  
7. Select the **Send Oam** check box to send oam. |
### Tracing Layer 2 Circuit Creation and Changes (NSM Procedure)

You can trace traffic flowing through a Layer 2 circuit using the Traceoptions option.

To configure tracing operations in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **L2 Circuit**.
4. Select **Traceoptions**.
5. Add or modify settings as specified in Table 138 on page 261.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

#### Table 138: Layer2 Circuit Traceoption Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trace traffic flowing through a Layer 2 circuit.</td>
<td>1. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
</tbody>
</table>
| Specify the name of the file to receive the output of the tracing operation and specifies the maximum number of trace files | 1. Click **File** next to Traceoptions.  
2. In the **Comment** box, enter the comment for the file.  
3. In the **Filename** box, enter the name of the file to receive the output of the tracing operation.  
4. In the **Size** box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).  
5. From the **Files** list, select the maximum number of trace files. Range: 2 through 1000.  
6. Select one of the following:  
   - **world-readable**—To enable unrestricted file access.  
   - **no-world-readable**—To restrict file access to owner. This is the default setting. |
| Specify the tracing operation to perform. | 1. Click **Flag** next to Traceoptions.  
2. Click **Add new entry** next to Flag.  
3. From the **Name** list, select the flag.  
4. In the **Comment** box, enter the comment for the flag.  
5. Select the modifier for the tracing flag. Select one the following check boxes:  
   - **Send**—Packets being transmitted  
   - **Receive**—Packets being received  
   - **Detail**—Detailed trace information  
   - **Disable**—Disable tracing |
Configuring Layer 2 Protocol Tunneling and BPDU Protection (NSM Procedure)

Layer 2 protocol tunneling allows Layer 2 protocol data units (PDUs) to be tunneled through a network. This is useful to provide a single Spanning Tree Protocol (STP) domain for subscribers across a service provider network. On the MX Series routers only, you can configure Bridge Protocol Data Unit (BPDU) protection to ignore BPDUs received on interfaces where none should be expected (for example, a LAN interface on a network edge with no other bridges present). If a BPDU is received on a blocked interface, the interface is disabled and stops forwarding frames. By default, all BPDUs are accepted and processed on all interfaces.

To configure layer 2 protocol tunneling and BPDU protection in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols > Layer2 Control.
4. Add or modify settings as specified in Table 139 on page 262.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 139: Layer2 Circuit Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable BPDUs blocking</td>
<td>1. Click Bpdu Block next to Layer2 Control.</td>
</tr>
<tr>
<td>on an interface</td>
<td>2. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. From the Disable Timeout list, select the disable timeout value.</td>
</tr>
<tr>
<td></td>
<td>Range: 10 through 3600</td>
</tr>
<tr>
<td></td>
<td>Default: If this option is not configured, the interface is not periodically checked and remains disabled</td>
</tr>
<tr>
<td></td>
<td>4. Click Interface next to Bpdu Block.</td>
</tr>
<tr>
<td></td>
<td>5. Click Add new entry next to Interface.</td>
</tr>
<tr>
<td></td>
<td>6. In the Name box, enter the interface name.</td>
</tr>
<tr>
<td></td>
<td>7. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td>Task</td>
<td>Your Action</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Enable rewriting of the MAC address for Layer 2 protocol tunneling. | 1. Click **mac Rewrite** next to Layer2 Control.  
2. In the **Comment** box, enter the comment.  
3. Click **Interface** next to Bpdu Block.  
4. Click **Add new entry** next to Interface.  
5. In the **Name** box, enter the interface name.  
6. In the **Comment** box, enter the comment.  
7. Click **Protocol** next to interface.  
8. In the **Comment** box, enter the comment.  
9. Click **Cdp** next to Protocol.  
10. In the **Comment** box, enter the comment.  
11. Click **Stp** next to Protocol.  
12. In the **Comment** box, enter the comment.  
13. Click **Vtp** next to Protocol.  
14. In the **Comment** box, enter the comment. |
| Define tracing options. | 1. Click **Traceoptions** next to Layer2 Control.  
2. In the **Comment** box, enter the comment for the traceoptions.  
3. Click **File** next to Traceoptions.  
4. In the **Comment** box, enter the comment for the file.  
5. In the **Filename** box, enter the name of the file to receive the output of the tracing operation.  
6. In the **Size** box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).  
7. From the **Files** list, select the maximum number of trace files. Range: 2 through 1000.  
8. Select one of the following:  
   - **world-readable**—To enable unrestricted file access.  
   - **no-world-readable**—To restrict file access to owner. This is the default setting.  
9. In the **Match** box, enter the regular expression.  
10. Click **Add new entry** next to Flag.  
11. From the **Name** list, select the flag.  
12. Select the **Disable** check box to disable the tracing operation. |

**Related Topics**
- Configuring Link Management Protocol (NSM Procedure) on page 275
- Configuring Layer 2 Address Learning and Forwarding Properties (NSM Procedure) on page 256
Configuring Label Distribution Protocol (NSM Procedure)

The Label Distribution Protocol (LDP) is a protocol for distributing labels in non-traffic-engineered applications. LDP allows routers to establish label-switched paths (LSPs) through a network by mapping network-layer routing information directly to data link layer-switched paths.

To configure LDP in NSM:

1. In the navigation tree select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. In the Configuration tab, expand Protocols > LDP.
4. Add or modify the settings as specified in Table 140 on page 265.
5. Click one:
   - OK — To save the changes
   - Cancel — To cancel the modifications
### Table 140: LDP Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure LDP. | 1. In the **Comment** box, enter the comment.  
2. From the **Preference** list, select the route preference level for LDP routes.  
   Range: 0 through 4,294,967,295  
3. Select the **No Forwarding** check box to omit the Ingress routes from the inet.0 routing table.  
4. Select the **L2 Smart Policy** check box to prevent LDP from exporting IPv6 FECs over sessions with layer 2 neighbors.  
5. Select the **Track IGP Metric** check box to cause the IGP route metric to be used for the LDP routes instead of the default LDP route metric.  
6. Select the **Strict Targeted Hellos** check box to prevent LDP sessions from being established with remote neighbors that have not been specifically configured.  
7. Select one of the following:  
   - **deaggregate**—To control forwarding equivalence class (FEC) deaggregation on the router.  
   - **no-deaggregate**—To control forwarding equivalence class (FEC) aggregation on the router.  
8. Select the **Explicit Null** check box to advertise label 0 to the egress router of a label-switched path (LSP).  
9. From the **Label Withdrawal Delay** list, select the number of seconds to wait before withdrawing labels for the LDP LSPs.  
   Default: 60 seconds  
   Range: 0 through 120 seconds  
10. From the **Keep Alive Interval** list, select a Keep Alive value.  
    Range: 1 through 65,535 seconds  
    Default: 10 seconds  
11. From the **Keep Alive Timeout** list, select a Keep Alive Timeout value.  
    Range: 1 through 65,535 seconds  
    Default: 30 seconds  

Configure the prefixes advertised into LDP from the routing table.  

1. Expand **LDP**.  
2. Click **Egress Policy** next to LDP.  
3. Click **Add** after selecting a policy member from the Non member list to add it to the Members list.  
4. Click **Remove** after selecting a policy from the Members list to remove it from the Members list.  
5. Click **Add All** to add all the Non members to the Members list.  
6. Click **Remove All** to remove all the members from the Members list.
### Table 140: LDP Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Apply policy filters to outbound LDP label bindings.                 | 1. Click **Export** next to LDP.  
2. Click **Add** after selecting a policy member from the Non-member list to add it to the Members list.  
3. Click **Remove** after selecting the policy from the Members list to remove it from the Members list.  
4. Click **Add All** to add all the Non-members to the Members list.  
5. Click **Remove All** to remove all the members from the Members list. |
| Enable LDP graceful restart on the LDP master protocol instance or for a specific routing instance. | 1. Click **Graceful Restart** next to LDP.  
2. Select the **Disable** check box to explicitly disable LDP on an interface, or explicitly disable LDP graceful restart.  
3. Select the **Helper Disable** check box to disable helper mode for LDP graceful restart.  
4. From the **Recovery Time** list, select the amount of time a router waits for LDP to restart gracefully.  
   Range: 120 through 1800 seconds  
   Default: 140 seconds  
5. From the **Maximum Neighbor Recovery Time** list, select the maximum amount of time to wait before giving up an attempt to gracefully restart.  
   Range: 120 through 1900 seconds  
   Default: 140 seconds  
6. From the **Reconnect Time** list, select the reconnect time.  
   Range: 30 through 300  
7. From the **Maximum Neighbor Reconnect Time** list, select the maximum time allowed for reconnection.  
   Range: 30 through 300 |
| Apply policy filters to received LDP label bindings.                 | 1. Click **Import** next to LDP.  
2. Click **Add** after selecting a policy member from the Non-member list to add it to the Members list.  
3. Click **Remove** after selecting a policy from the Members list to remove it from the Members list.  
4. Click **Add All** to add all the Non-members to the Members list.  
5. Click **Remove All** to remove all the members from the Members list. |
Table 140: LDP Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Enable LDP on one or more router interfaces. | 1. Click **Interface** next to LDP.  
2. Click **Add new entry** next to Interface.  
3. In the **Name** box, enter the name of the interface.  
4. Select the **Disable** check box to disable LDP on the interface.  
5. From the **Hello Interval** list, select a value to control the rate at which hello messages are sent on the interface.  
   Range: 1 through 65,535 seconds  
   Default: 5 seconds for link hello messages, 15 seconds for targeted hello messages  
6. From the **Hold Time** list, select a hold time to specify how long an LDP node should wait for a hello message before declaring a neighbor to be down.  
   Range: 1 through 65,535 seconds  
   Default: 15 seconds for link hello messages, 45 seconds for targeted hello messages  
7. From the **Transport Address** list, select the transport address. Select one of the following:  
   - router-id—The router identifier is used as the transport address  
   - interface—The first IP address on the interface is used as the transport address  
8. Select one of the following:  
   - **Allow-Subnet-Mismatch**—To ignore the LDP subnet check.  
   - **No-Allow-Subnet-Mismatch**—To enable the LDP subnet check. |
| Disable LDP traps. | 1. Click **Log Updown** next to LDP.  
2. In the **Comment** box, enter the comment.  
3. Click **Trap** next to Log Updown.  
4. In the **Comment** box, enter the comment.  
5. Select the **Disable** check box to disable LDP traps. |
Specify merged next-hop policy.

1. Click **Next Hop** next to LDP.
2. In the **Comment** box, enter the comment.
3. Click **Merged** next to Next Hop.
4. In the **Comment** box, enter the comment.
5. Click **Policy** next to Merged.
6. Click **Add** after selecting a policy member from the Non member list to add it to the Members list.
7. Click **Remove** after selecting a policy from the Members list to remove it from the Members list.
8. Click **Add All** to add all the Non members to the Members list.
9. Click **Remove All** to remove all the members from the Members list.

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify merged next-hop policy. | 1. Click **Next Hop** next to LDP.  
2. In the **Comment** box, enter the comment.  
3. Click **Merged** next to Next Hop.  
4. In the **Comment** box, enter the comment.  
5. Click **Policy** next to Merged.  
6. Click **Add** after selecting a policy member from the Non member list to add it to the Members list.  
7. Click **Remove** after selecting a policy from the Members list to remove it from the Members list.  
8. Click **Add All** to add all the Non members to the Members list.  
9. Click **Remove All** to remove all the members from the Members list. |
Table 140: LDP Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Enable OAM for all of the LDP LSPs or for a specific LDP LSP. | 1. Click **Oam** next to **LDP**.  
2. In the **Comment** box, enter the comment.  
3. From the **Lsp Ping Interval** list, select the time interval between LSP ping messages.  
   Range: 30 through 3600  
4. Click **Bfd Liveness Detection** next to **Oam**.  
5. In the **Comment** box, enter the comment.  
6. From the **Version** list, select the BFD protocol version to detect.  
   Range: 1 (BFD version 1), or automatic (autodetection)  
   Default: automatic  
7. From the **Minimum Interval** list, select the minimum transmit and receive interval.  
   Range: 1 through 255,000  
8. From the **Minimum Receive Interval** list, select the minimum receive interval.  
   Range: 1 through 255,000  
9. From the **Multiplier** list, select the detection time multiplier.  
   Range: 1 through 255  
   Default: 3  
10. Select the **No Adaptation** check box to disable BFD adaptation.  
11. Select the **Ecmp** check box to cause RSVP to establish BFD sessions for all ECMP paths configured for the specified FEC.  
12. From the **Holddown Interval** list, select the time the BFD session must remain up before state change notification is sent.  
   Range: 1 through 255000  
13. Click **Detection Time** next to **Bfd Liveness Detection**.  
14. In the **Comment** box, enter the comment.  
15. From the **Threshold** list, select the time the BFD session must remain up before state change notification is sent.  
   Range: 1 through 4294967295 |
Table 140: LDP Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure route and next-hop properties in the event of a BFD session failure event on an LDP LSP. | 1. Click **Failure Action** next to Bfd Liveness Detection.  
2. In the **Comment** box, enter the comment.  
3. Select one of the following:  
  - **remove-route**—To remove LDP route from the ribs  
  - **remove-nexthop**—To remove LDP nexthop from the route  
4. Click **Transmit Interval** next to Bfd Liveness Detection.  
5. In the **Comment** box, enter the comment.  
6. From the **Minimum Interval** list, select the minimum transmit and receive interval.  
   Range: 1 through 255,000  
7. From the **Threshold** list, select the time the BFD session must remain up before state change notification is sent.  
   Range: 1 through 4294967295 |
Table 140: LDP Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Enable Bidirectional Forwarding Detection (BFD) for all MPLS LSPs or for just a specific LSP. | 1. Click **Fec** next to Oam.  
2. In the **Name** box, enter the forwarding equivalence class (FEC) address.  
3. In the **Comment** box, enter the comment.  
4. Click **Bfd Liveness Detection** next to Fec.  
5. Select one of the following:  
   - *bf-liveness-detection*—To enable BFD for all MPLS LSPs or for just a specific LSP.  
   - *no-bfd-liveness-detection*—To disable BFD for all MPLS LSPs or for just a specific LSP.  
6. Click **Periodic Traceroute** next to fec.  
7. In the **Comment** box, enter the comment.  
8. From the **Frequency** list, select the interval between traceroute attempts.  
   Range: 15 through 120 minutes  
9. From the **Ttl** list, select the maximum time-to-live value.  
   Range: 1 through 255  
10. From the **Retries** list, select the number of attempts to send a probe to a specific node before giving up.  
   Range: 1 through 9  
11. From the **Wait** list, select the wait interval before resending a probe packet.  
   Range: 5 through 15 seconds  
12. From the **Paths** list, select the maximum number of paths to search.  
   Range: 1 through 255  
13. In the **Source** box, enter the IPv4 source address to use when sending probes.  
14. From the **Exp** list, select the class of service to use when sending probes.  
   Range: 0 through 7  
15. From the **Fanout** list, select the maximum number of next hops to search per node.  
   Range: 1 through 16  
16. Select **Disable** check box to disable tracing for a specific FEC.  
   Range: 1 through 16 |
<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Enable an OAM ingress policy. | 1. Click **Ingress Policy** next to Oam.  
2. Click **Add** after selecting a policy member from the Non member list to add it to the Members list.  
3. Click **Remove** after selecting a policy from the Members list to remove it from the Members list.  
4. Click **Add All** to add all the Non members to the Members list.  
5. Click **Remove All** to remove all the members from the Members list. |
| Enable tracing of forwarding equivalence classes (FECs) for LDP LSPs. | 1. Click **Periodic Traceroute** next to Oam.  
2. In the **Comment** box, enter the comment.  
3. From the **Frequency** list, select the interval between traceroute attempts.  
   Range: 15 through 120 minutes  
4. From the **Ttl** list, select the maximum time-to-live value.  
   Range: 1 through 255  
5. From the **Retries** list, select the number of attempts to send a probe to a specific node before giving up.  
   Range: 1 through 9  
6. From the **Wait** list, select the wait interval before resending a probe packet.  
   Range: 5 though 15 seconds  
7. From the **Paths** list, select the maximum number of paths to search.  
   Range: 1 through 255  
8. In the **Source** box, enter the IPv4 source address to use when sending probes.  
9. From the **Exp** list, select the class of service to use when sending probes.  
   Range: 0 through 7  
10. From the **Fanout** list, select the maximum number of next hops to search per node.  
   Range: 1 through 16 |
### Table 140: LDP Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable policing of forwarding equivalence classes (FECs) for LDP.</td>
<td>1. Click <strong>Policing</strong> next to Ldp.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Fec</strong> next to Policing.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Add new entry</strong> next to Fec.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Name</strong> box, enter the address for the FEC.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>7. From the <strong>Ingress Traffic</strong> list, select the name of the filter for policing ingress FEC traffic.</td>
</tr>
<tr>
<td></td>
<td>8. From the <strong>Transit Traffic</strong> list, select the name of the filter for policing transit FEC traffic.</td>
</tr>
<tr>
<td>Specify the LDP session to which you want to attach the Transmission Control Protocol (TCP) MD5 signature.</td>
<td>1. Click <strong>Session</strong> next to Ldp.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Session.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the address for the remote end of the LDP session.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Authentication Key</strong> box, enter the authentication key.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Authentication Algorithm</strong> list, select the algorithm.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Authentication Key Chain</strong> box, enter the MD5 authentication signature. The maximum length of the authentication signature is 69 characters.</td>
</tr>
<tr>
<td>Configure session protection.</td>
<td>1. Click <strong>Session Protection</strong> next to Ldp.</td>
</tr>
<tr>
<td></td>
<td>2. From the <strong>Timeout</strong> list, select the session protection timeout.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 65535</td>
</tr>
<tr>
<td>Specify parameters for targeted hellos.</td>
<td>1. Click <strong>Targeted Hello</strong> next to Ldp.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. From the <strong>Hello Interval</strong> list, select the hello interval in seconds.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 65535</td>
</tr>
<tr>
<td></td>
<td>4. From the <strong>Hold Time</strong> list, select the hold time interval in seconds.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 65535</td>
</tr>
</tbody>
</table>
### Table 140: LDP Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure LDP protocol-level trace options. | 1. Click **Traceoptions** next to Ldp.  
2. In the **Comment** box, enter the comment for the traceoptions.  
3. Click **File** next to Traceoptions.  
4. In the **Comment** box, enter the comment for the file.  
5. In the **Filename** box, enter the name of the file to receive the output of the tracing operation.  
6. In the **Size** box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).  
7. From the **Files** list, select the maximum number of trace files.  
   Range: 2 through 1000  
8. Select one of the following:  
   - **world-readable**—To enable unrestricted file access.  
   - **no-world-readable**—To restrict file access to owner. This is the default setting. |
| Configure LDP traffic statistics. | 1. Click **Traffic Statistics** next to Ldp.  
2. In the **Comment** box, enter the comment.  
3. From the **Interval** list, select the interval at which the statistics are polled and written to the file.  
   Range: 60 through 65535  
4. Select **No Penultimate Hop** check box to disable penultimate hop statistics collection.  
5. Click **File** next to Traffic Statistics.  
6. In the **Comment** box, enter the comment for the file.  
7. In the **Filename** box, enter the name of the file to receive the output of the tracing operation.  
8. In the **Size** box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).  
9. From the **Files** list, select the maximum number of trace files.  
   Range: 2 through 1000  
10. Select one of the following:  
   - **world-readable**—To enable unrestricted file access.  
   - **no-world-readable**—To restrict file access to owner. This is the default setting. |
Table 140: LDP Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Allow control of the transport address used by LDP. | 1. Click **Transport Address** next to Ldp.  
2. In the **Comment** box, enter the comment.  
3. Click **Router Id** next to Transport Address.  
4. Select one of the following:  
  - **router-id**—The router identifier is used as the transport address.  
  - **interface**—The first IP address on the interface is used as the transport address.  
  - **address**—IP address to be advertised as the transport address. |

**Related Topics**
- Configuring the ILMI Protocol (NSM Procedure) on page 255
- Configuring RSVP (NSM Procedure) on page 351
- Configuring Link Management Protocol (NSM Procedure) on page 275

**Configuring Link Management Protocol (NSM Procedure)**

Link Management is a protocol used to define a forwarding adjacency between peers and to maintain and allocate resources on the traffic engineering links. It defines the data channel connection and the control channel connection between devices.

To configure link management in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Protocols > Link Management**.
4. Add or modify the settings as specified in Table 141 on page 276.
5. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.
Table 141: Link Management Protocol Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a network peer.</td>
<td>1. Click <strong>Peer</strong> next to Link Management.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Peer.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the name of the peer.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Address</strong> box, enter the ID of the peer.</td>
</tr>
<tr>
<td></td>
<td>6. Expand <strong>Peer</strong>.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>Control Channel</strong> next to Peer.</td>
</tr>
<tr>
<td></td>
<td>8. Click <strong>Add new entry</strong> next to Control Channel.</td>
</tr>
<tr>
<td></td>
<td>9. In the dialog box, enter the name of the control channel interface.</td>
</tr>
</tbody>
</table>
Table 141: Link Management Protocol Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a Lmp Control Channel</td>
<td>1. Click Lmp Control Channel next to peer.</td>
</tr>
<tr>
<td></td>
<td>2. Click Add new entry next to Lmp Control Channel.</td>
</tr>
<tr>
<td></td>
<td>3. In the Name box, enter the peer name.</td>
</tr>
<tr>
<td></td>
<td>4. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. In the Remote Address box, enter the remote IP address for the Link Management Protocol (LMP) control channel interface.</td>
</tr>
<tr>
<td></td>
<td>6. Click Lmp Protocol next to peer.</td>
</tr>
<tr>
<td></td>
<td>7. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>8. From the Hello Interval list, select how often the router sends Link Management Protocol (LMP) hello packets.</td>
</tr>
<tr>
<td></td>
<td>Range: 150 through 21845</td>
</tr>
<tr>
<td></td>
<td>Default: 150 milliseconds</td>
</tr>
<tr>
<td></td>
<td>9. From the Hello Dead Interval list, select how long the Link Management Protocol (LMP) waits before declaring the control channel to be dead.</td>
</tr>
<tr>
<td></td>
<td>Range: 500 through 300,000</td>
</tr>
<tr>
<td></td>
<td>Default: 500 milliseconds (three times the hello interval)</td>
</tr>
<tr>
<td></td>
<td>10. From the Retransmission Interval list, select how often Link Management Protocol (LMP) sends Config and LinkSummary messages on the LMP control channel.</td>
</tr>
<tr>
<td></td>
<td>Range: 500 through 300,000</td>
</tr>
<tr>
<td></td>
<td>Default: 500 milliseconds</td>
</tr>
<tr>
<td></td>
<td>11. From the Retry Limit list, select the maximum number of times messages are sent without receiving an acknowledgment.</td>
</tr>
<tr>
<td></td>
<td>Range: 3 through 1000</td>
</tr>
<tr>
<td></td>
<td>Default: 3</td>
</tr>
<tr>
<td></td>
<td>12. Select Passive check box to specify the router to not configure the Link Management Protocol (LMP) control channels, but to wait for the remote peer to configure the LMP control channels.</td>
</tr>
<tr>
<td></td>
<td>13. Click Te-Link next to peer.</td>
</tr>
<tr>
<td></td>
<td>14. Click Add new entry next to Te-Link.</td>
</tr>
<tr>
<td></td>
<td>15. In the dialog box, enter the name of the te-link to be associated with this peer.</td>
</tr>
</tbody>
</table>
Table 141: Link Management Protocol Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Represent a collection of physical ports or time slots. | 1. Click Add new entry next to Te Link.  
2. In the Name box, enter the name of the collection of physical ports or the name of the time slots.  
3. In the Comment box, enter the comment.  
4. In the Local Address box, enter the local IP address associated with the traffic engineering link.  
5. In the Remote Address box, enter the remote IP address for the traffic engineering link.  
6. From the Remote ID list, select the ID assigned to a traffic engineering link or an interface on the peer node.  
Range: 1 through 4294967295  
7. From the Te Metric list, select the metric value.  
Range: 1 through 65535  
8. Select Disable check box to disable the traffic engineering link or an interface to a traffic engineering link.  
9. Expand te-link.  
10. Click Interface next to te-link.  
   • Select interface to specify the egress router interface.  
   • Select label-switched-path to specify the LSP to be used by the forwarding adjacency. |

Specify trace options for the LMP protocol. | 1. In the Comment box, enter the comment.  
2. Expand Traceoptions.  
3. Click File next to Trace Options.  
4. In the Comment box, enter the comment.  
5. In the Filename box, enter the name of the file to receive the output of the tracing operation. Enclose the name within quotation marks.  
6. In the Size box, enter the maximum size of each trace file in kilobytes (KB), megabytes (MB) or gigabytes (GB).  
7. From the Files list, select the maximum number of files.  
8. Select world-readable to enable log file access to all users.  
9. Select no-world-readable to prevent all users from reading the log file.  
10. Click Flag next to Trace Options.  
11. Click Add new entry next to flag.  
12. From the Name list, select a tracing operation to perform.  
13. In the Comment box, enter the comment. |

Related Topics  • Configuring the ILMI Protocol (NSM Procedure) on page 255
Configuring RSVP (NSM Procedure) on page 351
- Configuring Layer 2 Circuit (NSM Procedure) on page 257

Configuring MPLS Protocol (NSM Procedure)

You can enable MPLS on the router using the MPLS option. See the following topics:

- Enabling MPLS on the Router (NSM Procedure) on page 279
- Configuring Administrative Group (NSM Procedure) on page 282
- Configuring Administrative Groups (NSM Procedure) on page 282
- Configuring Bandwidth for the Reroute Path (NSM Procedure) on page 283
- Configuring DiffServ-Aware Traffic Engineering (NSM Procedure) on page 284
- Configuring MPLS on Interfaces (NSM Procedure) on page 285
- Configure a Label Switched Path (LSP) to Use in Dynamic MPLS on page 287
- Configuring System Log Messages and SNMP Traps for LSPs (NSM Procedure) on page 313
- Configuring BFD for MPLS IPv4 LSPs (NSM Procedure) on page 314
- Configuring Named Paths (NSM Procedure) on page 316
- Configuring MTU Signaling in RSVPs (NSM Procedure) on page 317
- Configuring static LSPs on the Ingress Router (NSM Procedure) on page 318
- Configuring MPLS Statistics (NSM Procedure) on page 319
- Tracing MPLS Packets and Operations (NSM Procedure) on page 320

Enabling MPLS on the Router (NSM Procedure)

You can enable MPLS on the router using the MPLS option.

To enable MPLS on the router in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols.
4. Select Mpls.
5. Add or modify settings as specified in Table 142 on page 280.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
Table 142: MPLS Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Enable MPLS on the router. | 1. In the **Comment** box, enter the comment.  
2. Select the **Disable** check box to disable the functionality of the configured object.  
3. From the **Traffic Engineering** list, select whether MPLS performs traffic engineering on BGP destinations only or on both BGP and IGP destinations.  
4. From the **Advertisement Hold Time** list, select the hold time, in seconds.  
   Range: 0 through 65,535 seconds  
   Default: 5 seconds  
5. From the **Rsvp Error Hold Time** list, select the amount of time MPLS retains RSVP PathErr messages and considers them for CSPF computations.  
   Range: 0 through 240 seconds  
   Default: 25 seconds  
6. Select the **Optimize Aggressive** check box to enable aggressive optimization.  
7. From the **Smart Optimize Timer** list, select the number of seconds to wait before switching an LSP back to its original path.  
   Range: 0 through 65,535 seconds  
   Default: 180 seconds  
8. Select the **No Propagate Ttl** check box to disable normal time-to-live (TTL) decrementing.  
9. Select the **Explicit Null** check box to advertise label 0 to the egress router of an LSP.  
10. Select the **Ipv6 Tunneling** check box to allow IPv6 routes to be resolved over an MPLS network.  
11. Select the **Icmp Tunneling** check box to enable ICMP tunneling, which can be used for debugging and tracing purposes.  
12. From the **Revert Timer** list, select the amount of time (in seconds) that an LSP must wait before traffic reverts to a primary path.  
   Range: 0 through 65,535 seconds  
   Default: 60 seconds |
Your Action

13. Select the **Expand Loose Hop** check box to allow an LSP to traverse multiple OSPF areas within a service provider’s network.

14. From the **Class Of Service** list, select the CoS value.
   - Range: 0 through 7
   - Default: If you do not specify a CoS value, the IP precedence bits from the packet’s IP header are used as the packet’s CoS value.

15. Select the **No Decrement Ttl** check box to disable normal time-to-live (TTL) decrementing.

16. From the **Hop Limit** list, select the maximum number of hops.
   - Range: 2 through 255 (for an LSP); 0 through 255 (for fast reroute)
   - Default: 255 (for an LSP); 6 (for fast reroute)

17. Select the **No Cspf** check box to disable constrained-path LSP computation.

18. Select the **Admin Down** check box to indicate the administrative down status for an LSP.

19. From the **Optimize Timer** list, select the length of the optimize timer, in seconds.
   - Range: 0 through 65,535 seconds
   - Default: 0 seconds (the optimize timer is disabled)

20. From the **Preference** list, select the preference to assign to the route. A route with a lower preference value is preferred.
    - Range: 0 through 4,294,967,295
    - Default: 5 for static MPLS LSPs, 7 for RSVP MPLS LSPs, 9 for LDP MPLS LSPs

21. From the **Setup Priority** list, select the setup priority.
    - Range: 0 through 7, where 0 is the highest and 7 is the lowest priority
    - Default: 7 (The session cannot preempt any existing sessions.)

22. From the **Reservation Priority** list, select the reservation priority, used to keep a reservation after it has been set up.
    - Range: 0 through 7, where 0 is the highest and 7 is the lowest priority
    - Default: 0 (Once the session is set up, no other session can preempt it.)

23. Select one of the following:
   - **record**—to specify whether an LSP should actively record the routes in the path.
   - **no-record**—to specify whether an LSP should not record the routes in the path.

24. Select the **standby** check box to have the path remain up at all times to provide instant switchover if connectivity problems occur.

---

**Table 142: MPLS Configuration Details (continued)**

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>13. Select the <strong>Expand Loose Hop</strong> check box to allow an LSP to traverse multiple OSPF areas within a service provider’s network.</td>
<td></td>
</tr>
</tbody>
</table>
| 14. From the **Class Of Service** list, select the CoS value.  
   - Range: 0 through 7  
   - Default: If you do not specify a CoS value, the IP precedence bits from the packet’s IP header are used as the packet’s CoS value. | |
| 15. Select the **No Decrement Ttl** check box to disable normal time-to-live (TTL) decrementing. | |
| 16. From the **Hop Limit** list, select the maximum number of hops.  
   - Range: 2 through 255 (for an LSP); 0 through 255 (for fast reroute)  
   - Default: 255 (for an LSP); 6 (for fast reroute) | |
| 17. Select the **No Cspf** check box to disable constrained-path LSP computation. | |
| 18. Select the **Admin Down** check box to indicate the administrative down status for an LSP. | |
| 19. From the **Optimize Timer** list, select the length of the optimize timer, in seconds.  
   - Range: 0 through 65,535 seconds  
   - Default: 0 seconds (the optimize timer is disabled) | |
| 20. From the **Preference** list, select the preference to assign to the route. A route with a lower preference value is preferred.  
   - Range: 0 through 4,294,967,295  
   - Default: 5 for static MPLS LSPs, 7 for RSVP MPLS LSPs, 9 for LDP MPLS LSPs | |
| 21. From the **Setup Priority** list, select the setup priority.  
   - Range: 0 through 7, where 0 is the highest and 7 is the lowest priority  
   - Default: 7 (The session cannot preempt any existing sessions.) | |
Configuring Administrative Group (NSM Procedure)

You can configure an administrative group constraint for each LSP or for each primary or secondary LSP path using the Admin Group option.

To configure an administrative group in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols.
4. Select Mpls.
5. Add or modify settings as specified in Table 143 on page 282.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

Table 143: Administrative Group Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure administrative group. | 1. Click Admin Group next to Mpls.  
2. In the Comment box, enter the comment. |
| Define the administrative groups to exclude for an LSP or for a path’s primary and secondary paths. | 1. Click Exclude next to Admin Group.  
2. Click Add new entry next to Exclude.  
3. In the New exclude window, enter the names of one or more groups. |
| Require the LSP to traverse links that include all of the defined administrative groups. | 1. Click Include All next to Admin Group.  
2. Click Add new entry next to Include All.  
3. In the New include-all window, enter the names of one or more groups. |
| Define the administrative groups to include for an LSP or for a path’s primary and secondary paths. | 1. Click Include Any next to Admin Group.  
2. Click Add new entry next to Include Any.  
3. In the New include-any window, enter the names of one or more groups. |

Configuring Administrative Groups (NSM Procedure)

You can configure administrative groups to implement link coloring of resource classes using the Admin Groups option.

To configure administrative groups in NSM:

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

5. Add or modify settings as specified in Table 144 on page 283.

6. Click one:

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

### Table 144: Administrative Groups Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure administrative groups.                                   | 1. Click **Admin Groups** next to Mpls.  
|                                                                     | 2. Click **Add new entry** next to Admin Groups.  
|                                                                     | 3. In the **Name** box, enter the name of the group. You can assign up to 32 names.  
|                                                                     | 4. In the **Comment** box, enter the comment.  
|                                                                     | 5. From the **Group Value** list, select the value assigned to the group.  
|                                                                     | Range: 0 through 31 |
| Define the administrative groups to exclude for an LSP or for a path’s primary and secondary paths. | 1. Click **Exclude** next to Admin Group.  
|                                                                     | 2. Click **Add new entry** next to Exclude.  
|                                                                     | 3. In the **New exclude** window, enter the names of one or more groups. |
| Require the LSP to traverse links that include all of the defined administrative groups. | 1. Click **Include All** next to Admin Group.  
|                                                                     | 2. Click **Add new entry** next to Include All.  
|                                                                     | 3. In the **New include-all** window, enter the names of one or more groups. |
| Define the administrative groups to include for an LSP or for a path’s primary and secondary paths. | 1. Click **Include Any** next to Admin Group.  
|                                                                     | 2. Click **Add new entry** next to Include Any.  
|                                                                     | 3. In the **New include-any** window, enter the names of one or more groups. |

### Configuring Bandwidth for the Reroute Path (NSM Procedure)

When configuring fast reroute, allocate bandwidth for the reroute path. By default, no bandwidth is reserved for the rerouted path. The fast reroute bandwidth does not need to be identical to that allocated for the LSP itself.

To configure bandwidth for the reroute path in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Mpls**.
5. Add or modify settings as specified in Table 145 on page 284.
6. Click one:
Table 145: Automatic Policers Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Allocate bandwidth for the reroute path. | 1. Click **Bandwidth** next to Mpls.  
| | 2. In the **Comment** box, enter the comment.  
| | 3. In the **Per Traffic Class Bandwidth** box, enter the bandwidth, in bits per second.  
| | 4. In the **Ct0** box, enter the bandwidth, for the specified class.  
| | 5. In the **Ct1** box, enter the bandwidth, for the specified class.  
| | 6. In the **Ct2** box, enter the bandwidth, for the specified class.  
| | 7. In the **Ct3** box, enter the bandwidth, for the specified class. |
| Apply the same policer action to all the class types. | 1. Click **Class** next to Automatic Policing.  
| | 2. Click **Add new entry** next to Class.  
| | 3. From the **Name** list, select the class type to which the policer action is to be applied.  
| | 4. In the **Comment** box, enter the comment.  
| | 5. Select one of the policer actions.  
| | • **drop**—Drop all packets.  
| | • **loss-priority-high**—Set the packet loss priority (PLP) to high.  
| | • **loss-priority-low**—Set the PLP to low. |

Configuring DiffServ-Aware Traffic Engineering (NSM Procedure)

Differentiated Services (DiffServ)-aware traffic engineering provides a way to guarantee a specified level of service over an MPLS network. The routers providing DiffServ-aware traffic engineering are part of a differentiated services network domain. All routers participating in a differentiated services domain must have DiffServ-aware traffic engineering enabled.

To configure DiffServ-aware traffic engineering in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Mpls**.
5. Add or modify settings as specified in Table 146 on page 285.
6. Click one:  
   • **OK**—Saves the changes.  
   • **Cancel**— Cancels the modifications.
Table 146: Diffserv-Aware Traffic Engineering Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure Diffserv-aware traffic engineering. | 1. Click Diffserv Te next to Mpls.  
2. In the Comment box, enter the comment.  
3. In the Per Traffic Class Bandwidth box, enter the bandwidth, in bits per second.  
4. From the Bandwidth Model list, select the bandwidth model for differentiated services.  
   - extended-mam—The extended maximum allocation model (MAM) is a bandwidth model based on MAM.  
   - mam—The MAM is defined in RFC 4125, Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering.  
   - rdm—The Russian dolls bandwidth allocation model (RDM) is defined in RFC 4127, Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering. |

Specify the traffic engineering class matrix for a multiclass label switched path (LSP) or a Diffserv-aware traffic engineering LSP.

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
|      | 1. Click Te Class Matrix next to Diffserv Te.  
2. In the Comment box, enter the comment.  
3. For the traffic engineering classes, configure the following:  
a. In the Comment box, enter the comment.  
b. From the Traffic Class list, select the traffic class for the traffic engineering class.  
c. From the Priority list, select the priority of the class type. Range: 0 through 7 |

Configuring MPLS on Interfaces (NSM Procedure)

To configure MPLS on interfaces in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols.
4. Select Mpls.
5. Add or modify settings as specified in Table 147 on page 286.
6. Click one:  
   - OK—Saves the changes.  
   - Cancel— Cancels the modifications.
### Table 147: Interface Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| **Enable MPLS on one or more interfaces.** | 1. Click **Interface** next to Mpls.  
2. Click **Add new entry** next to Interface.  
3. In the **Name** box, enter the Name of the interface on which to configure MPLS.  
4. In the **Comment** box, enter the comment.  
5. Select the **Disable** check box to disable the functionality of the configured object. |
| **Define administrative groups for an interface.** | 1. Click **Admin Group** next to interface.  
2. In the **Comment** box, enter the comment.  
3. Click **Add new entry** next to Admin Group.  
4. In the **New admin-group** window, enter one or more names of groups. |
| **Label MPLS packets.** | 1. Click **Label Map** next to interface.  
2. Click **Add new entry** next to Label Map.  
3. In the **Name** box, enter the interface name.  
4. From the **Swap** list, select the label value.  
   Range: 1,000,000 through 1,048,575. Labels 0 through 999,999 are for internal use. Labels 1,000,000 through 1,048,575 are unassigned by the JUNOS Software and are available for static label switched paths (LSPs). When you configure static LSPs, you can use only this range of labels.  
5. From the **Swap Label** list, select the label value.  
6. From the **Push Label** list, select the label value.  
   Range: 0 through 1,048,575  
7. Select the **Pop** check box to remove the label from the top of the label stack.  
8. From the **Preference** list, select the preference to be assigned to the route.  
   Range: 0 through 4,294,967,295  
   Default: 5 for static MPLS LSPs, 7 for RSVP MPLS LSPs, 9 for LDP MPLS LSPs  
9. From the **Class of Service** list, select the CoS value.  
   Range: 0 through 7  
   Default: If you do not specify a CoS value, the IP precedence bits from the packet’s IP header are used as the packet’s CoS value |
| **Configure IP address of the next hop to the destination.** | 1. Select one of the following:  
   - **next-hop**—to configure the IP address of the next hop to the destination.  
     a. Enter the IP address of the next-hop router.  
   - **reject**—to reject the packet.  
   - **discard**—to discard the packet. |
Configure a Label Switched Path (LSP) to Use in Dynamic MPLS

- Configuring Label Switched Path (NSM Procedure) on page 287
- Configuring Administrative Group (NSM Procedure) on page 290
- Configuring Automatic Bandwidth Allocation for LSPs (NSM Procedure) on page 291
- Configuring Bandwidth for the Reroute Path (NSM Procedure) on page 292
- Configuring Fast Reroute (NSM Procedure) on page 293
- Adding LSP-Related Routes to the inet.3 Routing Table (NSM Procedure) on page 294
- Configuring MPLS LSPs for GMPLS (NSM Procedure) on page 295
- Configuring BFD for MPLS IPv4 LSPs (NSM Procedure) on page 296
- Configuring the Primary Point-to-Multipoint LSP (NSM Procedure) on page 298
- Configuring Policers for LSPs (NSM Procedure) on page 299
- Configuring Primary Paths for an LSP (NSM Procedure) on page 300
- Configuring Secondary Paths for an LSP (NSM Procedure) on page 305

**Configuring Label Switched Path (NSM Procedure)**

You can configure a label switched path (LSP) to use in dynamic MPLS.

To configure a LSP in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in Table 148 on page 288.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.
Table 148: LSP Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure label switched path. | 1. Click **Add new entry** next to Label Switched Path.  
2. In the **Name** box, enter the name that identifies the LSP.  
3. In the **Comment** box, enter the comment.  
4. Select the **Disable** check box to disable the functionality of the configured object.  
5. Select the **No Install To Address** check box to prevent the egress router address configured using the to statement from being installed into the inet.3 and inet.0 routing tables.  
6. Select the **Backup** check box to configure a backup provider edge (PE) group for ingress PE router redundancy when point-to-multipoint LSP are used for multicast distribution.  
7. In the **From** box, enter the source address to use for the LSP.  
8. Select the **Ldp Tunneling** check box to enable the LSP to be used for LDP tunneling.  
9. From the **Metric** list, select the LSP metric value  
   Default: No metric assigned (dynamic)  
   Range: 1 through 16,777,215  
10. From the **Retry Timer** list, select the amount of time between attempts to connect to the primary path.  
    Default: 30 seconds  
    Range: 1 through 600 seconds  
11. From the **Retry Limit** list, select the maximum number of tries to establish the primary path.  
    Default: 0 (The ingress node never stops trying to establish the primary path.)  
    Range: 0 through 10,000  
12. From the **Revert Timer** list, select the amount of time (in seconds) that an LSP must wait before traffic reverts to a primary path.  
    Default: 60 seconds  
    Range: 0 through 65,535 seconds  
13. From the **Class Of Service** list, select the CoS value.  
    Range: 0 through 7  
    Default: If you do not specify a CoS value, the IP precedence bits from the packet's IP header are used as the packet's CoS value.  
14. Select the **No Decrement Ttl** check box to disable normal time-to-live (TTL) decrementing.  
15. From the **Hop Limit** list, select the maximum number of hops.  
    Range: 2 through 255 (for an LSP); 0 through 255 (for fast reroute)  
    Default: 255 (for an LSP); 6 (for fast reroute)  
16. Select the **No Csfp** check box to disable constrained-path LSP computation. |
Table 148: LSP Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.</td>
<td>Select the Admin Down check box to set the A-bit in the Admin Status object.</td>
</tr>
</tbody>
</table>
| 18.  | From the Optimize Timer list, select the length of the optimize timer, in seconds.  
    | Range: 0 through 65,535 seconds  
    | Default: 0 seconds (the optimize timer is disabled) |
| 19.  | From the Preference list, select the preference to assign to the route.  
    | Range: 1 through 255  
    | Default: 5 for static MPLS LSPs, 7 for RSVP MPLS LSPs, 9 for LDP MPLS LSPs |
| 20.  | From the Setup Priority list, select the setup priority.  
    | Range: 0 through 7, where 0 is the highest and 7 is the lowest priority.  
    | Default: 7 (The session cannot preempt any existing sessions.) |
| 21.  | From the Reservation Priority list, select the reservation priority.  
    | Range: 0 through 7, where 0 is the highest and 7 is the lowest priority.  
    | Default: 0 (Once the session is set up, no other session can preempt it.) |
Table 148: LSP Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 22.  | Select one of the following:  
|      | • record—Record routes  
|      | • no-record—Does not record routes |
| 23.  | Select the Standby check box to have the path remain up at all times to provide instant switchover if connectivity problems occur.  
| 24.  | Select one of the following options:  
|      | • random—Choose the path at random.  
|      | • least-fill—Prefer the path with the most available bandwidth (with the largest minimum available bandwidth ratio).  
|      | • most-fill—Prefer the path with the least available bandwidth (with the minimum available bandwidth ratio). The minimum available bandwidth ratio of a path is the smallest available bandwidth ratio belonging to any of the links in the path.  
| 25.  | In the Description box, enter the textual description of the LSP.  
| 26.  | Select one of the following options:  
|      | • link-protection—Enable link protection.  
|      | • node-link-protection—Enable node and link protection on the specified LSP.  
|      | • most-fill—Prefer the path with the least available bandwidth (with the minimum available bandwidth ratio). The minimum available bandwidth ratio of a path is the smallest available bandwidth ratio belonging to any of the links in the path.  
| 27.  | Select the Adaptive check box for RSVP to use shared explicit (SE) reservation styles and assists in smooth transition during rerouting.  
| 28.  | Select the Associate backup Pe Groups check box to enable an LSP to monitor the status of its destination PE router.  

Configuring Administrative Group (NSM Procedure)

You can configure an administrative group constraint for each Label Switched Path (LSP) or for each primary or secondary LSP path using the Admin Group option.

To configure an administrative group in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.  
2. Click the Device Tree tab, and then double-click the device to select it.  
3. Click the Configuration tab. In the configuration tree, expand Protocols > MPLS.  
4. Select Label Switched Path.  
5. Add or modify settings as specified in Table 149 on page 291.  
6. Click one:  
   • OK—Saves the changes.
• Cancel—Cancels the modifications.

Table 149: Administrative Group Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure administrative group.</td>
<td>1. Click Add new entry next to Label Switched Path.</td>
</tr>
<tr>
<td></td>
<td>2. Click Admin Group next to label-switched-path.</td>
</tr>
<tr>
<td></td>
<td>3. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td>Define the administrative groups to exclude for an LSP or for a path’s primary and secondary paths.</td>
<td>1. Click Exclude next to Admin Group.</td>
</tr>
<tr>
<td></td>
<td>2. Click Add new entry next to Exclude.</td>
</tr>
<tr>
<td></td>
<td>3. In the New exclude window, enter the names of one or more groups.</td>
</tr>
<tr>
<td>Require the LSP to traverse links that include all of the defined administrative groups.</td>
<td>1. Click Include All next to Admin Group.</td>
</tr>
<tr>
<td></td>
<td>2. Click Add new entry next to Include All.</td>
</tr>
<tr>
<td></td>
<td>3. In the New include-all window, enter the names of one or more groups.</td>
</tr>
<tr>
<td>Define the administrative groups to include for an LSP or for a path’s primary and secondary paths.</td>
<td>1. Click Include Any next to Admin Group.</td>
</tr>
<tr>
<td></td>
<td>2. Click Add new entry next to Include Any.</td>
</tr>
<tr>
<td></td>
<td>3. In the New include-any window, enter the names of one or more groups.</td>
</tr>
</tbody>
</table>

Configuring Automatic Bandwidth Allocation for LSPs (NSM Procedure)

Automatic bandwidth allocation allows an MPLS tunnel to automatically adjust its bandwidth allocation based on the volume of traffic flowing through the tunnel. You can configure an LSP with minimal bandwidth, and this feature can dynamically adjust the LSP’s bandwidth allocation based on current traffic patterns.

To configure automatic bandwidth allocation in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols > MPLS.
4. Select Label Switched Path.
5. Add or modify settings as specified in Table 150 on page 292.
6. Click one:
   • OK—Saves the changes.
   • Cancel— Cancels the modifications.
Table 150: Automatic Bandwidth Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure automatic bandwidth.</td>
<td>1. Click Add new entry next to Label Switched Path.</td>
</tr>
<tr>
<td></td>
<td>2. Click Auto Bandwidth next to label-switched-path.</td>
</tr>
<tr>
<td></td>
<td>3. Select the Enable Feature check box to enable the option.</td>
</tr>
<tr>
<td></td>
<td>4. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. From the Adjust Interval list, select the bandwidth reallocation interval, in seconds.</td>
</tr>
<tr>
<td></td>
<td>Range: 300 through 4,294,967,295 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 86,400 seconds</td>
</tr>
<tr>
<td></td>
<td>6. From the Adjust Threshold list, select the threshold for automatic bandwidth adjustment.</td>
</tr>
<tr>
<td></td>
<td>7. In the Minimum Bandwidth box, enter the minimum bandwidth in bits per second (bps) for an LSP with automatic bandwidth allocation enabled.</td>
</tr>
<tr>
<td></td>
<td>8. In the Maximum Bandwidth box, enter the maximum amount of bandwidth in bits per second (bps).</td>
</tr>
<tr>
<td></td>
<td>9. Select the Monitor Bandwidth check box to configure passive bandwidth utilization monitoring.</td>
</tr>
<tr>
<td></td>
<td>10. From the Adjust Threshold Overflow Limit list, select the number of consecutive bandwidth overflow samples.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 65,535</td>
</tr>
</tbody>
</table>

Configuring Bandwidth for the Reroute Path (NSM Procedure)

When configuring fast reroute, allocate bandwidth for the reroute path. By default, no bandwidth is reserved for the rerouted path. The fast reroute bandwidth does not need to be identical to that allocated for the LSP itself.

To configure bandwidth for the reroute path in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols > Mpls.
4. Select Label Switched Path.
5. Add or modify settings as specified in Table 151 on page 293.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.
Table 151: Bandwidth Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocate bandwidth for the reroute path.</td>
<td>1. Click <strong>Add new entry</strong> next to Label Switched Path.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Bandwidth</strong> next to label-switched-path.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Per Traffic Class Bandwidth</strong> box, enter the bandwidth, in bits per second.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Ct0</strong> box, enter the bandwidth, for the specified class.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Ct1</strong> box, enter the bandwidth, for the specified class.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Ct2</strong> box, enter the bandwidth, for the specified class.</td>
</tr>
<tr>
<td></td>
<td>8. In the <strong>Ct3</strong> box, enter the bandwidth, for the specified class.</td>
</tr>
</tbody>
</table>

**Configuring Fast Reroute (NSM Procedure)**

Fast reroute provides a mechanism for automatically rerouting traffic on an LSP if a node or link in an LSP fails, thus reducing the loss of packets traveling over the LSP.

To configure fast reroute in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **LabelSwitchedPath**.
5. Add or modify settings as specified in Table 152 on page 293.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.

Table 152: Fast Reroute Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure fast reroute.</td>
<td>1. Click <strong>Fast Reroute</strong> next to Label Switched Path.</td>
</tr>
<tr>
<td></td>
<td>2. Select the <strong>Enable Feature</strong> check box to enable the option.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. From the <strong>Hop Limit</strong> list, select the maximum number of hops. Range: 2 through 255 (for an LSP); 0 through 255 (for fast reroute) Default: 255 (for an LSP); 6 (for fast reroute)</td>
</tr>
</tbody>
</table>

Allocate bandwidth for the reroute path.

1. Click **Bandwidth** next to Fast Reroute.
2. Select one of the following:
   - **bandwidth**—specify the traffic rate associated with the LSP and enter the bandwidth.
   - **bandwidth-percent**—configure the percentage of bandwidth to reserve for the detour path in case the primary path for a traffic engineered LSP or a multiclass LSP fails and select the bandwidth percentage.
Table 152: Fast Reroute Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control exclusion of administrative groups.</td>
<td>1. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• exclude—Define the administrative groups to exclude for fast reroute.</td>
</tr>
<tr>
<td></td>
<td>a. Click Add new entry next to exclude.</td>
</tr>
<tr>
<td></td>
<td>b. In the New exclude window, enter the names of one or more groups.</td>
</tr>
<tr>
<td></td>
<td>• no-exclude—Disable administrative group exclusion.</td>
</tr>
<tr>
<td>Control inclusion of administrative groups.</td>
<td>1. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• include-all—Define the administrative groups that must all be included for fast reroute.</td>
</tr>
<tr>
<td></td>
<td>a. Click Add new entry next to include-all.</td>
</tr>
<tr>
<td></td>
<td>b. In the New include-all window, enter the names of one or more groups.</td>
</tr>
<tr>
<td></td>
<td>• no-include-all—Disable administrative group inclusion.</td>
</tr>
<tr>
<td>Control inclusion of administrative groups.</td>
<td>1. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• include-any—Define the administrative groups to include for fast reroute.</td>
</tr>
<tr>
<td></td>
<td>a. Click Add new entry next to include-any.</td>
</tr>
<tr>
<td></td>
<td>b. In the New include-any window, enter the names of one or more groups.</td>
</tr>
<tr>
<td></td>
<td>• no-include-any—Disable administrative group inclusion.</td>
</tr>
</tbody>
</table>

Adding LSP-Related Routes to the inet.3 Routing Table (NSM Procedure)

By default, a host route toward the egress router is installed in the inet.3 routing table. Installing the host route allows BGP to perform next-hop resolution. It also prevents the host route from interfering with prefixes learned from dynamic routing protocols and stored in the inet.0 routing table.

To add additional routes into the inet.3 routing table in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in Table 153 on page 295.
6. Click one:
   • **OK**—Saves the changes.
   • **Cancel**— Cancels the modifications.
Table 153: Install Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Associate one or more prefixes with an LSP. | 1. Click **Add new entry** next to Label Switched Path.  
2. Click **Install** next to label-switched-path.  
3. Click **Add new entry** next to Install.  
4. In the **Name** box, enter the routing table.  
5. In the **Comment** box, enter the comment.  
6. Select the **Active** check box to install the route into the inet.0 routing table. This allows you to issue a ping or traceroute command on this address. |

Configuring MPLS LSPs for GMPLS (NSM Procedure)

To enable the proper GMPLS switching parameters you can use the Lsp Attributes option.

To configure the LSP attributes in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in Table 154 on page 296.
6. Click one:  
   - **OK**—Saves the changes.  
   - **Cancel**— Cancels the modifications.
Table 154: Lsp Attributes Configuration Details

<table>
<thead>
<tr>
<th>Task Description</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define the parameters signaled during LSP setup.</td>
<td>1. Click <strong>Add new entry</strong> next to Label Switched Path.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Lsp Attributes</strong> next to label-switched-path.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. From the <strong>Signal Bandwidth</strong> list, select the type of bandwidth encoding used on the LSP. The options available for selection are 10gigether, ds1, ds3, e1, e3, ethernet, fastether, gigether, stm-1, stm-4, stm-16, stm-64, stm-256, sts-1, vt1-5, or vt2.</td>
</tr>
<tr>
<td></td>
<td>5. From the <strong>Switching Type</strong> list, select the switching method for the LSP. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>fiber</strong>—Fiber switching</td>
</tr>
<tr>
<td></td>
<td>• <strong>lambda</strong>—Lambda switching</td>
</tr>
<tr>
<td></td>
<td>• <strong>psc-1</strong>—Packet switching</td>
</tr>
<tr>
<td></td>
<td>• <strong>tdm</strong>—Time-division multiplexing (TDM) switching</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Encoding Type</strong> list, select the encoding type of payload carried by the LSP. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>ethernet</strong>—Ethernet</td>
</tr>
<tr>
<td></td>
<td>• <strong>packet</strong>—Packet</td>
</tr>
<tr>
<td></td>
<td>• <strong>pdh</strong>—Plesiochronous digital hierarchy (PDH)</td>
</tr>
<tr>
<td></td>
<td>• <strong>sonet-sdh</strong>—SONET/SDH</td>
</tr>
<tr>
<td></td>
<td>7. From the <strong>Gpid</strong> list, select the type of payload carried by the LSP. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>ethernet</strong>—Ethernet (GPID value: 33)</td>
</tr>
<tr>
<td></td>
<td>• <strong>hdlc</strong>—High-level Data Link Control (HDLC) (GPID value: 44)</td>
</tr>
<tr>
<td></td>
<td>• <strong>ipv4</strong>—IP version 4 (GPID value: 0x0800)</td>
</tr>
<tr>
<td></td>
<td>• <strong>pos-no-scrambling-crc-16</strong>—for interoperability with other vendors’ equipment (GPID value: 29)</td>
</tr>
<tr>
<td></td>
<td>• <strong>pos-no-scrambling-crc-32</strong>—for interoperability with other vendors’ equipment (GPID value: 30)</td>
</tr>
<tr>
<td></td>
<td>• <strong>pos-scrambling-crc-16</strong>—for interoperability with other vendors’ equipment (GPID value: 31)</td>
</tr>
<tr>
<td></td>
<td>• <strong>pos-scrambling-crc-32</strong>—for interoperability with other vendors’ equipment (GPID value: 32)</td>
</tr>
<tr>
<td></td>
<td>• <strong>ppp</strong>—Point-to-Point Protocol (PPP) (GPID value: 50)</td>
</tr>
</tbody>
</table>

**Configuring BFD for MPLS IPv4 LSPs (NSM Procedure)**

You can configure BFD for LSPs that use either LDP or RSVP as the signaling protocol using the Oam option.

To configure BFD for LSPs in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in Table 155 on page 297.

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

### Table 155: Oam Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable OAM for RSVP-signaled LSPs.</td>
<td>1. Click <strong>Add new entry</strong> next to Label Switched Path.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Oam</strong> next to label-switched-path.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. From the <strong>Lsp Ping Interval</strong> list, select the duration of the LSP</td>
</tr>
<tr>
<td></td>
<td>ping interval in seconds.</td>
</tr>
<tr>
<td></td>
<td>Range: 30 through 3,600 seconds</td>
</tr>
<tr>
<td>Enable Bidirectional Forwarding Detection (BFD) for all of the MPLS</td>
<td>1. Click <strong>Bfd Liveness Detection</strong> next to Oam.</td>
</tr>
<tr>
<td>LSPs or for just a specific LSP.</td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. From the <strong>Version</strong> list, select the BFD version to be used for detection.</td>
</tr>
<tr>
<td></td>
<td>4. From the <strong>Minimum Interval</strong> list, select the minimum transmit and</td>
</tr>
<tr>
<td></td>
<td>receive interval.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 255,000 milliseconds</td>
</tr>
<tr>
<td></td>
<td>5. From the <strong>Minimum Receive Interval</strong> list, select the minimum receive</td>
</tr>
<tr>
<td></td>
<td>interval.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 255,000 milliseconds</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Multiplier</strong> list, select the detection time multiplier.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 255</td>
</tr>
<tr>
<td></td>
<td>Default: 3</td>
</tr>
<tr>
<td></td>
<td>7. Select the <strong>No Adaptation</strong> check box to disable BFD adaptation.</td>
</tr>
<tr>
<td>Specify the threshold for the adaptation of the detection time.</td>
<td>1. Click <strong>Detection Time</strong> next to Bfd Liveness Detection.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. From the <strong>Threshold</strong> list, select the threshold for detecting the</td>
</tr>
<tr>
<td></td>
<td>adaptation of the transmit interval.</td>
</tr>
<tr>
<td>Configure route and next-hop properties in the event of a BFD</td>
<td>1. Click <strong>Failure Action</strong> next to Bfd Liveness Detection.</td>
</tr>
<tr>
<td>protocol session failure event on an RSVP label-switched path.</td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Teardown</strong> next to Failure Action.</td>
</tr>
<tr>
<td></td>
<td>4. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• teardown—when a BFD session fails for an RSVP LSP, the associated</td>
</tr>
<tr>
<td></td>
<td>LSP path is taken down and resignaled immediately.</td>
</tr>
<tr>
<td></td>
<td>• make-before-break—when a BFD session fails for an RSVP LSP, an attempt</td>
</tr>
<tr>
<td></td>
<td>is made to signal a new LSP path before tearing down the old LSP path.</td>
</tr>
<tr>
<td></td>
<td>a. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>b. From the <strong>Teardown Timeout</strong> list, select the time in seconds.</td>
</tr>
</tbody>
</table>
Table 155: Oam Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify the minimum transmit interval for failure detection. | 1. Click **Transmit Interval** next to Failure Action Detection.  
2. In the **Comment** box, enter the comment.  
3. From the **Minimum Interval** list, select the minimum interval at which the local router transmits hello packets to the neighbor with which it has established a BFD session.  
4. From the **Threshold** list, select the threshold for detecting the adaptation of the transmit interval. Range: 0 to 4,294,967,295 |
| Configure MPLS tracing options. | 1. Click **Traceoptions** next to Oam.  
2. In the **Comment** box, enter the comment.  
3. Select the **No Remote Trace** check box to disable remote tracing globally or for a specific tracing operation.  
4. Click **File** next to Traceoptions.  
5. In the **Filename** box, enter the name of the file to receive the output of the tracing operation.  
6. In the **Size** box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).  
7. From the **Files** list, select the maximum number of trace files. Range: 2 through 1000  
8. Select one of the following:  
   • world-readable—To enable unrestricted file access.  
   • no-world-readable—To restrict file access to owner.  
9. In the **Match** box, enter the regular expression.  
10. Click **Flag** next to Traceoptions.  
11. Click **Add new entry** next to Flag  
12. From the **Name** list, select the flag.  
13. In the **Comment** box, enter the comment. |

Configuring the Primary Point-to-Multipoint LSP (NSM Procedure)
A point-to-multipoint LSP must have a configured primary point-to-multipoint LSP to carry traffic from the ingress router. The configuration of the primary point-to-multipoint LSP is similar to a signaled LSP. You can specify an LSP as either a point-to-multipoint LSP or as a branch LSP of a point-to-multipoint LSP by specifying the point-to-multipoint LSP path name.

To configure the primary Point-to-Multipoint LSP in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.  
2. Click the **Device Tree** tab, and then double-click the device to select it.  
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.  
4. Select **Label Switched Path**.  
5. Add or modify settings as specified in Table 156 on page 299.  
6. Click one:
• OK—Saves the changes.
• Cancel—Cancels the modifications.

Table 156: P2mp Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure the primary Point-to-Multipoint LSP. | 1. Click Add new entry next to Label Switched Path.  
2. Click P2mp next to label-switched-path.  
3. Select the Enable Feature check box to enable the option.  
4. In the Comment box, enter the comment.  
5. In the Path_name box, enter the name of the point-to-multipoint LSP path that identifies the sequence of nodes that form the point-to-multipoint LSP. |

Configuring Policers for LSPs (NSM Procedure)

MPLS LSP policing allows you to control the amount of traffic forwarded through a particular LSP. Policing helps to ensure that the amount of traffic forwarded through an LSP never exceeds the requested bandwidth allocation. LSP policing is supported on regular LSPs, LSPs configured with DiffServ-aware traffic engineering, and multiclass LSPs. You can configure multiple policers for each multiclass LSP. For regular LSPs, each LSP policer is applied to all of the traffic traversing the LSP. The policer's bandwidth limitations become effective as soon as the total sum of traffic traversing the LSP exceeds the configured limit.

To configure policers for LSPs in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols > Mpls.
4. Select Label Switched Path.
5. Add or modify settings as specified in Table 157 on page 299.
6. Click one:
   • OK—Saves the changes.
   • Cancel—Cancels the modifications.

Table 157: Policer Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify the policing filter for the LSP. | 1. Click Add new entry next to Label Switched Path.  
2. Click Policing next to label-switched-path.  
3. In the Comment box, enter the comment.  
4. From the Filter list, select the name of the policing filter.  
5. Select the No Auto Policing check box to disable automatic policing on this LSP. |
Configuring Primary Paths for an LSP (NSM Procedure)

You can specify the primary path to use for an LSP using the Primary option. You can configure only one primary path. You can optionally specify preference, CoS, and bandwidth values for the primary path, which override any equivalent values that you configure for the LSP.

To configure primary paths for an LSP in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols > Mpls.
4. Select LabelSwitchedPath.
5. Add or modify settings as specified in Table 158 on page 300.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 158: Primary Paths Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the primary paths for an LSP.</td>
<td>1. Click <strong>Add new entry</strong> next to Label Switched Path.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Primary</strong> next to label-switched-path.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add new entry</strong> next to Primary.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Name</strong> box, enter the name of a path.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Class Of Service</strong> list, select the CoS value. Range: 0 through 7.</td>
</tr>
<tr>
<td></td>
<td>Default: If you do not specify a CoS value, the IP precedence bits from the packet’s IP header are used as the packet’s CoS value.</td>
</tr>
<tr>
<td></td>
<td>7. Select the <strong>No Decrement Ttl</strong> check box to disable normal time-to-live (TTL) decrementing.</td>
</tr>
<tr>
<td></td>
<td>8. From the <strong>Hop Limit</strong> list, select the maximum number of hops. Range: 2 through 255 (for an LSP); 0 through 255 (for fast reroute)</td>
</tr>
<tr>
<td></td>
<td>9. Select the <strong>No Cspf</strong> check box to disable constrained-path LSP computation.</td>
</tr>
</tbody>
</table>
Your Action

10. Select the **Admin Down** check box to set the A-bit in the Admin Status object.
11. From the **Optimize Timer** list, select the length of the optimize timer, in seconds.
   Range: 0 through 65,535 seconds
   Default: 0 seconds (the optimize timer is disabled)
12. From the **Preference** list, select the preference to assign to the route.
   Range: 0 to 4,294,967,295
   Default: 5 for static MPLS LSPs, 7 for RSVP MPLS LSPs, 9 for LDP MPLS LSPs
13. From the **Setup Priority** list, select the setup priority.
   Range: 0 through 7, where 0 is the highest and 7 is the lowest priority.
14. From the **Reservation Priority** list, select the reservation priority.
   Range: 0 through 7, where 0 is the highest and 7 is the lowest priority.
15. Select one of the following:
   - **record**—Record routes
   - **no-record**—Does not record routes
16. Select the **Standby** check box to have the path remain up at all times to provide instant switchover if connectivity problems occur.
17. Select the **Adaptive** check box for RSVP to use shared explicit (SE) reservation styles and assists in smooth transition during rerouting.
18. From the **Select** list, select the conditions under which the path is selected to carry traffic. Select one the following:
   - **manual**—The path is selected for carrying traffic if it is up and stable for at least the revert timer window (potentially before the revert timer has elapsed). Traffic is sent to other working paths if the current path is down or degraded (receiving errors).
   - **unconditional**—The path is always selected for carrying traffic, even if it is currently down or degraded (receiving errors).

### Configuring Administrative Group (NSM Procedure)

You can configure an administrative group constraint for each LSP or for each primary or secondary LSP path using the Admin Group option.

To configure administrative group in NSM:

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

5. Add or modify settings as specified in Table 159 on page 302.

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

### Table 159: Administrative Group Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure administrative group. | 1. Click **Add new entry** next to Label Switched Path.  
2. Click **Primary** next to label-switched-path.  
3. Click **Add new entry** next to Primary.  
4. Click **Admin Group** next to Primary.  
5. In the **Comment** box, enter the comment. |
| Define the administrative groups to exclude for an LSP or for a path’s primary and secondary paths. | 1. Click **Exclude** next to Admin Group.  
2. Click **Add new entry** next to Exclude.  
3. In the **New exclude** window, enter the names of one or more groups. |
| Require the LSP to traverse links that include all of the defined administrative groups. | 1. Click **Include All** next to Admin Group.  
2. Click **Add new entry** next to Include All.  
3. In the **New include-all** window, enter the names of one or more groups. |
| Define the administrative groups to include for an LSP or for a path’s primary and secondary paths. | 1. Click **Include Any** next to Admin Group.  
2. Click **Add new entry** next to Include Any.  
3. In the **New include-any** window, enter the names of one or more groups. |

### Configuring Class-Type Bandwidth Constraints for Multiclass LSPs (NSM Procedure)

You configure a multiclass LSP by using the Bandwidth option.

To configure bandwidth for the multiclass LSP in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in Table 160 on page 303.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
Table 160: Bandwidth Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure an LSP as a multiclass LSP.</td>
<td>1. Click <strong>Add new entry</strong> next to Label Switched Path.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Primary</strong> next to label-switched-path.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add new entry</strong> next to primary.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Bandwidth</strong> next to Primary.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Per Traffic Class Bandwidth</strong> box, enter the bandwidth, in bits per second.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Ct0</strong> box, enter the bandwidth, for the specified class.</td>
</tr>
<tr>
<td></td>
<td>8. In the <strong>Ct1</strong> box, enter the bandwidth, for the specified class.</td>
</tr>
<tr>
<td></td>
<td>9. In the <strong>Ct2</strong> box, enter the bandwidth, for the specified class.</td>
</tr>
<tr>
<td></td>
<td>10. In the <strong>Ct3</strong> box, enter the bandwidth, for the specified class.</td>
</tr>
</tbody>
</table>

Configuring BFD for MPLS IPv4 LSPs (NSM Procedure)
You can configure BFD for LSPs that use either LDP or RSVP as the signaling protocol using the Oam option.

To configure BFD for LSPs in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in Table 161 on page 303.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 161: Oam Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable OAM for RSVP-signaled LSPs.</td>
<td>1. Click <strong>Add new entry</strong> next to Label Switched Path.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Primary</strong> next to label-switched-path.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add new entry</strong> next to Primary.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Oam</strong> next to primary.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Lsp Ping Interval</strong> list, select the duration of the LSP ping interval in seconds.</td>
</tr>
</tbody>
</table>
### Table 161: Oam Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Enable Bidirectional Forwarding Detection (BFD) for all of the MPLS LSPs or for just a specific LSP. | 1. Click Bfd Liveness Detection next to Oam.  
2. In the Comment box, enter the comment.  
3. From the Version list, select the BFD version to be used for detection.  
4. From the Minimum Interval list, select the minimum transmit and receive interval.  
   Range: 1 through 255,000 milliseconds  
5. From the Minimum Receive Interval list, select the minimum receive interval.  
   Range: 1 through 255,000 milliseconds  
6. From the Multiplier list, select the detection time multiplier.  
   Range: 1 through 255  
   Default: 3  
7. Select the No Adaptation check box to disable BFD adaptation. |
| Specify the threshold for the adaptation of the detection time.     | 1. Click Detection Time next to Bfd Liveness Detection.  
2. In the Comment box, enter the comment.  
3. From the Threshold list, select the threshold for detecting the adaptation of the transmit interval. |
| Configure route and next-hop properties in the event of a BFD protocol session failure event on an RSVP label-switched path. | 1. Click Failure Action next to Bfd Liveness Detection.  
2. In the Comment box, enter the comment.  
3. Click Teardown next to Failure Action.  
4. Select one of the following:  
   - teardown—when a BFD session fails for an RSVP LSP, the associated LSP path is taken down and ressignaled immediately.  
   - make-before-break—when a BFD session fails for an RSVP LSP, an attempt is made to signal a new LSP path before tearing down the old LSP path.  
     a. In the Comment box, enter the comment.  
     b. From the Teardown Timeout list, select the time in seconds. |
| Specify the minimum transmit interval for failure detection.         | 1. Click Transmit Interval next to Failure Action.  
2. In the Comment box, enter the comment.  
3. From the Minimum Interval list, select the minimum interval at which the local router transmits hello packets to the neighbor with which it has established a BFD session.  
   Range: 1 through 255,000 milliseconds  
4. From the Threshold list, select the threshold for detecting the adaptation of the transmit interval.  
   Range: 0 through 4,294,967,295 milliseconds |
Table 161: Oam Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure MPLS tracing options.</td>
<td>1. Click <strong>Traceoptions</strong> next to Oam.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. Select the <strong>No Remote Trace</strong> check box to disable remote tracing globally or for a specific tracing operation.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>File</strong> next to Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Filename</strong> box, enter the name of the file to receive the output of the tracing operation.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Size</strong> box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).</td>
</tr>
<tr>
<td></td>
<td>7. From the <strong>Files</strong> list, select the maximum number of trace files. Range: 2 through 1000</td>
</tr>
<tr>
<td></td>
<td>8. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>world-readable</strong>—To enable unrestricted file access.</td>
</tr>
<tr>
<td></td>
<td>• <strong>no-world-readable</strong>—To restrict file access to owner.</td>
</tr>
<tr>
<td></td>
<td>9. In the <strong>Match</strong> box, enter the regular expression.</td>
</tr>
<tr>
<td></td>
<td>10. Click <strong>Flag</strong> next to Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>11. Click <strong>Add new entry</strong> next to Flag.</td>
</tr>
<tr>
<td></td>
<td>12. From the <strong>Name</strong> list, select the flag.</td>
</tr>
<tr>
<td></td>
<td>13. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
</tbody>
</table>

Configuring Secondary Paths for an LSP (NSM Procedure)

- Configuring Secondary Paths for an LSP (NSM Procedure) on page 305
- Configuring Administrative Group (NSM Procedure) on page 307
- Configuring Class-Type Bandwidth Constraints for Multiclass LSPs (NSM Procedure) on page 308
- Configuring BFD for MPLS IPv4 LSPs (NSM Procedure) on page 309
- Configuring the Egress Router Address for LSPs (NSM Procedure) on page 311
- Tracing LSP Packets and Operations (NSM Procedure) on page 312

**Configuring Secondary Paths for an LSP (NSM Procedure)**

You can specify one or more secondary paths to use for the LSP. You can configure more than one secondary path. All secondary paths are equal, and the first one that is available is chosen. You can specify secondary paths even if you have not specified any primary paths. Optionally, you can specify preference, CoS, and bandwidth values for the secondary path, which override any equivalent values that you configure for the LSP.

To configure secondary paths for an LSP in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in Table 162 on page 306.

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

Table 162: Secondary Paths Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the secondary paths for an LSP.</td>
<td>1. Click Add new entry next to Label Switched Path.</td>
</tr>
<tr>
<td></td>
<td>2. Click Secondary next to label-switched-path.</td>
</tr>
<tr>
<td></td>
<td>3. Click Add new entry next to Secondary.</td>
</tr>
<tr>
<td></td>
<td>4. In the Name box, enter the name of a path.</td>
</tr>
<tr>
<td></td>
<td>5. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. From the Class Of Service list, select the CoS value.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 7.</td>
</tr>
<tr>
<td></td>
<td>Default: If you do not specify a CoS value, the IP precedence bits from the packet’s IP header are used as the packet’s CoS value.</td>
</tr>
<tr>
<td></td>
<td>7. Select the No Decrement Ttl check box to disable normal time-to-live (TTL) decrementing.</td>
</tr>
<tr>
<td></td>
<td>8. From the Hop Limit list, select the maximum number of hops.</td>
</tr>
<tr>
<td></td>
<td>Range: 2 through 255 (for an LSP); 0 through 255 (for fast reroute)</td>
</tr>
<tr>
<td></td>
<td>Default: 255 (for an LSP); 6 (for fast reroute)</td>
</tr>
<tr>
<td></td>
<td>9. Select the No Cspf check box to disable constrained-path LSP computation.</td>
</tr>
</tbody>
</table>
10. Select the **Admin Down** check box to set the A-bit in the Admin Status object.

11. From the **Optimize Timer** list, select the length of the optimize timer, in seconds.
   - Range: 0 through 65,535 seconds
   - Default: 0 seconds (the optimize timer is disabled)

12. From the **Preference** list, select the preference to assign to the route.
   - Range: 0 to 4,294,967,295
   - Default: 5 for static MPLS LSPs, 7 for RSVP MPLS LSPs, 9 for LDP MPLS LSPs

13. From the **Setup Priority** list, select the setup priority.
   - Range: 0 through 7, where 0 is the highest and 7 is the lowest priority.

14. From the **Reservation Priority** list, select the reservation priority.
   - Range: 0 through 7, where 0 is the highest and 7 is the lowest priority.

15. Select one of the following:
   - **record**—Record routes
   - **no-record**—Does not record routes

16. Select the **Standby** check box to have the path remain up at all times to provide instant switchover if connectivity problems occur.

17. Select the **Adaptive** check box for RSVP to use shared explicit (SE) reservation styles and assists in smooth transition during rerouting.

18. From the **Select** list, select the conditions under which the path is selected to carry traffic. Select one the following:
   - **manual**—The path is selected for carrying traffic if it is up and stable for at least the revert timer window (potentially before the revert timer has elapsed). Traffic is sent to other working paths if the current path is down or degraded (receiving errors).
   - **unconditional**—The path is always selected for carrying traffic, even if it is currently down or degraded (receiving errors).

---

### Configuring Administrative Group (NSM Procedure)

You can configure an administrative group constraint for each LSP or for each primary or secondary LSP path using the Admin Group option.

To configure administrative group in NSM:

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

5. Add or modify settings as specified in Table 163 on page 308.

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

### Table 163: Administrative Group Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure administrative group.                                      | 1. Click **Add new entry** next to Label Switched Path.  
|                                                                      | 2. Click **Secondary** next to label-switched-path.  
|                                                                      | 3. Click **Add new entry** next to Secondary.  
|                                                                      | 4. Click **Admin Group** next to secondary.  
|                                                                      | 5. In the **Comment** box, enter the comment. |
| Define the administrative groups to exclude for an LSP or for a path's secondary paths. | 1. Click **Exclude** next to Admin Group.  
|                                                                      | 2. Click **Add new entry** next to Exclude.  
|                                                                      | 3. In the **New exclude** window, enter the names of one or more groups. |
| Require the LSP to traverse links that include all of the defined administrative groups. | 1. Click **Include All** next to Admin Group.  
|                                                                      | 2. Click **Add new entry** next to Include All.  
|                                                                      | 3. In the **New include-all** window, enter the names of one or more groups. |
| Define the administrative groups to include for an LSP or for a path's primary and secondary paths. | 1. Click **Include Any** next to Admin Group.  
|                                                                      | 2. Click **Add new entry** next to Include Any.  
|                                                                      | 3. In the **New include-any** window, enter the names of one or more groups. |

**Configuring Class-Type Bandwidth Constraints for Multiclass LSPs (NSM Procedure)**

You configure a multiclass LSP by using the Bandwidth option.

To configure bandwidth for the multiclass LSP in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in Table 164 on page 309.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
Table 164: Bandwidth Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure an LSP as a multiclass LSP.</td>
<td>1. Click <strong>Add new entry</strong> next to Label Switched Path.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Secondary</strong> next to label-switched-path.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add new entry</strong> next to Secondary.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Bandwidth</strong> next to secondary.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Per Traffic Class Bandwidth</strong> box, enter the bandwidth, in bits per second.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Ct0</strong> box, enter the bandwidth, for the specified class.</td>
</tr>
<tr>
<td></td>
<td>8. In the <strong>Ct1</strong> box, enter the bandwidth, for the specified class.</td>
</tr>
<tr>
<td></td>
<td>9. In the <strong>Ct2</strong> box, enter the bandwidth, for the specified class.</td>
</tr>
<tr>
<td></td>
<td>10. In the <strong>Ct3</strong> box, enter the bandwidth, for the specified class.</td>
</tr>
</tbody>
</table>

Configuring BFD for MPLS IPv4 LSPs (NSM Procedure)

You can configure BFD for LSPs that use either LDP or RSVP as the signaling protocol using the Oam option.

To configure BFD for LSPs in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in Table 165 on page 309.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 165: Oam Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable OAM for RSVP-signaled LSPs.</td>
<td>1. Click <strong>Add new entry</strong> next to Label Switched Path.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Secondary</strong> next to label-switched-path.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add new entry</strong> next to Secondary.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Oam</strong> next to secondary.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Lsp Ping Interval</strong> list, select the duration of the LSP ping interval in seconds.</td>
</tr>
</tbody>
</table>
### Table 165: Oam Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Enable Bidirectional          | 1. Click **Bfd Liveness Detection** next to Oam.  
| Forwarding Detection (BFD)    | 2. In the **Comment** box, enter the comment.  
| for all of the MPLS LSPs or   | 3. From the **Version** list, select the BFD version to be used for detection.  
| for just a specific LSP.      | 4. From the **Minimum Interval** list, select the minimum transmit and receive interval. Range: 1 through 255,000 milliseconds  
|                               | 5. From the **Minimum Receive Interval** list, select the minimum receive interval. Range: 1 through 255,000 milliseconds  
|                               | 6. From the **Multiplier** list, select the detection time multiplier. Range: 1 through 255 Default: 3  
|                               | 7. Select the **No Adaptation** check box to disable BFD adaptation.  
| Specify the threshold for     | 1. Click **Detection Time** next to Bfd Liveness Detection.  
| the adaptation of the         | 2. In the **Comment** box, enter the comment.  
| detection time.               | 3. From the **Threshold** list, select the threshold for detecting the adaptation of the transmit interval.  
| Configure route and next-hop  | 1. Click **Failure Action** next to Bfd Liveness Detection.  
| properties in the event of a  | 2. In the **Comment** box, enter the comment.  
| BFD protocol session failure  | 3. Click **Teardown** next to Failure Action.  
| event on an RSVP              | 4. Select one of the following:  
| label-switched path.          |   - **teardown**—when a BFD session fails for an RSVP LSP, the associated LSP path is taken down and signaled immediately.  
|                               |   - **make-before-break**—when a BFD session fails for an RSVP LSP, an attempt is made to signal a new LSP path before tearing down the old LSP path.  
| Specify the minimum transmit  | 1. Click **Transmit Interval** next to Failure Action.  
| interval for failure          | 2. In the **Comment** box, enter the comment.  
| detection.                    | 3. From the **Minimum Interval** list, select the minimum interval at which the local router transmits hello packets to the neighbor with which it has established a BFD session.  
|                               | 4. From the **Threshold** list, select the threshold for detecting the adaptation of the transmit interval. Range: 0 to 4,294,967,295  

**Note:** The values provided are for demonstration purposes only and may differ in actual implementations.
Configure LSP tracing options.

1. Click Traceoptions next to Oam.
2. In the Comment box, enter the comment.
3. Select the No Remote Trace check box to disable remote tracing globally or for a specific tracing operation.
4. Click File next to Traceoptions.
5. In the Filename box, enter the name of the file to receive the output of the tracing operation.
6. In the Size box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).
7. From the Files list, select the maximum number of trace files.
   Range: 2 through 1000
8. Select one of the following:
   - world-readable—To enable unrestricted file access.
   - no-world-readable—To restrict file access to owner.
9. In the Match box, enter the regular expression.
10. Click Flag next to Traceoptions.
11. Click Add new entry next to Flag
12. From the Name list, select the flag.
13. In the Comment box, enter the comment.

Configuring the Egress Router Address for LSPs (NSM Procedure)

When configuring an LSP, you must specify the address of the egress router by using the To option.

To configure the egress router of a dynamic LSP in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols > Mpls.
4. Select Label Switched Path.
5. Add or modify settings as specified in Table 166 on page 312.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
Table 166: Egress Router Address Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the address of the egress router.</td>
<td>1. Click <strong>Add new entry</strong> next to Label Switched Path.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>To</strong> next to label-switched-path.</td>
</tr>
<tr>
<td></td>
<td>3. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>To</strong>—Specify the egress router of a dynamic LSP and enter the address of the egress router.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Template</strong>—Configure an LSP template.</td>
</tr>
</tbody>
</table>

Tracing LSP Packets and Operations (NSM Procedure)

You can trace LSP packets and operations using the Traceoptions option.

To trace LSP packets and operations in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols > Mpls**.
4. Select **Label Switched Path**.
5. Add or modify settings as specified in Table 167 on page 312.
6. Click one:
   • OK—Saves the changes.
   • Cancel—Cancels the modifications.

Table 167: LSP Traceoptions Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trace LSP packets and operations.</td>
<td>1. Click <strong>Add new entry</strong> next to Label Switched Path.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Traceoptions</strong> next to label-switched-path.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>File</strong> next to Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Filename</strong> box, enter the name of the file to receive the output.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Size</strong> box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).</td>
</tr>
<tr>
<td></td>
<td>8. From the <strong>Files</strong> list, select the maximum number of trace files.</td>
</tr>
<tr>
<td></td>
<td>Range: 2 through 1000</td>
</tr>
<tr>
<td></td>
<td>9. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>world-readable</strong>—To enable unrestricted file access.</td>
</tr>
<tr>
<td></td>
<td>• <strong>no-world-readable</strong>—To restrict file access to owner.</td>
</tr>
</tbody>
</table>
Table 167: LSP Traceoptions Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the tracing operation to perform.</td>
<td>1. Click Flag next to Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>2. Click Add new entry next to Flag.</td>
</tr>
<tr>
<td></td>
<td>3. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. From the Name list, select the tracing operation to be performed.</td>
</tr>
<tr>
<td></td>
<td>5. In the Comment box, enter the comment.</td>
</tr>
</tbody>
</table>

Configuring System Log Messages and SNMP Traps for LSPs (NSM Procedure)

Whenever a label switched paths (LSPs) makes a transition from up to down, or down to up, and whenever an LSP switches from one active path to another, the ingress router generates a system log message and sends an SNMP trap.

To configure system log messages and SNMP traps for LSPs in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols.
4. Select Mpls.
5. Add or modify settings as specified in Table 168 on page 313.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

Table 168: Log Updown Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log a message or send an SNMP trap whenever an LSP makes a transition from up to down, or vice versa.</td>
<td>1. Click Log Updown next to Mpls.</td>
</tr>
<tr>
<td></td>
<td>2. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• syslog—To log a message to the system log file.</td>
</tr>
<tr>
<td></td>
<td>• no-syslog—Does not log a message to the system log file.</td>
</tr>
<tr>
<td></td>
<td>4. Select the Trap Path Down check box to generate SNMP traps whenever an LSP path goes down.</td>
</tr>
<tr>
<td></td>
<td>5. Select the Trap Path Up check box to generate SNMP traps whenever an LSP path goes up.</td>
</tr>
</tbody>
</table>
Table 168: Log Updown Configuration Details *(continued)*

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send an SNMP trap.</td>
<td>1. Click Trap next to Log Updown.</td>
</tr>
<tr>
<td></td>
<td>2. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>trap—To send an SNMP trap.</td>
</tr>
<tr>
<td></td>
<td>no–trap—Does not send an SNMP trap.</td>
</tr>
<tr>
<td></td>
<td>a. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>b. Select the Mpls Lsp Traps check box to block the MPLS LSP traps</td>
</tr>
<tr>
<td></td>
<td>defined in the jnx-mpls.mib but to allow the rfc3812.mib traps.</td>
</tr>
<tr>
<td></td>
<td>c. Select the Rfc3812 Traps check box to block the traps defined in the</td>
</tr>
<tr>
<td></td>
<td>rfc3812.mib but to allow the MPLS LSP traps defined in the jnx-mpls.mib</td>
</tr>
</tbody>
</table>

Configuring BFD for MPLS IPv4 LSPs (NSM Procedure)

You can configure BFD for label switched paths (LSPs) that use either LDP or RSVP as the signaling protocol using the Oam option.

To configure BFD for LSPs in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols.
4. Select Mpls.
5. Add or modify settings as specified in Table 169 on page 314.
6. Click one:
   * OK—Saves the changes.
   * Cancel— Cancels the modifications.

Table 169: Oam Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable OAM for RSVP-sigaled</td>
<td>1. Click Oam next to Mpls.</td>
</tr>
<tr>
<td>LSPs.</td>
<td>2. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. From the Lsp Ping Interval list, select the duration of the LSP</td>
</tr>
<tr>
<td></td>
<td>ping interval in seconds.</td>
</tr>
</tbody>
</table>
Table 169: Oam Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Enable Bidirectional Forwarding Detection (BFD) for all of the MPLS LSPs or just a specific LSP. | 1. Click Bfd Liveness Detection next to Oam.  
2. In the Comment box, enter the comment.  
3. From the Version list, select the BFD version to be used for detection.  
4. From the Minimum Interval list, select the minimum transmit and receive interval.  
   Range: 1 through 255,000 milliseconds  
5. From the Minimum Receive Interval list, select the minimum receive interval.  
   Range: 1 through 255,000 milliseconds  
6. From the Multiplier list, select the detection time multiplier.  
   Range: 1 through 255  
   Default: 3  
7. Select the No Adaptation check box to disable BFD adaptation. |
| Specify the threshold for the adaptation of the detection time. | 1. Click Detection Time next to Bfd Liveness Detection.  
2. In the Comment box, enter the comment.  
3. From the Threshold list, select the threshold for detecting the adaptation of the transmit interval. |
| Configure route and next-hop properties in the event of a BFD protocol session failure event on an RSVP label-switched path. | 1. Click Failure Action next to Bfd Liveness Detection.  
2. In the Comment box, enter the comment.  
3. Click Teardown next to Failure Action.  
4. Select one of the following:  
   • teardown—when a BFD session fails for an RSVP LSP, the associated LSP path is taken down and resignal immediately.  
   • make-before-break—when a BFD session fails for an RSVP LSP, an attempt is made to signal a new LSP path before tearing down the old LSP path.  
      a. In the Comment box, enter the comment.  
      b. From the Teardown Timeout list, select the time in seconds. |
| Specify the minimum transmit interval for failure detection. | 1. Click Transmit Interval next to Failure Action.  
2. In the Comment box, enter the comment.  
3. From the Minimum Interval list, select the minimum interval at which the local router transmits hello packets to the neighbor with which it has established a BFD session.  
   Range: 1 to 255,000 milliseconds  
4. From the Threshold list, select the threshold for detecting the adaptation of the transmit interval.  
   Range: 0 to 4,294,967,295 |
Table 169: Oam Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure MPLS tracing options.</td>
<td>1. Click <strong>Traceoptions</strong> next to Oam.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. Select the <strong>No Remote Trace</strong> check box to disable remote tracing globally or for a specific tracing operation.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>File</strong> next to Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Filename</strong> box, enter the name of the file to receive the output of the tracing operation.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Size</strong> box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).</td>
</tr>
<tr>
<td></td>
<td>7. From the <strong>Files</strong> list, select the maximum number of trace files.</td>
</tr>
<tr>
<td></td>
<td>Range: 2 through 1000</td>
</tr>
<tr>
<td></td>
<td>8. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>world-readable</strong>—To enable unrestricted file access.</td>
</tr>
<tr>
<td></td>
<td>• <strong>no-world-readable</strong>—To restrict file access to owner.</td>
</tr>
<tr>
<td></td>
<td>9. In the <strong>Match</strong> box, enter the regular expression.</td>
</tr>
<tr>
<td></td>
<td>10. Click <strong>Flag</strong> next to Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>11. Click <strong>Add new entry</strong> next to Flag.</td>
</tr>
<tr>
<td></td>
<td>12. From the <strong>Name</strong> list, select the flag.</td>
</tr>
<tr>
<td></td>
<td>13. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
</tbody>
</table>

Configuring Named Paths (NSM Procedure)

To configure signaled label switched paths (LSPs), you must first create one or more named paths on the ingress router. For each path, you can specify some or all transit routers in the path, or you can leave it empty. Each pathname can contain up to 32 characters and can include letters, digits, periods, and hyphens. The name must be unique within the ingress router.

To configure named paths in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Mpls**.
5. Add or modify settings as specified in Table 170 on page 317.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.
Table 170: Named Path Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Create a named path. | 1. Click **Path** next to Mpls.  
2. Click **Add new entry** next to Path.  
3. In the **Name** box, enter the hostname.  
4. In the **Comment** box, enter the comment. |

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify the sequence of explicit routers that form the path. | 1. Click **Path List** next to Path.  
2. In the **Name** box, enter the Name that identifies the sequence of nodes that form an LSP.  
3. In the **Comment** box, enter the comment.  
4. Select one of the following:  
   - **loose**—indicate that the next address in the path statement is a loose link. This means that the LSP can traverse through other routers before reaching this router.  
   - **strict**—indicate that the LSP must go to the next address specified in the path statement without traversing other nodes. |

### Configuring MTU Signaling in RSVPs (NSM Procedure)

To configure maximum transmission unit (MTU) signaling in RSVP, you need to configure MPLS to allow IP packets to be fragmented before they are encapsulated in MPLS. You also need to configure MTU signaling in RSVP. For troubleshooting purposes, you can configure MTU signaling alone without enabling packet fragmentation.

To configure MTU signaling in RSVP in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Mpls**.
5. Add or modify settings as specified in Table 171 on page 317.
6. Click one:  
   - **OK**—Saves the changes.  
   - **Cancel**—Cancels the modifications.

Table 171: Path MTU Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure MTU options for MPLS paths, including packet fragmentation and MTU signaling. | 1. Click **Path Mtu** next to Mpls.  
2. Select the **Enable Feature** check box to enable the option.  
3. In the **Comment** box, enter the comment.  
4. Select the **Allow Fragmentation** check box to allow IP packets to be fragmented before they are encapsulated in MPLS. |
Table 171: Path MTU Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure MTU signaling in RSVP. | 1. Click Rsvp next to Path Mtu.  
2. Select the Enable Feature check box to enable the option.  
3. In the Comment box, enter the comment.  
4. Select the Mtu Signaling check box to enable MTU signaling in RSVP. |

Configuring static LSPs on the Ingress Router (NSM Procedure)

You can configure static LSPs on the ingress router using the Static Path option.

To configure static path in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols.
4. Select Mpls.
5. Add or modify settings as specified in Table 172 on page 318.
6. Click one:  
   - OK—Saves the changes.  
   - Cancel—Cancels the modifications.

Table 172: Static Path Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure static path. | 1. Click Static Path next to Mpls.  
2. Click Add new entry next to Static Path.  
3. From the Name list, select the routing table.  
4. In the Comment box, enter the comment. |
| Configure static LSPs on the ingress router. | 1. Click Path next to static-path.  
2. Click Add new entry next to Path.  
3. In the Name box, enter the name of the routing table.  
4. In the Comment box, enter the comment.  
5. In the Next Hop box, enter the IP address of the next hop to the destination. |
Table 172: Static Path Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 6. | From the Push list, select the out-label value.  
Range: 0 through 1,048,575 |
| 7. | From the Double Push Bottom list, select the bottom-label value.  
Range: Labels 0 through 999,999 are for internal use. Labels 1,000,000 through 1,048,575 are unassigned by the JUNOS Software and are available for static LSPs. |
| 8. | From the Double Push Top list, select the top-label value.  
Range: Labels 0 through 999,999 are for internal use. Labels 1,000,000 through 1,048,575 are unassigned by the JUNOS Software and are available for static LSPs. |
| 9. | From the Triple Push Bottom list, select the bottom-label value.  
Range: 0 through 1,048,575. Labels 0 through 999,999 are for internal use. Labels 1,000,000 through 1,048,575 are unassigned by the JUNOS Software and are available for static LSPs. |
| 10. | From the Triple Push Middle list, select the middle-label value.  
Range: 0 through 1,048,575. Labels 0 through 999,999 are for internal use. Labels 1,000,000 through 1,048,575 are unassigned by the JUNOS Software and are available for static LSPs. |
| 11. | From the Triple Push Top list, select the top-label value.  
Range: 0 through 1,048,575. Labels 0 through 999,999 are for internal use. Labels 1,000,000 through 1,048,575 are unassigned by the JUNOS Software and are available for static LSPs. |
| 12. | From the Preference list, select the preference to be assigned to the route. |
| 13. | From the Class Of Service list, select the CoS value.  
Range: 0 through 7  
Default: If you do not specify a CoS value, the IP precedence bits from the packet’s IP header are used as the packet’s CoS value. |

Configuring MPLS Statistics (NSM Procedure)

You can enable MPLS statistics collection and reporting using the Statistics option.

To configure static path in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols.
4. Select Mpls.
5. Add or modify settings as specified in Table 173 on page 320.
6. Click one:
• OK—Saves the changes.
• Cancel—Cancels the modifications.

Table 173: MPLS Statistics Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable MPLS statistics collection and reporting.</td>
<td>1. Click <strong>Statistics</strong> next to Mpls.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. From the <strong>Interval</strong> list, select the interval at which to periodically collect statistics.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 65,535</td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
</tr>
<tr>
<td></td>
<td>4. Select the <strong>Auto Bandwidth</strong> check box to collect statistics related to automatic bandwidth.</td>
</tr>
<tr>
<td>Configure the file.</td>
<td>1. Click <strong>File</strong> next to Statistics.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Filename</strong> box, enter the name of the file to receive the output.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Size</strong> box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).</td>
</tr>
<tr>
<td></td>
<td>5. From the <strong>Files</strong> list, select the maximum number of trace files.</td>
</tr>
<tr>
<td></td>
<td>Range: 2 through 1000</td>
</tr>
<tr>
<td></td>
<td>6. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>world-readable</strong>—To enable unrestricted file access.</td>
</tr>
<tr>
<td></td>
<td>• <strong>no-world-readable</strong>—To restrict file access to owner.</td>
</tr>
</tbody>
</table>

Tracing MPLS Packets and Operations (NSM Procedure)

You can trace MPLS packets and operations using the Traceoptions option.

To trace MPLS packets and operations in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Mpls**.
5. Add or modify settings as specified in Table 174 on page 321.
6. Click one:
   • OK—Saves the changes.
   • Cancel—Cancels the modifications.
### Configuring MSDP Protocol (NSM Procedure)

The Multicast Source Discovery Protocol (MSDP) is used to connect multicast routing domains. It typically runs on the same router as the Protocol Independent Multicast (PIM) sparse-mode rendezvous point (RP). Each MSDP router establishes adjacencies with internal and external MSDP peers similar to the Border Gateway Protocol (BGP). These peer routers inform each other about active sources within the domain. When they detect active sources, the routers can send PIM sparse-mode explicit join messages to the active source. You can enable MSDP on the router using the MSDP option. See the following topics.

- Configuring MSDP on the Router (NSM Procedure) on page 321
- Configuring the MSDP Active Source Limit (NSM Procedure) on page 322
- Configuring Export Policy (NSM Procedure) on page 323
- Configuring MSDP Peer Group on page 324

### Configuring MSDP on the Router (NSM Procedure)

You can enable multicast source discovery protocol (MSDP) on the router using the MSDP option.

To enable MSDP on the router in NSM:

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

4. Select **MSDP**.

5. Add or modify settings as specified in Table 175 on page 322.

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

### Table 175: MSDP Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable MSDP on the router.</td>
<td>1. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>2. From the <strong>Data Encapsulation</strong> list, select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>disable</strong>—Do not use MSDP data encapsulation.</td>
</tr>
<tr>
<td></td>
<td>• <strong>enable</strong>—Use MSDP data encapsulation.</td>
</tr>
<tr>
<td></td>
<td>3. Select the <strong>Disable</strong> check box to disable MSDP.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Local Address</strong> box, enter the IP address of the local end of the connection.</td>
</tr>
</tbody>
</table>

### Configuring the MSDP Active Source Limit (NSM Procedure)

A router interested in MSDP messages, such as a rendezvous point (RP), might have to process a large number of MSDP messages, especially source-active messages, arriving from other routers. Because of the potential need for a router to examine, process, and create state tables for many MSDP packets, there is a possibility of an MSDP-based DoS attack on a router running MSDP. To minimize this possibility, you can configure the router to limit the number of source active messages the router accepts. Also, you can configure a threshold for applying random early discard (RED) to drop some but not all MSDP active source messages.

To configure the MSDP active source limit on the router in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Msdp**.
5. Add or modify settings as specified in Table 176 on page 323.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.
Table 176: Active Source Limit Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure active source limit | 1. Click **Active Source Limit** next to Msdp.  
                               | 2. In the **Comment** box, enter the comment.  
                               | 3. From the **Maximum** list, select the maximum number of active source messages.  
                               | Range: 1 through 1,000,000  
                               | Default: 25,000  
                               | 4. From the **Threshold** list, select the RED threshold for active source messages.  
                               | Range: 1 through 1,000,000  
                               | Default: 24,000 |

Configuring Export Policy (NSM Procedure)

To apply policies to source-active messages being exported from the source-active cache into MSDP, use the Export option.

To configure export policy in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Msdp**.
5. Add or modify settings as specified in Table 177 on page 323.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 177: Export Policy Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Apply one or more policies to | 1. Click **Export Policy** next to Msdp.  
                               | routes being exported from the routing table into MSDP.  
                               | 2. Use the following options to select the policies to export.  
                               | • Click **Add** after selecting a policy member from the Non member list to add it to the Members list.  
                               | • Click **Remove** after selecting a policy from the Members list to remove it from the Members list.  
                               | • Click **Add All** to add all the Non members to the Members list.  
                               | • Click **Remove All** to remove all the members from the Members list. |
Configuring MSDP Peer Group

- Configuring MSDP Peer Group (NSM Procedure) on page 324
- Configuring MSDP Peers (NSM Procedure) on page 325
- Configuring a Routing Table Group with MSDP (NSM Procedure) on page 327
- Configuring Per-Source Active Source Limit (NSM Procedure) on page 328
- Configuring MSDP Traceoptions (NSM Procedure) on page 328

**Configuring MSDP Peer Group (NSM Procedure)**

You can define an MSDP peer group using the Group option.

To configure an MSDP peer group in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Msdp**.
5. Add or modify settings as specified in Table 178 on page 324.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

**Table 178: Peer Group Configuration Details**

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define an MSDP peer group.</td>
<td>1. Click <strong>Group</strong> next to Msdp.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Group.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the name of the MSDP group.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. From the <strong>Mode</strong> list, select the mesh groups.</td>
</tr>
<tr>
<td></td>
<td>6. Select the <strong>Disable</strong> check box to disable MSDP.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Local Address</strong> box, enter the IP address of the local end of the connection.</td>
</tr>
</tbody>
</table>

Apply one or more policies to routes being exported from the routing table into MSDP.

1. Click **Export** next to Group.
2. Use the following options to select the policies to export:
   - Click **Add** after selecting a policy member from the Non member list to add it to the Members list.
   - Click **Remove** after selecting a policy from the Members list to remove it from the Members list.
   - Click **Add All** to add all the Non members to the Members list.
   - Click **Remove All** to remove all the members from the Members list.
Table 178: Peer Group Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply one or more policies to routes being imported into the routing table from MSDP.</td>
<td>1. Click Import next to Group.</td>
</tr>
<tr>
<td></td>
<td>2. Use the following options to select the policies to import:</td>
</tr>
<tr>
<td></td>
<td>• Click Add after selecting a policy member from the Non member list to add it to the Members list.</td>
</tr>
<tr>
<td></td>
<td>• Click Remove after selecting a policy from the Members list to remove it from the Members list.</td>
</tr>
<tr>
<td></td>
<td>• Click Add All to add all the Non members to the Members list.</td>
</tr>
<tr>
<td></td>
<td>• Click Remove All to remove all the members from the Members list.</td>
</tr>
</tbody>
</table>

Configuring MSDP Peers (NSM Procedure)

An MSDP router must know which routers are its peers. You define the peer relationships explicitly by configuring the neighboring routers that are the MSDP peers of the local router. After peer relationships are established, the MSDP peers exchange messages to advertise active multicast sources. You must configure at least one peer for MSDP to function.

To configure MSDP peers in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols.
4. Select Msdp.
5. Add or modify settings as specified in Table 179 on page 326.
6. Click one:
   • OK—Saves the changes.
   • Cancel— Cancels the modifications.
Table 179: MSDP Peer Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure MSDP peers.</td>
<td>1. Click <strong>Group</strong> next to Msdp.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Group.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Peer</strong> next to group.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Add new entry</strong> next to Peer.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Name</strong> box, enter the name of the MSDP group.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>7. From the <strong>Mode</strong> list, select the mesh groups.</td>
</tr>
<tr>
<td></td>
<td>8. Select the <strong>Disable</strong> check box to disable MSDP.</td>
</tr>
<tr>
<td></td>
<td>9. In the <strong>Local Address</strong> box, enter the IP address of the local end of the connection.</td>
</tr>
<tr>
<td></td>
<td>10. Select the <strong>Default Peer</strong> check box to establish this peer as the default MSDP peer and accept source-active messages from the peer without the usual peer-reverse-path-forwarding (peer-RPF) check.</td>
</tr>
<tr>
<td></td>
<td>11. In the <strong>Authentication Key</strong> box, enter the MD5 authentication key.</td>
</tr>
<tr>
<td>Configure active source limit.</td>
<td>1. Click <strong>Active Source Limit</strong> next to Peer.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. From the <strong>Maximum</strong> list, select the maximum number of active source messages.</td>
</tr>
<tr>
<td></td>
<td><strong>Range</strong>: 1 through 1,000,000</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 25,000</td>
</tr>
<tr>
<td></td>
<td>4. From the <strong>Threshold</strong> list, select the RED threshold for active source messages.</td>
</tr>
<tr>
<td></td>
<td><strong>Range</strong>: 1 through 1,000,000</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 24,000</td>
</tr>
<tr>
<td>Apply one or more policies to routes being exported from the routing table into MSDP.</td>
<td>1. Click <strong>Export</strong> next to Peer.</td>
</tr>
<tr>
<td></td>
<td>2. Use the following options to select the policies to export:</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Add</strong> after selecting a policy member from the Non member list to add it to the Members list.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Remove</strong> after selecting a policy from the Members list to remove it from the Members list.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Add All</strong> to add all the Non members to the Members list.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Remove All</strong> to remove all the members from the Members list.</td>
</tr>
<tr>
<td>Apply one or more policies to routes being imported into the routing table from MSDP.</td>
<td>1. Click <strong>Import</strong> next to Peer.</td>
</tr>
<tr>
<td></td>
<td>2. Use the following options to select the policies to import:</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Add</strong> after selecting a policy member from the Non member list to add it to the Members list.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Remove</strong> after selecting a policy from the Members list to remove it from the Members list.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Add All</strong> to add all the Non members to the Members list.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Remove All</strong> to remove all the members from the Members list.</td>
</tr>
</tbody>
</table>
### Configuring a Routing Table Group with MSDP (NSM Procedure)

To associate with MSDP a routing table group that imports and exports routes into the specified routing table group, you can use the Rib Group option.

To associate a routing table group with MSDP in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Msdp**.
5. Add or modify settings as specified in Table 180 on page 327.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

### Table 180: Rib Group Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Associate a routing table group with MSDP. | 1. Click **Rib Group** next to Msdp.  
2. In the **Comment** box, enter the comment.  
3. In the **Ribgroup Name** box, enter the name of the routing table group. |
Configuring Per-Source Active Source Limit (NSM Procedure)

You can configure an active source limit for an address range as well as for a specific peer. A per-source active source limit uses an IP prefix and prefix length instead of a specific address. You can configure more than one per-source active source limit. The longest match determines the limit.

To configure an active source limit for an address range as well as for a specific peer in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols.
4. Select Msdp.
5. Add or modify settings as specified in Table 181 on page 328.
6. Click one:
   • OK—Saves the changes.
   • Cancel—Cancels the modifications.

Table 181: Active Source Limit Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure an active source limit for an address range</td>
<td>1. Click Source next to Msdp.</td>
</tr>
<tr>
<td>as well as for a specific peer.</td>
<td>2. Click Add new entry next to Source.</td>
</tr>
<tr>
<td></td>
<td>3. In the Name box, enter the IP address.</td>
</tr>
<tr>
<td></td>
<td>4. In the Comment box, enter the comment.</td>
</tr>
</tbody>
</table>

Configure active source limit. 1. Click Active Source Limit next to source. 2. In the Comment box, enter the comment. 3. From the Maximum list, select the maximum number of active source messages. Range: 1 through 1,000,000 Default: 25,000 4. From the Threshold list, select the RED threshold for active source messages. Range: 1 through 1,000,000 Default: 24,000

Configuring MSDP Traceoptions (NSM Procedure)

You can configure the MSDP traceoption using the Traceoption option.

To configure traceoptions in NSM:

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

5. Add or modify settings as specified in Table 182 on page 329.

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

Table 182: MSDP Traceoption Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure traceoptions.</td>
<td>1. Click Traceoptions next to Msdp.</td>
</tr>
<tr>
<td></td>
<td>2. In the Comment box, enter the comment for the traceoptions.</td>
</tr>
<tr>
<td></td>
<td>3. Click File next to Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>4. In the Comment box, enter the comment for the filename.</td>
</tr>
<tr>
<td></td>
<td>5. In the Filename box, enter the name of the file to receive the output of</td>
</tr>
<tr>
<td></td>
<td>the tracing operation.</td>
</tr>
<tr>
<td></td>
<td>6. In the Size box, enter the maximum trace file size.</td>
</tr>
<tr>
<td></td>
<td>7. From the Files list, select the maximum number of trace files.</td>
</tr>
<tr>
<td></td>
<td>8. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• no-world-readable—To restrict the file access to owner.</td>
</tr>
<tr>
<td></td>
<td>• world-readable—To enable unrestricted access.</td>
</tr>
<tr>
<td></td>
<td>9. Click Flag next to Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>10. Click Add new entry next to Flag.</td>
</tr>
<tr>
<td></td>
<td>11. From the Name list, select the flag to perform the trace operation.</td>
</tr>
<tr>
<td></td>
<td>12. In the Comment box, enter the comment for the flag.</td>
</tr>
<tr>
<td></td>
<td>13. Select the corresponding modifier for the tracing flag.</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 183 on page 330.
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 183: 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 BPDU is discarded.</td>
<td>Select a value.</td>
</tr>
<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>

Copyright © 2010, Juniper Networks, Inc.
Table 183: MSTP Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Specifies MSTP settings for the interface.</td>
<td>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 Bpdudtimeoutaction:</td>
</tr>
<tr>
<td>Msti</td>
<td>Specifies MST instances settings for an interface or VLAN.</td>
<td>1. Specify the Msti ID. 2. Enter a comment. 3. Specify the bridge priority. 4. Click OK.</td>
</tr>
</tbody>
</table>

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 184 on page 332.
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 184: 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 184: 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>
</tbody>
</table>
| Disable           | Specifies whether to disable the OSPF configuration.                     | 1. Specify whether to enable or disable OSPF.  
|                   | • To enable OSPF, clear the check box.                                   |             |
|                   | • To disable OSPF, select the check box.                                  |             |
| Prefix Export Limit| Configure a limit to the number of prefixes to be exported.             | 1. Enter the prefix export limit or select from the list. |
| Rib Group         | Specifies the routing table group.                                       | 1. Select rib group from the list. |
| Route Type Community| Specifies an extended community value to encode the OSPF route type      | 1. Select route type community from the list. |
| Domain VPN Tag    | Virtual private network (VPN) tag for OSPFv2 external routes generated by the provider edge (PE) router. | 1. Enter the domain VPN tag or select from the list. |
| Preference        | Specifies the route preference for OSPF internal routes.                 | 1. Enter the preference or select from the list. |
| External Preference| Specifies the external route preference.                                 | 1. Enter the external route preference or select from the list. |
| Reference Bandwidth| Specifies the reference bandwidth used in calculating the default interface cost. | 1. Enter the reference bandwidth. |
| No RFC 1583       | Disable compatibility with RFC 1583. Disabling compatibility with RFC 1583 can prevent routing loops. | 1. Specify whether to configure RFC 1583.  
|                   | • To enable compatibility with RFC 1583, clear the check box.            |             |
|                   | • To disable compatibility with RFC 1583, select the check box.          |             |
| No NSSA ABR       | Disable compatibility with NSSA ABR.                                     | 1. Specify whether NSSA ABR has to be configured.  
|                   | • To enable NSSA ABR, clear the check box.                               |             |
|                   | • To disable NSSA ABR, select the check the check box.                   |             |
| Area              | Enables you to set up the area details for OSPF.                        |             |
## Table 184: OSPF Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1. Expand the <strong>OSPF</strong> tree and select <strong>Area</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Set up the area range, interface, sham link remote, stub and virtual link.</td>
</tr>
<tr>
<td>Domain ID</td>
<td>Enables you to configure domain ID for the <strong>OSPF</strong>.</td>
<td>1. Expand the <strong>OSPF</strong> tree and select <strong>Domain ID</strong>.</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 <strong>OSPF</strong> tree and select <strong>Export</strong>.</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 <strong>OSPF</strong>.</td>
<td>1. Expand the <strong>OSPF</strong> tree and select <strong>Graceful Restart</strong>.</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 <strong>OSPF</strong> tree and select <strong>Import</strong>.</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 <strong>OSPF</strong> tree and select <strong>Overload</strong>.</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 <strong>OSPF</strong> tree and select <strong>Sham Link</strong>.</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 <strong>OSPF</strong> tree and select <strong>SPF Options</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Specify the comment, delay, holddown and rapid runs.</td>
</tr>
</tbody>
</table>
Table 184: 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 185 on page 336.
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 185: RIP Configuration Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RIP</strong></td>
<td></td>
<td></td>
</tr>
<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></td>
<td></td>
<td>2. Enable the feature and set up the graceful restart parameters.</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></td>
<td></td>
<td>2. Click the New button or select a group and click Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Set up the Bfd Liveness Detection, Export, Import and Neighbor for RIP.</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></td>
<td></td>
<td>2. Specify the import policies.</td>
</tr>
</tbody>
</table>
Table 185: RIP Configuration Fields (continued)

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

Configuring RIPng Protocol (NSM Procedure)

To have a router exchange routes with other routers, you must configure RIP next generation (RIPng) groups and neighbors. RIPng routes received from routers not configured as RIPng neighbors are ignored. Likewise, RIPng routes are advertised only to routers configured as RIPng neighbors. See the following topics:

- Configuring RIPng on the Router (NSM Procedure) on page 337
- Configuring Graceful Restart for RIPng (NSM Procedure) on page 338
- Configuring Group on page 339
- Enable or Disable Receiving of Update Messages (NSM Procedure) on page 345
- Configuring RIPng Send Update Messages (NSM Procedure) on page 345
- Configuring RIPng Traceoptions (NSM Procedure) on page 346

Configuring RIPng on the Router (NSM Procedure)

To configure RIPng in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols.
4. Select Ripng.
5. Add or modify settings as specified in Table 186 on page 338.
6. Click one:

Copyright © 2010, Juniper Networks, Inc.
• OK—Saves the changes.
• Cancel— Cancels the modifications.

Table 186: RIPng Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure RIPng | 1. In the **Comment** box, enter the comment.  
2. From the **Metric In** list, select the metric value.  
   Range: 1 through 15  
   Default: 1  
3. From the **Holddown** list, select the estimated time to wait before making updates to the routing table.  
   Range: 10 through 180 seconds  
   Default: 180 seconds  
4. From the **Route Timeout** list, select the estimated time to wait before making updates to the routing table.  
   Range: 30 through 360 seconds  
   Default: 180 seconds  
5. From the **Update Interval** list, select the estimated time to wait before making updates to the routing table.  
   Range: 10 through 60 seconds  
   Default: 30 seconds |

**Configuring Graceful Restart for RIPng (NSM Procedure)**

You can configure graceful restart parameters specifically for RIPng using the Graceful Restart option.

To configure graceful restart for RIPng in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Ripng**.
5. Add or modify settings as specified in Table 187 on page 339.
6. Click one:  
   • OK—Saves the changes.  
   • Cancel— Cancels the modifications.
Table 187: Graceful Restart Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure graceful restart.</td>
<td>1. Click Graceful Restart next to Ripng.</td>
</tr>
<tr>
<td></td>
<td>2. Select the Enable Feature check box to enable this option.</td>
</tr>
<tr>
<td></td>
<td>3. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. Select the Disable check box to disable the graceful restart.</td>
</tr>
<tr>
<td></td>
<td>5. From the Restart Time list, select the estimated time period for the restart to finish.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 600 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 60 seconds</td>
</tr>
</tbody>
</table>

Configuring Group

- Configuring Group-Specific RIPng Properties (NSM Procedure) on page 339
- Applying Policies to Routes Exported by RIPng (NSM Procedure) on page 341
- Applying Policies to Routes Imported by RIPng (NSM Procedure) on page 341
- Configuring RIPng Neighbor Properties on page 342

Configuring Group-Specific RIPng Properties (NSM Procedure)

You can group together neighbors that share the same export policy and export metric defaults. You configure group-specific RIPng properties by using the Group option.

To configure group specific properties for RIPng in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols.
4. Select Ripng.
5. Add or modify settings as specified in Table 188 on page 340.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.
### Table 188: Group Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configuring group specific properties. | 1. Click **Group** next to Ripng.  
2. Click **Add new entry** next to Group.  
3. In the **Name** box, enter the name of the group.  
4. In the **Comment** box, enter the comment.  
5. From the **Route Timeout** list, select the estimated time to wait before making updates to the routing table.  
   Range: 30 through 360 seconds  
   Default: 180 seconds  
6. From the **Update Interval** list, select the estimated time to wait before making updates to the routing table.  
   Range: 10 through 60 seconds  
   Default: 30 seconds  
7. From the **Preference** list, select the preference value. A lower value indicates a more preferred route.  
   Range: 0 through 4,294,967,295 ($2^{32} - 1$)  
   Default: 100  
8. From the **Metric Out** list, select the metric value.  
   Range: 1 through 15  
   Default: 1 |

| Apply a policy or list of policies to routes being exported to the neighbors. | 1. Click **Export** next to Group.  
2. Use the following options to select the policies to export:  
   • Click **Add** after selecting a policy member from the Non member list to add it to the Members list.  
   • Click **Remove** after selecting a policy from the Members list to remove it from the Members list.  
   • Click **Add All** to add all the Non members to the Members list.  
   • Click **Remove All** to remove all the members from the Members list. |

| Apply one or more policies to routes being imported into the local routing device from the neighbors. | 1. Click **Import** next to Group.  
2. Use the following options to select the policies to import:  
   • Click **Add** after selecting a policy member from the Non member list to add it to the Members list.  
   • Click **Remove** after selecting a policy from the Members list to remove it from the Members list.  
   • Click **Add All** to add all the Non members to the Members list.  
   • Click **Remove All** to remove all the members from the Members list. |
Applying Policies to Routes Exported by RIPng (NSM Procedure)

By default, RIPng does not export routes it has learned to its neighbors. To have RIPng export routes, apply one or more export policies. To apply export policies and to filter routes being exported from the local routing device to its neighbors use the Export option.

To apply for export policies for RIPng in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols.
4. Select Ripng.
5. Add or modify settings as specified in Table 189 on page 341.
6. Click one:
   - OK — Saves the changes.
   - Cancel — Cancels the modifications.

Table 189: RIPng Export Policy Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Apply a policy or list of policies to routes being exported to the neighbors. | 1. Click Export next to Group.  
2. Use the following options to select the policies to export:  
   - Click Add after selecting a policy member from the Non member list to add it to the Members list.  
   - Click Remove after selecting a policy from the Members list to remove it from the Members list.  
   - Click Add All to add all the Non members to the Members list.  
   - Click Remove All to remove all the members from the Members list. |

Applying Policies to Routes Imported by RIPng (NSM Procedure)

To filter routes being imported by the local routing device from its neighbors, use the Import option and list the names of one or more policies to be evaluated. If you specify more than one policy, they are evaluated in order (first to last) and the first matching policy is applied to the route. If no match is found, the local routing device does not import any routes.

To apply export policies for RIPng in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols.
4. Select Ripng.
5. Add or modify settings as specified in Table 190 on page 342.

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

Table 190: Import Policy Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Apply one or more policies to routes being imported into the local routing device from the neighbors. | 1. Click Import next to Group.  
2. Use the following options to select the policies to import:  
   - Click Add after selecting a policy member from the Non member list to add it to the Members list.  
   - Click Remove after selecting a policy from the Members list to remove it from the Members list.  
   - Click Add All to add all the Non members to the Members list.  
   - Click Remove All to remove all the members from the Members list. |

Configuring RIPng Neighbor Properties

- Configuring RIPng Neighbor Properties (NSM Procedure) on page 342
- Applying Policies to RIPng Routes Imported from Neighbors (NSM Procedure) on page 343
- Configuring RIPng Update Messages (NSM Procedure) on page 344
- Enable or Disable Sending of Update Messages (NSM Procedure) on page 344

**Configuring RIPng Neighbor Properties (NSM Procedure)**

To define neighbor-specific properties use the Neighbor option.

To configure neighbor specific parameters for RIPng in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Ripng**.
5. Add or modify settings as specified in Table 191 on page 343.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.
Table 191: Neighbor Properties Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define neighbor-specific properties.</td>
<td>1. Click Neighbor next to Group.</td>
</tr>
<tr>
<td></td>
<td>2. In the Name box, enter the name of an interface over which a routing</td>
</tr>
<tr>
<td></td>
<td>device communicates to its neighbors.</td>
</tr>
<tr>
<td></td>
<td>3. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. From the Route Timeout list, select the estimated time to wait before</td>
</tr>
<tr>
<td></td>
<td>making updates to the routing table.</td>
</tr>
<tr>
<td></td>
<td>5. From the Update Interval list, select the estimated time to wait before</td>
</tr>
<tr>
<td></td>
<td>making updates to the routing table.</td>
</tr>
<tr>
<td></td>
<td>6. From the Metric In list, select the metric value.</td>
</tr>
</tbody>
</table>

Applying Policies to RIPng Routes Imported from Neighbors (NSM Procedure)

To filter routes being imported by the local routing device from its neighbors, use the Import option and list the names of one or more policies to be evaluated. If you specify more than one policy, they are evaluated in order (first to last) and the first matching policy is applied to the route. If no match is found, the local routing device does not import any routes.

To configure neighbor specific parameters for RIPng in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols.
4. Select Ripng.
5. Add or modify settings as specified in Table 192 on page 343.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 192: Import Policy Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply one or more policies to routes</td>
<td>1. Click Import Policy next to Neighbor.</td>
</tr>
<tr>
<td>being imported into the local routing</td>
<td>2. Use the following options to select the policies to import:</td>
</tr>
<tr>
<td>device from the neighbors.</td>
<td>• Click Add after selecting a policy member from the Non member list to</td>
</tr>
<tr>
<td></td>
<td>add it to the Members list.</td>
</tr>
<tr>
<td></td>
<td>• Click Remove after selecting a policy from the Members list to remove</td>
</tr>
<tr>
<td></td>
<td>it from the Members list.</td>
</tr>
<tr>
<td></td>
<td>• Click Add All to add all the Non members to the Members list.</td>
</tr>
<tr>
<td></td>
<td>• Click Remove All to remove all the members from the Members list.</td>
</tr>
</tbody>
</table>
Configuring RIPng Update Messages (NSM Procedure)
You can enable and disable the receiving of update messages. By default, receiving update messages is enabled.

To enable or disable the receiving update messages in NSM:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols.
4. Select Ripng.
5. Add or modify settings as specified in Table 193 on page 344.
6. Click one:
   • OK—Saves the changes.
   • Cancel—Cancels the modifications.

Table 193: Receive Message Update Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable or disable the receiving update messages.</td>
<td>1. Click Receive next to Neighbor.</td>
</tr>
<tr>
<td></td>
<td>2. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. Select the None check box to disable receiving update messages.</td>
</tr>
</tbody>
</table>

Enable or Disable Sending of Update Messages (NSM Procedure)
You can enable and disable the sending of update messages. By default, sending update messages is enabled.

To enable or disable the sending update messages in NSM:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Protocols.
4. Select Ripng.
5. Add or modify settings as specified in Table 194 on page 345.
6. Click one:
   • OK—Saves the changes.
   • Cancel—Cancels the modifications.
Table 194: Send Update Message Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable or disable the sending update messages.</td>
<td>1. Click <strong>Send</strong> next to Neighbor.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. Select the <strong>None</strong> check box to disable sending update messages.</td>
</tr>
</tbody>
</table>

Enable or Disable Receiving of Update Messages (NSM Procedure)

You can enable and disable the receiving of update messages. By default, receiving update messages is enabled.

To enable or disable the receiving update messages in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Ripng**.
5. Add or modify settings as specified in Table 195 on page 345.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

Table 195: Receive Message Update Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable or disable the receiving update messages.</td>
<td>1. Click <strong>Receive</strong> next to Ripng.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. Select the <strong>None</strong> check box to disable receiving update messages.</td>
</tr>
</tbody>
</table>

Configuring RIPng Send Update Messages (NSM Procedure)

You can enable and disable the sending of update messages. By default, sending update messages is enabled.

To enable or disable the sending update messages in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Ripng**.
5. Add or modify settings as specified in Table 196 on page 346.
6. Click one:
- OK—Saves the changes.
- Cancel— Cancels the modifications.

### Table 196: RIPng Send Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable or disable the sending update messages.</td>
<td>1. Click <strong>Send</strong> next to Ripng.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. Select the <strong>None</strong> check box to disable sending update messages.</td>
</tr>
</tbody>
</table>

#### Configuring RIPng Traceoptions (NSM Procedure)

You can configure the RIPng traceoption using the Traceoption option.

To configure traceoptions in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Ripng**.
5. Add or modify settings as specified in Table 197 on page 347.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
Table 197: RIPng Traceoption Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure traceoptions.</td>
<td>1. Click <strong>Traceoptions</strong> next to Ripng.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment for the traceoptions.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>File</strong> next to Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment for the filename.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Filename</strong> box, enter the name of the file to receive the</td>
</tr>
<tr>
<td></td>
<td>output of the tracing operation.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Size</strong> box, enter the maximum trace file size.</td>
</tr>
<tr>
<td></td>
<td>7. From the <strong>Files</strong> list, select the maximum number of trace files.</td>
</tr>
<tr>
<td></td>
<td>8. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>none</strong>—To skip the option.</td>
</tr>
<tr>
<td></td>
<td>• <strong>no-world-readable</strong>—To restrict the file access to owner.</td>
</tr>
<tr>
<td></td>
<td>• <strong>world-readable</strong>—To enable unrestricted access.</td>
</tr>
<tr>
<td></td>
<td>9. Click <strong>Flag</strong> next to Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>10. Click <strong>Add new entry</strong> next to Flag.</td>
</tr>
<tr>
<td></td>
<td>11. From the <strong>Name</strong> list, select the flag to perform the trace operation.</td>
</tr>
<tr>
<td></td>
<td>12. In the <strong>Comment</strong> box, enter the comment for the flag.</td>
</tr>
<tr>
<td></td>
<td>13. Select the corresponding modifier for the tracing flag.</td>
</tr>
</tbody>
</table>

Configuring Router Advertisement (NSM Procedure)

You can configure neighbor discovery router advertisement using the Router Advertisement option.

To configure router advertisement in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Router Advertisement**.
5. Add or modify settings as specified in Table 198 on page 348.
6. Click one:
   • **OK**—Saves the changes.
   • **Cancel**—Cancels the modifications.
Configure router advertisement properties on an interface.

Table 198: Router Advertisement Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Click <strong>Interface</strong> next to Router Advertisement.</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Add new entry</strong> next to Interface.</td>
</tr>
<tr>
<td>3.</td>
<td>In the <strong>Name</strong> box, enter the name of an interface.</td>
</tr>
<tr>
<td>4.</td>
<td>In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
</tbody>
</table>
| 5.   | From the **Max Advertisement Interval** list, select the maximum interval between each router advertisement message.  
Range: 4 through 1800 seconds  
Default: 600 seconds |
| 6.   | From the **Min Advertisement Interval** list, select the minimum interval between each router advertisement message.  
Range: 3 seconds through three-quarter times the maximum advertisement interval value  
Default: One-third the maximum advertisement interval value |
| 7.   | Select one of the following:  
• **None**—To skip the option.  
• **managed-configuration**—Enable host to use stateful autoconfiguration.  
• **no-managed-configuration**—Disable host from using stateful autoconfiguration. |
| 8.   | Select one of the following:  
• **None**—To skip the option.  
• **other-stateful-configuration**—Enable autoconfiguration of other nonaddress-related information.  
• **no-other-stateful-configuration**—Disable autoconfiguration of other nonaddress-related information. |
| 9.   | From the **Reachable Time** list, select the length of time that a node considers a neighbor reachable until another reachability confirmation is received from that neighbor.  
Range: 0 through 3,600,000 milliseconds  
Default: 0 milliseconds |
| 10.  | From the **Retransmit Timer** list, select the retransmission frequency of neighbor solicitation messages.  
Range: 0 through 4,294,967,295 milliseconds  
Default: 0 milliseconds |
| 11.  | Select the **Virtual Router Only** check box to specify a virtual router. |
| 12.  | From the **Current Hop Limit** list, select the hop limit.  
Range: 0 through 255  
Default: 6 |
| 13.  | From the **Default Lifetime** list, select the default lifetime.  
Range: Maximum advertisement interval value through 9000 seconds  
Default: Three times the maximum advertisement interval value |
### Table 198: Router Advertisement Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure prefix properties in router advertisement messages.</strong></td>
<td>1. Click <strong>Prefix</strong> next to interface.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Name</strong> box, enter the prefix name.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. From the <strong>Valid Lifetime</strong> list, select the valid lifetime.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 4,294,967,295 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 2,592,000 seconds</td>
</tr>
<tr>
<td></td>
<td>5. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong>—To skip the option.</td>
</tr>
<tr>
<td></td>
<td>• <strong>on-link</strong>—Enable prefixes to be used for onlink determination.</td>
</tr>
<tr>
<td></td>
<td>• <strong>no-on-link</strong>—Disable prefixes from being used for onlink determination.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Preferred Lifetime</strong> list, select how long the prefix</td>
</tr>
<tr>
<td></td>
<td>generated by stateless autoconfiguration remains preferred.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 4,294,967,295</td>
</tr>
<tr>
<td></td>
<td>Default: 604,800 seconds</td>
</tr>
<tr>
<td></td>
<td>7. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong>—To skip the option.</td>
</tr>
<tr>
<td></td>
<td>• <strong>autonomous</strong>—Use prefixes for address autoconfiguration.</td>
</tr>
<tr>
<td></td>
<td>• <strong>no-autonomous</strong>—Do not use prefixes for address autoconfiguration.</td>
</tr>
<tr>
<td><strong>Specify router advertisement protocol-level tracing options.</strong></td>
<td>1. Click <strong>Traceoptions</strong> next to Router Advertisement.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment for the traceoptions.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>File</strong> next to Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment for the filename.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Filename</strong> box, enter the name of the file to receive the</td>
</tr>
<tr>
<td></td>
<td>output of the tracing operation.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Size</strong> box, enter the maximum trace file size.</td>
</tr>
<tr>
<td></td>
<td>7. From the <strong>Files</strong> list, select the maximum number of trace files.</td>
</tr>
<tr>
<td></td>
<td>8. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong>—To skip the option.</td>
</tr>
<tr>
<td></td>
<td>• <strong>no-world-readable</strong>—To restrict the file access to owner.</td>
</tr>
<tr>
<td></td>
<td>• <strong>world-readable</strong>—To enable unrestricted access.</td>
</tr>
<tr>
<td></td>
<td>9. Click <strong>Flag</strong> next to Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>10. Click <strong>Add new entry</strong> next to Flag.</td>
</tr>
<tr>
<td></td>
<td>11. From the <strong>Name</strong> list, select the flag to perform the trace operation.</td>
</tr>
<tr>
<td></td>
<td>12. In the <strong>Comment</strong> box, enter the comment for the flag.</td>
</tr>
</tbody>
</table>
Configuring ICMP Router Discovery (NSM Procedure)

To configure a router as a server for Internet Control Message Protocol (ICMP) router discovery, use the Router Discovery option.

To configure router discovery in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Protocols**.
4. Select **Router Discovery**.
5. Add or modify settings as specified in Table 199 on page 350.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 199: Router Discovery Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure router discovery. | 1. Click **Router Discovery** next to Protocols.  
2. In the **Comment** box, enter the comment.  
3. Select the **Disable** check box to disable router discovery. |
| Configure IP addresses to include in router advertisement packets. | 1. Click **Address** next to Router Discovery.  
2. In the **Name** box, enter the IP address.  
3. In the **Comment** box, enter the comment.  
4. Select the **Advertise** check box to advertise the IP address in its router advertisement packets.  
5. Select the **Ignore** check box to not advertise the IP addresses in router advertisement packets.  
6. Select the **Broadcast** check box to include some addresses in broadcast packets.  
7. Select the **Multicast** check box to include some addresses in multicast packets.  
8. Select the **Ineligible** check box to prevent the address from becoming the default router.  
9. From the **Priority** list, select the preference of the addresses for becoming the default router.  
   Range: 0 through 0x80000000  
   Default: 0 (This address has the least chance of becoming the default router.) |
Table 199: Router Discovery Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure physical interfaces.| 1. Click **Interface** next to Router Discovery.  
                                  2. In the **Name** box, enter the name of the interface.  
                                  3. In the **Comment** box, enter the comment.  
                                  4. In the **Name** box, enter the name of an interface.  
                                  5. In the **Comment** box, enter the comment.  
                                  6. From the **Max Advertisement Interval** list, select the maximum interval between each router advertisement message.  
                                     Range: 4 through 1800 seconds  
                                     Default: 600 seconds  
                                  7. From the **Min Advertisement Interval** list, select the minimum interval between each router advertisement message.  
                                     Range: 3 seconds through 1800 seconds  
                                     Default: 400 seconds  
                                  8. From the **Lifetime** list, select the lifetime value. |
| Specify tracing options.      | 1. Click **Traceoptions** next to Router Discovery.  
                                  2. In the **Comment** box, enter the comment for the traceoptions.  
                                  3. Click **File** next to Traceoptions.  
                                  4. In the **Comment** box, enter the comment for the filename.  
                                  5. In the **Filename** box, enter the name of the file to receive the output of the tracing operation.  
                                  6. In the **Size** box, enter the maximum trace file size.  
                                  7. From the **Files** list, select the maximum number of trace files.  
                                  8. Select one of the following:  
                                     • **no-world-readable**—To restrict the file access to owner.  
                                     • **world-readable**—To enable unrestricted access.  
                                  9. Click **Flag** next to Traceoptions.  
                                  10. Click **Add new entry** next to Flag.  
                                  11. From the **Name** list, select the flag to perform the trace operation.  
                                  12. In the **Comment** box, enter the comment for the flag.  
                                  13. Select the corresponding modifier for the tracing flag. |

Configuring RSVP (NSM Procedure)

To configure the Resource ReSerVation Protocol (RSVP) in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand **Protocols**.
4. Select **RSVP**.
5. Add or modify settings as specified in Table 200 on page 352.

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

Table 200: RSVP Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure RSVP.</td>
<td>1. Expand RSVP.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. Select the <strong>Disable</strong> check box to explicitly disable RSVP or RSVP graceful restart.</td>
</tr>
<tr>
<td></td>
<td>4. Select the <strong>No-P2mp-Subisp</strong> check box to reject Resv messages which include the S2L_SUB_LSP object.</td>
</tr>
<tr>
<td></td>
<td>5. From the <strong>Refresh Time</strong> list, select the refresh time.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 255</td>
</tr>
<tr>
<td></td>
<td>Default: 3</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Keep Multiplier</strong> list, select the keep multiplier value.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 65,535</td>
</tr>
<tr>
<td></td>
<td>Default: 30 seconds</td>
</tr>
<tr>
<td></td>
<td>7. From the <strong>Graceful Deletion-Timeout</strong> list, select the time before completing graceful deletion of signaling.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 300 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 30 seconds</td>
</tr>
</tbody>
</table>

| Configure the optimization interval for fast reroute paths. | 1. Expand RSVP.                                                             |
|                                                           | 2. Click **Fast Reroute** next to RSVP.                                    |
|                                                           | 3. In the **Comment** box, enter the comment for the fast reroute.        |
|                                                           | 4. From the **Optimize Timer** list, select the number of seconds between fast reroute detour Label-Switched Paths (LSP). |
|                                                           |   Range: 0 through 65,535                                                 |
|                                                           |   Default: 0 (disabled)                                                   |
### Table 200: RSVP Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure RSVP graceful restart. | 1. Expand RSVP.  
|                                | 2. In the Comment box, enter the comment for the filename.                 |
|                                | 3. Select the Disable check box to explicitly disable RSVP or RSVP graceful restart. |
|                                | 4. Select the Helper Disable check box to Disable RSVP graceful restart helper mode. |
|                                | 5. From the Maximum Helper Restart Time list, select the maximum length of time the router waits between when it discovers that a neighboring router has gone down and when it declares the neighbor down. Range: 1 through 1800 seconds Default: 20 seconds |
|                                | 6. From the Maximum Helper Recovery Time list, select the maximum length of time the router stores the state of neighboring routers when they undergo a graceful restart. Range: 1 through 3600 seconds Default: 0 (disabled) |

| Enable RSVP on one or more router interfaces. | 1. Click Interface next to Rsvp.  
|                                              | 2. Click Add new entry next to interface.  
|                                              | 3. In the Name box, enter the name of the interface.  
|                                              | 4. In the Comment box, enter the comment.  
|                                              | 5. Select Disable check box to explicitly disable RSVP or RSVP graceful restart.  
|                                              | 6. In the Authentication Key box, enter the authentication key (password).  
|                                              | 7. Select one of the following:  
|                                              | • aggregate—To use RSVP aggregate messages.  
|                                              | • no-aggregate—To not to use RSVP aggregate messages.  
|                                              | 8. Select one of the following:  
|                                              | • reliable—To enable reliable message delivery on the interface.  
|                                              | • no-reliable—To disable reliable message delivery on the interface.  
|                                              | 9. From the hello Interval list, select the length of time between hello packets. A value of 0 disables the sending of hello packets on the interface. Range: 1 through 60 seconds Default: 9 seconds  
|                                              | 10. In the Bandwidth box, enter the bandwidth in bits per second.  
<p>|                                              | 11. From the Update Threshold list, select the percentage change in bandwidth to trigger an Interior Gateway Protocol (IGP) update. Range: 1 through 60 seconds Default: 9 seconds |</p>
<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configuring link protection on interfaces. | 1. Click **Link Protection** next to interface.  
2. In the **Comment** box, enter the comment.  
3. Select the **Disable** check box to explicitly disable link protection on the specified interface.  
4. From the **Max Bypasses** list, select the maximum number of bypass LSPs. If you configure a value of 0, no dynamic bypass LSPs are allowed to be established for the interface.  
   Range: 1 through 99  
   Default: 1  
5. From the **Subscription** list, select the percent of the class-type or bypass LSP bandwidth that RSVP allows to be used for reservations. If you specify a value greater than 100, you are oversubscribing the class type or bypass LSP.  
   Range: 0 through 65,000  
   Default: 100 percent  
6. Select **No Node Protection** to disable node protection  
7. From the **Class of Service** list, select the CoS value.  
   Range: 0 through 7  
   Default: If you do not specify a Class of Service (CoS) value, the IP precedence bits from the packet’s IP header are used as the packet’s CoS value.  
8. From the **Hop Limit** list, select the maximum number of hops a bypass can traverse.  
   Range: 2 through 255 hops  
   Default: 255 hops  
9. Select the **No Cspf** check box to disable CSPF computation on all bypass LSPs or on a specific bypass LSP. You need to disable Constraint Shortest Path First (CSPF) for link protection to function properly on interarea paths.  
10. From the **Setup Priority** list, select the setup priority.  
    Range: 0 through 7, where 0 is the highest and 7 is the lowest priority  
    Default: 7 (The session cannot preempt any existing sessions.)  
11. From the **Reservation Priority** list, select the reservation priority.  
    Range: 0 through 7, where 0 is the highest and 7 is the lowest priority. Default: 0 (Once the session is set up, no other session can preempt it.)
### Table 200: RSVP Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure administrative groups for bypass LSPs.</td>
<td>1. Click <strong>Admin Group</strong> next to Link Protection.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Exclude</strong> next to Admin Group.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add new entry</strong> next to Exclude.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>New exclude window</strong>, enter the administrative groups to exclude for a bypass LSP.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Include All</strong> next to Admin Group.</td>
</tr>
<tr>
<td></td>
<td>6. Click <strong>Add new entry</strong> next to Include All.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>New include-all window</strong>, enter the administrative groups whose links the bypass LSP must traverse.</td>
</tr>
<tr>
<td></td>
<td>8. Click <strong>Include Any</strong> next to Admin Group.</td>
</tr>
<tr>
<td></td>
<td>9. Click <strong>Add new entry</strong> next to Include Any.</td>
</tr>
<tr>
<td></td>
<td>10. In the <strong>New include-any window</strong>, enter the administrative groups whose links the bypass LSP can traverse.</td>
</tr>
<tr>
<td>Configuring the bandwidth for bypass LSPs.</td>
<td>1. Click <strong>Bandwidth</strong> next to Link Protection.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Per Traffic Class Bandwidth</strong> box, enter the bandwidth.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>class-type number</strong> box, enter the class-type bandwidth.</td>
</tr>
<tr>
<td>Configure a bypass LSP</td>
<td>1. Click <strong>Bypass</strong> next to Link Protection.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Bypass.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Admin Group</strong> next to Bypass.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Exclude</strong> next to Admin Group.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Add new entry</strong> next to Exclude.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>New exclude window</strong>, enter the administrative groups to exclude for a bypass LSP.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>Include All</strong> next to Admin Group.</td>
</tr>
<tr>
<td></td>
<td>8. Click <strong>Add new entry</strong> next to Include All.</td>
</tr>
<tr>
<td></td>
<td>9. In the <strong>New include-all window</strong>, enter the administrative groups whose links the bypass LSP must traverse.</td>
</tr>
<tr>
<td></td>
<td>10. Click <strong>Include Any</strong> next to Admin Group.</td>
</tr>
<tr>
<td></td>
<td>11. Click <strong>Add new entry</strong> next to Include Any.</td>
</tr>
<tr>
<td></td>
<td>12. In the <strong>New include-any window</strong>, enter the administrative groups whose links the bypass LSP can traverse.</td>
</tr>
<tr>
<td></td>
<td>13. Click <strong>Bandwidth</strong> next to Link Protection.</td>
</tr>
<tr>
<td></td>
<td>14. In the <strong>Per Traffic Class Bandwidth</strong> box, enter the bandwidth.</td>
</tr>
<tr>
<td></td>
<td>15. In the class-type number box, enter the class-type bandwidth.</td>
</tr>
<tr>
<td></td>
<td>16. Click <strong>Path</strong> next to Bypass.</td>
</tr>
<tr>
<td></td>
<td>17. Click <strong>Add new entry</strong> next to Path.</td>
</tr>
<tr>
<td></td>
<td>18. In the <strong>Name</strong> box, enter the IP address of each transit router in the LSP.</td>
</tr>
<tr>
<td></td>
<td>19. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>loose</strong>—If the LSP can traverse other routers before reaching this router.</td>
</tr>
<tr>
<td></td>
<td>• <strong>strict</strong>—If the LSP must go to the next address specified in the path statement without traversing other nodes.</td>
</tr>
</tbody>
</table>
### Table 200: RSVP Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring an explicit path for bypass LSPs.</td>
<td>1. Click <strong>Path</strong> next to Link Protection.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Path.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the IP address of each transit router in the LSP.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>loose</strong>—If the LSP can traverse other routers before reaching this router.</td>
</tr>
<tr>
<td></td>
<td>• <strong>strict</strong>—If the LSP must go to the next address specified in the path statement without traversing other nodes.</td>
</tr>
<tr>
<td>Configuring the bandwidth subscription percentage for LSPs.</td>
<td>1. Click <strong>Subscription</strong> next to interface.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Link Subscription</strong> box, enter the class-type bandwidth that RSVP allows to be used for reservations.</td>
</tr>
<tr>
<td></td>
<td>3. In the class-type number percentage box, enter the percent of class-type bandwidth. You can specify bandwidth subscriptions for class types 0 through 3.</td>
</tr>
<tr>
<td>Configuring load balancing across RSVP LSPs.</td>
<td>1. Click <strong>Load Balance</strong> next to Rsvp.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. Select the <strong>Bandwidth</strong> check box to load-balance traffic between RSVP LSPs based on the bandwidth configured for each LSP.</td>
</tr>
<tr>
<td>Configuring RSVP for LMP peer interfaces.</td>
<td>1. Click <strong>Peer Interface</strong> next to Rsvp.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Peer Interface.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the peer interface name.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. Select <strong>Disable</strong> check box Explicitly disable RSVP or RSVP graceful restart.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Authentication Key</strong> box, enter the authentication key (password).</td>
</tr>
<tr>
<td></td>
<td>7. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>aggregate</strong>—To use RSVP aggregate messages.</td>
</tr>
<tr>
<td></td>
<td>• <strong>no-aggregate</strong>—To not to use RSVP aggregate messages.</td>
</tr>
<tr>
<td></td>
<td>8. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>reliable</strong>—To enable reliable message delivery on the interface.</td>
</tr>
<tr>
<td></td>
<td>• <strong>no-reliable</strong>—To disable reliable message delivery on the interface.</td>
</tr>
<tr>
<td></td>
<td>9. From the <strong>Hello Interval</strong> list, select the length of time between hello packets. A value of 0 disables the sending of hello packets on the interface. Range: 1 through 60 seconds Default: 9 seconds.</td>
</tr>
</tbody>
</table>
### Table 200: RSVP Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Preempt RSVP sessions. | 1. Click **Preemption** next to Rsvp.  
2. In the **Comment** box, enter the comment.  
3. Select one of the following:  
   - **disabled**—To stop preempt RSVP sessions.  
   - **normal**—To preempt RSVP sessions to accommodate new higher-priority sessions when bandwidth is insufficient to handle all sessions.  
   - **aggressive**—To preempt RSVP sessions whenever bandwidth is insufficient to handle all sessions.  
4. Click **Soft Preemption** next to Preemption.  
5. From the **Cleanup Timer** list, select a timer value for soft preemption  
   A value of 0 disables soft preemption.  
   Range: 0 through 180 seconds  
   Default: 30 seconds |

| Enable RSVP protocol–level trace options. | 1. Click **Traceoptions** next to Rsvp.  
2. In the **Comment** box, enter the comment for the traceoptions.  
3. Click **File** next to Traceoptions.  
4. In the **Comment** box, enter the comment for the filename.  
5. In the **Filename** box, enter the name of the file to receive the output of the tracing operation.  
6. In the **Size** box, enter the maximum trace file size.  
7. From the **Files** list, select the maximum number of trace files.  
8. Select one of the following:  
   - **no-world-readable**—To restrict the file access to owner.  
   - **world-readable**—To enable unrestricted access.  
9. Click **Flag** next to Traceoptions.  
10. Click **Add new entry** next to Flag.  
11. From the **Name** list, select the flag to perform the trace operation.  
12. In the **Comment** box, enter the comment for the flag.  
13. Select the corresponding modifier for the tracing flag. |

| Enable ultimate-hop popping on point-to-multipoint LSPs. | 1. Click **Tunnel Services** next to Rsvp.  
2. Click **Devices** next to Tunnel Services.  
3. Click **Add new entry** next to Devices.  
4. In the **New devices** window, enter the device names that specify which virtual tunnel interfaces are used to handle the RSVP traffic.  
   Range: 0 to 8 devices |

**Related Topics**  
- Configuring the ILMI Protocol (NSM Procedure) on page 255  
- Configuring Link Management Protocol (NSM Procedure) on page 275
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 201 on page 358.
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>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRRP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Comment | Specifies comment for VRRP.        | 1. Expand the Protocol tree and select VRRP.  
          |                                    | 2. Enter the comment.                    |
Table 201: VRRP Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Startup Silent Period</td>
<td>Enables the system to ignore the Master Down Event when an interface</td>
<td>1. Expand the Protocol tree and select VRRP.</td>
</tr>
<tr>
<td></td>
<td>transitions from the disabled state to the enabled state. It avoids an</td>
<td>2. Enter the startup silent period or select from the list.</td>
</tr>
<tr>
<td></td>
<td>incorrect error alarm caused by delay or interruption of incoming VRRP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>advertisement packets during the interface startup phase.</td>
<td></td>
</tr>
<tr>
<td>Traceoptions</td>
<td>Enables you to configure VRRP level tracing options.</td>
<td>1. Expand the Protocol tree.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select VRRP 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 VSTP (NSM Procedure)

VLAN Spanning Tree Protocol (VSTP) is a spanning tree protocol which creates a loop-free topology in VLANs. VSTP maintains a separate spanning tree instance for each VLAN. Different VLANs can use different spanning tree paths and VSTP can support up to 4094 different spanning tree topologies.

To configure VSTP in NSM:

1. In the navigation tree select Device Manager > Devices and select the device from the list.
2. In the configuration tree, expand Protocols.
3. Select VSTP.
4. Add/Modify the parameters under the respective tabs as specified in Table 202 on page 360.
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 202: 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.</td>
<td>1. Expand the Protocol tree and select VSTP.</td>
</tr>
<tr>
<td></td>
<td>If two bridges have the same path cost to the root bridge, the bridge</td>
<td>2. Enter the bridge priority.</td>
</tr>
<tr>
<td></td>
<td>priority determines which bridge becomes the designated bridge for a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LAN segment.</td>
<td></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</td>
<td>1. Expand the Protocol tree and select VSTP.</td>
</tr>
<tr>
<td></td>
<td>learning states before transitioning to the forwarding state.</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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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>
CHAPTER 21

Configuring Routing Options

- Configuring Confederation (NSM Procedure) on page 362
- Configuring Dynamic Tunnels (NSM Procedure) on page 363
- Configuring Fate Sharing (NSM Procedure) on page 364
- Configuring Flow Route (NSM Procedure) on page 366
- Configuring Forwarding Table (NSM Procedure) on page 368
- Configuring Generated Routes (NSM Procedure) on page 369
- Configuring Instance Export (NSM Procedure) on page 370
- Configuring Instance Import (NSM Procedure) on page 371
- Configuring Interface Routes (NSM Procedure) on page 372
- Configuring Martian Addresses (NSM Procedure) on page 373
- Configuring Maximum Paths (NSM Procedure) on page 374
- Configuring Maximum Prefixes (NSM Procedure) on page 375
- Configuring Multicast (NSM Procedure) on page 377
- Configuring Options (NSM Procedure) on page 380
- Configuring Routing Tables (NSM Procedure) on page 381
- Configuring Routing Table Groups (NSM Procedure) on page 383
- Configuring Source Routing (NSM Procedure) on page 384
- Configuring Static Routes (NSM Procedure) on page 385
- Configuring Topologies (NSM Procedure) on page 386
- Configuring Traceoptions (NSM Procedure) on page 387
Configuring Confederation (NSM Procedure)

Grouping autonomous systems (ASs) into confederations reduces the number of BGP connections required to interconnect ASs. If you administer multiple ASs that contain many BGP systems, you can group them into one or more confederations. Each confederation is identified by its own AS number, which is called a confederation AS number. To external ASs, a confederation appears to be a single AS. Thus, the internal topology of the ASs (members) making up the confederation is hidden. Because each confederation is treated as if it were a single AS, you can apply the same routing policy to all the ASs that make up the confederation.

To configure a confederation in NSM:

1. In the navigation tree, select Device Manager > Devices.
2. In the Devices list, double click the device to select it.
3. Click the Configuration tab.
4. In the configuration tree, expand Routing Options.
5. Select Confederation.
6. Add or modify the parameters as specified in Table 203 on page 362.
7. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
   - Apply—To apply the routing option settings.

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

Table 203: Confederation 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</td>
<td>Enter a comment.</td>
</tr>
<tr>
<td></td>
<td>confederation.</td>
<td></td>
</tr>
<tr>
<td>Confederation As</td>
<td>Specifies the confederation AS</td>
<td>Enter a number from 1 through 65535.</td>
</tr>
<tr>
<td></td>
<td>number.</td>
<td></td>
</tr>
</tbody>
</table>
Table 203: Confederation Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Members</td>
<td>Specifies the AS number of the confederation member, allowing you to add members to the confederation.</td>
<td>1. Expand the Confederation tree and select Members.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the New button or select a member and click the Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the AS number of the member.</td>
</tr>
</tbody>
</table>

Configuring Dynamic Tunnels (NSM Procedure)

A Virtual Private Network (VPN) that travels through a non-MPLS network requires a generic routing encapsulation (GRE) tunnel. This tunnel can be either a static tunnel or a dynamic tunnel. A static tunnel is configured manually between two provider edge (PE) routers. A dynamic tunnel is configured using BGP route resolution. You can specify the type of tunnel to be dynamically created by including the tunnel-type option.

To configure dynamic tunnels in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Routing Options.
4. Select Dynamic Tunnels.
5. Add or modify settings as specified in Table 204 on page 363.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 204: Dynamic Tunnels Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a dynamic tunnel between two PE routers</td>
<td>1. Expand Dynamic Tunnels.</td>
</tr>
<tr>
<td></td>
<td>2. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. Click Dynamic Tunnel next to Dynamic Tunnels.</td>
</tr>
<tr>
<td></td>
<td>4. Click Add new entry next to Dynamic Tunnel.</td>
</tr>
<tr>
<td></td>
<td>5. In the Name box, enter the name of the dynamic tunnel.</td>
</tr>
<tr>
<td></td>
<td>6. In the Source Address box, enter the source address.</td>
</tr>
<tr>
<td></td>
<td>7. From the Tunnel Type list, select the type of tunnel to be dynamically created. The only valid value is gre (for GRE tunnels).</td>
</tr>
<tr>
<td></td>
<td>8. Click Destination Networks next to dynamic-tunnel.</td>
</tr>
<tr>
<td></td>
<td>9. Click Add new entry next to Destination Networks.</td>
</tr>
<tr>
<td></td>
<td>10. In the Name box, enter the prefix name.</td>
</tr>
<tr>
<td></td>
<td>11. In the Comment box, enter the comment.</td>
</tr>
</tbody>
</table>
Define tracing operations that track all routing protocol functionality in the router

1. Click **Traceoptions** next to Dynamic Tunnels.
2. Expand **Traceoptions**.
3. In the **Comment** box, enter the comment for the traceoptions.
4. Click **File** next to Traceoptions.
5. In the **Comment** box, enter the comment for the filename.
6. In the **Filename** box, enter the name of the file to receive the output of the tracing operation.
7. In the **Size** box, enter the maximum trace file size.
8. From the **Files** list, select the maximum number of trace files.
9. Select one of the following:
   - Select **no-world-readable**—To restrict the file access to owner.
   - Select **world-readable**—To enable unrestricted access.
10. Click **Flag** next to Traceoptions.
11. Click **Add new entry** next to Flag.
12. From the **Name** list, select the flag to perform the trace operation.
13. In the **Comment** box, enter the comment for the flag.
14. Select the **Disable** check box to disable the tracing operation.
15. Select the modifier for the tracing flag. You can specify one or more of these modifiers:
   - Select the **Send** check box for packets being transmitted.
   - Select the **Receive** check box for packets being received.
   - Select the **Detail** check box for detailed trace information.
   - Select the **Disable** check box to disable the tracing operation.

### Configuring Fate Sharing (NSM Procedure)

Fate sharing allows you to create a database of information that the constrained shortest path first (CSPF) algorithm uses to compute one or more backup routing paths to use in case the primary path becomes unstable. The database describes the relationships between elements of the network. Through fate sharing, you can configure backup paths that minimize the number of shared links and fiber optic cables, to ensure that in the event of damage to a fiber optic cable, only the minimum amount of data is lost and that a path still exists to the destination. For a backup path to work optimally, it must not share links or physical fiber optic cables with the primary path. This ensures that a single point of failure will not affect the primary and backup paths at the same time.

This feature enables you to specify groups of objects that share characteristics resulting in backup paths to be used if primary paths fail. All objects are treated as /32 host addresses. You can specify one or more objects within a group. The objects can be LAN interfaces, device IDs, or point-to-point links.

To configure fate sharing in NSM:
1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Fate Sharing**.
6. Add or modify the parameters as specified in Table 205 on page 365.
7. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.
   - **Apply**—To apply the routing option settings.

---

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

---

### Table 205: 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><strong>Group</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</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. |
Table 205: Fate Sharing Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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 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 206 on page 367.
7. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
   - Apply—To apply the routing option settings.

NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the Updating Devices section in the Network and Security Manager Administration Guide for more information.
### Table 206: 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>
<tr>
<td>Route</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the name of the flow route.</td>
<td>1. Expand the Flow tree and select Route.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the New button or select a flow route and click the Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the flow route name.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for the flow route.</td>
<td>1. Expand the Flow tree and select Route.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the New button or select a flow route and click the Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the comment for the flow route.</td>
</tr>
<tr>
<td>Match</td>
<td>Specifies the conditions that the packet must match for the packet to be included in flow route. Match conditions are:</td>
<td>1. Expand the Route tree and select Match.</td>
</tr>
<tr>
<td></td>
<td>• Destination Port</td>
<td>2. Enter a comment for Comment, a destination address for Destination, and a source address for Source.</td>
</tr>
<tr>
<td></td>
<td>• DSCP</td>
<td>3. Configure the match conditions.</td>
</tr>
<tr>
<td></td>
<td>• Fragment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Icmp Code</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Icmp Type</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Packet Length</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Protocol</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Source Port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Tcp Flag</td>
<td></td>
</tr>
<tr>
<td>Then</td>
<td>Enables you to specify the action to take if the packet matches the conditions you have configured in the flow route.</td>
<td>1. Expand the Route tree and select Then.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Configure the then conditions for the packet.</td>
</tr>
<tr>
<td>Validation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td>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.</td>
<td>1. Expand the Flow tree and select Validation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the comment for the validation procedure.</td>
</tr>
</tbody>
</table>
Table 206: Flow Route Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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 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 207 on page 368.
7. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
   - Apply—To apply the routing option settings.

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

Table 207: 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>
</tbody>
</table>
### 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 208 on page 370.
7. Click one:
   • OK—To save the changes.
   • Cancel—To cancel the modifications.
   • Apply—To apply the routing option settings.

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

Table 208: 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>
</tbody>
</table>
| Defaults | Enables you to specify globally generated route options. These are treated as global defaults and apply to all the generated routes you configure. | 1. Expand the Generate tree and select Defaults.  
2. Configure the default route options. |
| Route    | Enables you to configure individually generated routes. You can also configure globally generated route options. These options apply to the individual destination only and override any options you configured in Defaults. | 1. Expand the Generate tree and select Route.  
2. Configure the individual route options. |

Configuring Instance Export (NSM Procedure)

Current configurations that use routing table groups define a policy to select routes in an IGP export policy. However, no policy controls the export process itself. You can configure the instance export policy to control the export process. The policy model supports both interinstance route export and IGP export.

To configure an instance export policy in NSM:

1. In the navigation tree, select Device Manager > Devices.
2. In the Devices list, double click the device to select it.
3. Click the Configuration tab.
4. In the configuration tree, expand Routing Options.
5. **Select Instance Export** and specify the export policies for routes being exported from a routing instance.

6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
   - Apply—To apply the routing option settings.

---

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

---

### Configuring Instance Import (NSM Procedure)

You can apply one or more policies to routes being imported into a routing instance.

To configure instance import in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. **Select Instance Import** and specify the import policies to be applied to the routes that are imported to a routing instance.
6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
   - Apply—To apply the routing option settings.

---

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

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

To configure interface routes in NSM:

1. In the navigation tree, select Device Manager > Devices.
2. In the Devices list, double click the device to select it.
3. Click the Configuration tab.
4. In the configuration tree, expand Routing Options.
5. Select Interface Routes.
6. Add or modify the parameters as specified in Table 209 on page 372.
7. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
   - Apply—To apply the routing option settings.

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

### Table 209: 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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Family</th>
<th>Specifies the address family as IPv4 or IPv6.</th>
<th>1. Expand the Interface Routes tree and select Family.</th>
</tr>
</thead>
<tbody>
<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 209: 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 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 210 on page 373.
7. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
   - Apply—To apply the routing option settings.

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

Table 210: 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. |
Table 210: Configuring Martian Address Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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  
• Orlonger  
• 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. |

Configuring Maximum Paths (NSM Procedure)

You can configure a limit for the number of routes installed in a routing table based upon the number of route paths in the table.

To configure a maximum paths limit in NSM:

1. In the navigation tree, select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. Click the Configuration tab.
4. In the configuration tree, expand Routing Options.
5. Select Maximum Paths.
6. Enter the parameters as specified in Table 211 on page 375.
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 path limit.</td>
<td>Enter the comment.</td>
</tr>
<tr>
<td>Limit</td>
<td>Indicates the maximum number of routes. If this limit is reached, a warning is triggered and additional routes are rejected.</td>
<td>Enter limit value or select a value 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 a value from the list.</td>
</tr>
</tbody>
</table>
| Threshold | Specifies what is to be done when the routing table reaches the maximum path value. The options are:  
• None  
• threshold—Percentage of the maximum number of routes when installed, starts triggering the warning. You can configure a percentage of the Limit value that when reached starts triggering the warnings.  
• log-only—Sets the route limit as an advisory limit. An advisory limit triggers only a warning, and additional routes are not rejected. | 1. Expand the Maximum Paths tree and select Threshold.  
2. Select the radio-button. |

---

**Configuring Maximum Prefixes (NSM Procedure)**

You can configure a limit for the number of routes installed in a routing table based upon the number of route prefixes in the table.

To configure maximum prefixes limit in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.

5. Select **Maximum Prefixes**.

6. Enter the parameters as specified in Table 212 on page 376.

7. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
   - Apply—To apply the routing option settings.

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

<table>
<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>
<tr>
<td>Threshold</td>
<td>Specifies what is to be done when the routing table reaches the maximum prefix value. The options are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• None—No action is to be taken.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• threshold—You can configure a percentage for the maximum number of prefixes, which when installed, triggers the warning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• log-only—Sets the prefix limit as an advisory limit. An advisory limit triggers only a warning, and additional routes are not rejected.</td>
<td>1. Expand the <strong>Maximum Prefixes</strong> tree and select <strong>Threshold</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Select the option button.</td>
<td></td>
</tr>
</tbody>
</table>
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 213 on page 377.
7. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
   - Apply—To apply the routing option settings.

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

Table 213: Configuring Multicast 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 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>
<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 213: Configuring Multicast Fields (continued)

<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. |
### Table 213: Configuring Multicast Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Ssm Map | SSM mapping translate IGMPv1 or IGMPv2 membership reports to an IGMPv3 report allowing you to support an SSM network without requiring all hosts to support IGMPv3. | 1. Expand the **Multicast** tree and select **Ssm Map**.  
2. Click the New button or select an SSM map and click the Edit button.  
3. Specify the SSM policy for the SSM map and the source address. |
| Traceoptions | Defines tracing options for the multicast group. You can also set up the file management and access control parameters. | 1. Expand the **Multicast** tree and select the **Traceoptions** tab.  
2. Set up the file and flag parameters. |

### Configuring Options (NSM Procedure)

You can configure the types of system logging messages sent about the routing protocols process to the system log message file. These messages are also displayed on the system console. You can log messages at a particular level or up to and including a particular level.

To configure options in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Options**.
6. Enter the parameters as specified in Table 214 on page 381.
7. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.
   - **Apply**—To apply the routing option settings.

**NOTE:** After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the **Updating Devices** section in the *Network and Security Manager Administration Guide* for more information.
### Table 214: 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 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 215 on page 382.
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>Name</td>
<td>Specifies the unique name for the routing table.</td>
<td>1. Expand the <strong>Routing Options</strong> tree and select <strong>Rib</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the New button or select a routing table and click the Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the name for the routing table.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for the route resolution.</td>
<td>1. Expand the <strong>Routing Options</strong> tree and select <strong>Rib</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the New button or select a routing table and click the Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the comment for the routing table.</td>
</tr>
<tr>
<td>Aggregate</td>
<td>Enables you to configure the aggregate routes for the routing table.</td>
<td>1. Expand the <strong>Rib</strong> tree and select <strong>Aggregate</strong>.</td>
</tr>
<tr>
<td></td>
<td>Aggregation allows you to combine groups of routes with common addresses</td>
<td>2. Select the global aggregate route options in <strong>Defaults</strong> and individual aggregate route options in <strong>Route</strong>.</td>
</tr>
<tr>
<td></td>
<td>into a single entry in the routing table. This decreases the size of the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>routing table as well as the number of route advertisements sent by the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>router.</td>
<td></td>
</tr>
<tr>
<td>Generate</td>
<td>Enables you to configure generated routes, which are used as routes of</td>
<td>1. Expand the <strong>Rib</strong> tree and select <strong>Generate</strong>.</td>
</tr>
<tr>
<td></td>
<td>last resort in the routing table.</td>
<td>2. Select the default route to the destination address in <strong>Defaults</strong> and individually generated route options in <strong>Route</strong>.</td>
</tr>
<tr>
<td>Martians</td>
<td>Enables you to configure martian addresses in the routing table.</td>
<td>1. Expand the <strong>Rib</strong> tree and select <strong>Martian</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the martian addresses.</td>
</tr>
<tr>
<td>Maximum Paths</td>
<td>Enables you to configure a limit for the number of routes installed in a</td>
<td>1. Expand the <strong>Rib</strong> tree and select <strong>Maximum Paths</strong>.</td>
</tr>
<tr>
<td></td>
<td>routing table.</td>
<td>2. Enter the <strong>Maximum Paths</strong> and the <strong>Threshold</strong>.</td>
</tr>
<tr>
<td>Maximum Prefixes</td>
<td>Enables you to configure a limit for the number of routes installed in a</td>
<td>1. Expand the <strong>Rib</strong> tree and select <strong>Maximum Prefixes</strong>.</td>
</tr>
<tr>
<td></td>
<td>routing table.</td>
<td>2. Set up the <strong>Maximum Prefixes</strong> and the <strong>Threshold</strong>.</td>
</tr>
</tbody>
</table>
Table 215: 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 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 216 on page 384.
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 216: 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 Routing Options tree and select Rib Group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the New button or select a routing table group and click the Edit 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 Routing Options tree and select Rib Group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the New button or select a routing table group and click the Edit 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 Routing Options tree and select Rib Group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the New button or select a routing table group and click the Edit 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 rib-group tree and select Import Policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Set up the import policies for the routing table group.</td>
</tr>
<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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the name of the routing table.</td>
</tr>
</tbody>
</table>

### Configuring Source Routing (NSM Procedure)

You can configure source routing to specify IP addresses of the devices along the path, that you want an IP packet to take on its way to its destination.

To configure source routing in NSM:

1. In the navigation tree, select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. Click the **Configuration** tab.

4. In the configuration tree, expand **Routing Options**.

5. Select **Source Routing**.

6. Enter the parameters as specified in Table 217 on page 385.

7. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.
   - **Apply**—To apply the routing option settings.

---

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

---

**Table 217: 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>
<tr>
<td>Ip</td>
<td>Specifies the IPv4/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 218 on page 386.

7. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
   - Apply—To apply the routing option settings.

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

<table>
<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 Topologies (NSM Procedure)

For Multitopology Routing to run on the router, you need to configure one or more topologies. For each topology, you specify a string value, such as voice, that defines the type of traffic, as well as an interface family, such as IPv4. In addition, a default topology is automatically created. You can also enable a topology for IPv4 multicast traffic. Each topology that you configure creates a new routing table and populates it with direct routes from the topology.

To configure topologies in NSM:
1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Routing Options**.
4. Select **Topologies**.
5. Add or modify settings as specified in Table 219 on page 387.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.

### Table 219: Topology Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure topologies.</td>
<td>1. Expand <strong>Topologies</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td>Configure the type of family address type.</td>
<td>1. Click <strong>Family</strong> next to Topologies.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Family.</td>
</tr>
<tr>
<td></td>
<td>3. Expand <strong>key-chain</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. From the <strong>Name</strong> list, select the type of family address type.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. Click <strong>Topology</strong> next to family.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>Add new entry</strong> next to Topology.</td>
</tr>
<tr>
<td></td>
<td>8. In the <strong>Name</strong> box, enter the name of the topology.</td>
</tr>
<tr>
<td></td>
<td>9. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
</tbody>
</table>

### Configuring Trace Options (NSM Procedure)

You can configure tracing operations for routing protocols to track all general routing operations and record them in a log file. Any global tracing operations that you configure are inherited by the individual routing protocols. To modify the global tracing operations for an individual protocol, configure the tracing option when configuring that protocol.

To configure tracing options for routing protocols in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Traceoptions**.
6. Add or modify the parameters as specified in Table 220 on page 388.
7. Click one:
   - **OK**—To save the changes.
• Cancel—To cancel the modifications.
• Apply—To apply the routing option settings.

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

Table 220: Traceoption 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 tracing options.</td>
<td>Enter the comment.</td>
</tr>
</tbody>
</table>
| File | Specifies the file to receive the output of the tracing operation. | 1. Expand the Traceoptions tree and select File.  
2. Enter the file parameters. |
| Flag | Specifies the global routing protocol tracing options to be performed. You can specify more than one option. | 1. Expand the Traceoptions tree and select File.  
2. Enter the flag parameters. |
Configuring Security

- Configuring Authentication Key Updates (NSM Procedure) on page 389

**Configuring Authentication Key Updates (NSM Procedure)**

You can configure authentication key updates for the Border Gateway Protocol (BGP) and Label Distribution Protocol (LDP) routing protocols. Authentication key updates can occur without interrupting routing and signaling protocols such as Open Shortest Path First (OSPF), and Resource Reservation Setup Protocol (RSVP) when configured using this option.

To configure authentication keys 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 **Security**.
4. Select **Authentication Key Chains**.
5. Add or modify settings as specified in Table 221 on page 390.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.
Configure authentication key updates for BGP and LDP routing protocols.

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Expand <strong>Authentication Key Chains</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Key Chain</strong> next to Authentication Key Chains.</td>
</tr>
<tr>
<td>3.</td>
<td>Click <strong>Add new entry</strong> next to Key Chains.</td>
</tr>
<tr>
<td>4.</td>
<td>Expand <strong>key-chain</strong>.</td>
</tr>
<tr>
<td>5.</td>
<td>In the <strong>Name</strong> box, enter the keychain name.</td>
</tr>
<tr>
<td>6.</td>
<td>In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td>7.</td>
<td>In the <strong>Description</strong> box, enter the text description of the authentication keychain in quotes.</td>
</tr>
<tr>
<td>8.</td>
<td>From the <strong>Tolerance</strong> list, select the clock skew tolerance.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 999999999</td>
</tr>
<tr>
<td>9.</td>
<td>Click <strong>Key</strong> next to key-chain.</td>
</tr>
<tr>
<td>10.</td>
<td>Click <strong>Add new entry</strong> next to Key.</td>
</tr>
<tr>
<td>11.</td>
<td>From the <strong>Name</strong> list, select the key value.</td>
</tr>
<tr>
<td>12.</td>
<td>In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td>13.</td>
<td>In the <strong>Secret</strong> box, enter the secret for the key in encrypted text.</td>
</tr>
<tr>
<td>14.</td>
<td>In the <strong>Start Time</strong> box, enter the start time in UTC (Coordinated Universal Time).</td>
</tr>
</tbody>
</table>
CHAPTER 23

Configuring Services

- Configuring Adaptive Services PICs (NSM Procedure) on page 391
- Configuring Border Signaling Gateways (NSM Procedure) on page 392
- Configuring Class of Service (NSM Procedure) on page 412
- Configuring Intrusion Detection Service (NSM Procedure) on page 415
- Tracing Services PIC Operations (NSM Procedure) on page 419
- Configuring Network Address Translation (NSM Procedure) on page 420
- Configuring PGCP (NSM Procedure) on page 425
- Configuring Service Interface Pools (NSM Procedure) on page 455
- Configuring a Service Set (NSM Procedure) on page 456
- Configuring Stateful Firewall (NSM Procedure) on page 460

Configuring Adaptive Services PICs (NSM Procedure)

The Adaptive Services (AS) and Multiservices PICs provide adaptive services interfaces, which allow you to coordinate multiple services on a single PIC by configuring a set of services and applications. The AS and Multiservices PICs offer a special range of services you configure in one or more service sets.

To configure adaptive services PICs in NSM:

1. In the navigation tree select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. In the Configuration tab, expand Services.
5. Add or modify the settings as specified in Table 222 on page 392.
6. Click one:
   • OK—To save the changes.
   • Cancel—To cancel the modifications.
### Table 222: Adaptive Services Pics Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure adaptive services or multiservices PIC tracing operations. | 1. Click **Traceoptions** next to Adaptive Services Pics.  
2. Select the **No Remote Trace** check box to disable remote tracing.  
3. Expand **Traceoptions**.  
4. Click **File** next to Trace Options.  
5. In the **Comment** box, enter the comment.  
6. In the **Filename** box, enter the name of the file to receive the output of the tracing operation.  
7. In the **Comment** box, enter the comment.  
8. In the **Size** box, enter the maximum size of each trace file in kilobytes (KB), megabytes (MB) or gigabytes (GB).  
   Range: 2 through 1000 files  
   Default: 3 files  
9. From the **Files** list, select the maximum number of trace files.  
10. Select one of the following:  
   - **no-world-readable**—To allow any user to read the log file.  
   - **world-readable**—To prevent any user from reading the log file.  
11. Click **Flag** next to Trace Options.  
12. Click **Add new entry** next to flag.  
13. From the **Name** list, select a tracing operation to perform.  
14. In the **Comment** box, enter the comment. |

**Related Topics**
- Configuring Service Interface Pools (NSM Procedure) on page 455
- Configuring a Service Set (NSM Procedure) on page 456
- Tracing Services PIC Operations (NSM Procedure) on page 419

---

### Configuring Border Signaling Gateways (NSM Procedure)

You can configure border signaling gateways using this option. See the following topics:

- Configuring Gateway Properties (NSM Procedure) on page 392

### Configuring Gateway Properties (NSM Procedure)

- Configuring Gateway (NSM Procedure) on page 393
- Configuring an Admission Controller (NSM Procedure) on page 393
- Configuring Session Policy Decision Function (NSM Procedure) on page 394
- Configuring Service Point (NSM Procedure) on page 396
Configuring Gateway (NSM Procedure)

To configure a gateway in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Services > Border Signaling Gateway.
4. Select Gateway.
5. Add or modify settings as specified in Table 223 on page 393.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

Table 223: Gateway Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a gateway.</td>
<td>1. Click Add new entry next to Gateway.</td>
</tr>
<tr>
<td></td>
<td>2. In the Name box, enter the identifier for the BSG.</td>
</tr>
<tr>
<td></td>
<td>3. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. From the Service Interface list, select the name and logical unit number of the Multiservices PIC or DPC.</td>
</tr>
</tbody>
</table>

Configuring an Admission Controller (NSM Procedure)

To configure an admission controller in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Services > Border Signaling Gateway.
4. Select Gateway.
5. Add or modify settings as specified in Table 224 on page 394.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.
NOTE: For devices running JUNOS Release 9.5 and later, admission controller settings will be available in the device editor only when the policy-management mode is in the in-device mode. By default, admission controller settings can be created only in the Policy Manager and Object Manager.

### Table 224: Admission Controller Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| **Configure an admission controller for a border signaling gateway (BSG).** | 1. Click **Add new entry** next to Gateway.  
2. Click **Admission Controller** next to gateway.  
3. In the **Name** box, enter the identifier for the BSG.  
4. In the **Comment** box, enter the comment.  
5. From the **Service Interface** list, select the name and logical unit number of the Multiservices PIC or DPC.  
6. Click **Admission Control** next to gateway.  
7. Click **Add new entry** next to Admission Control.  
8. In the **Name** box, enter the name of the admission controller.  
9. In the **Comment** box, enter the comment. |
| **Configure admission control settings for dialogs.** | 1. Click **Dialogs** next to admission-control.  
2. From the **Maximum Concurrent** list, select the maximum number of concurrent dialogs. 0 causes all calls to be rejected.  
   Range: 0 through 100,000  
3. From the **Committed Attempts Rate** list, select the maximum number of attempts per second to initiate a dialog.  
   Range: 0 through 100  
4. From the **Committed Burst Rate** list, select the maximum number of dialogs allowed to burst above the committed rate and still be accepted. |
| **Configure admission control settings for out-of-dialog transactions.** | 1. Click **Transactions** next to admission-control.  
2. From the **Maximum Concurrent** list, select the maximum number of concurrent transactions. 0 causes all calls to be rejected.  
   Range: 0 through 50000  
3. From the **Committed Attempts Rate** list, select the maximum number of attempts per second to initiate an out-of-dialog transaction.  
   Range: 0 through 1500  
4. From the **Committed Burst Rate** list, select the maximum number of transactions allowed to burst above the committed rate and still be accepted.  
   Range: 0 through 3000 |

### Configuring Session Policy Decision Function (NSM Procedure)

To configure session policy decision function in NSM:
1. In the NSM navigation tree, select **Device Manager > Devices**.

2. Click the **Device Tree** tab, and then double-click the device to select it.

3. Click the **Configuration** tab. In the configuration tree, expand **Services > Border Signaling Gateway**.

4. Select **Gateway**.

5. Add or modify settings as specified in Table 225 on page 395.

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

### Table 225: Session Policy Decision Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| **Configure the SPDF.** | 1. Click **Add new entry** next to Gateway.  
2. Click **Embedded Spdf** next to gateway.  
3. In the **Comment** box, enter the comment. |

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| **Configure service classes for the embedded SPDF.** | 1. Click **Service Class** next to Embedded Spdf.  
2. From the **Service Interface** list, select the name and logical unit number of the Multiservices PIC or DPC.  
3. Click **Add new entry** next to Service Class.  
4. In the **Name** box, enter the identifier for the service class.  
5. In the **Comment** box, enter the comment. |
Table 225: Session Policy Decision Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify the service class term properties. | 1. Click Term next to service-class.  
2. Click Add new entry next to Term.  
3. In the Name box, enter the identifier for the term.  
4. In the Comment box, enter the comment.  
5. Click From next to term.  
6. In the Comment box, enter the comment.  
7. Click Media Type next to From.  
8. Click Add new entry next to Media Type.  
9. In the New media-type window, select the type of media that the service class matches.  
   • any-media—Match all media types.  
   • audio—Match audio traffic.  
   • video—Match video traffic.  
10. Click Then next to term.  
11. In the Comment box, enter the comment.  
12. Select the Reject check box to not accept the traffic and return a rejection message.  
13. From the Committed Information Rate list, select the maximum bandwidth that can be allocated to a packet that is flowing under normal line conditions.  
Range: 0 through 2147483647  
14. From the Committed Burst Size list, select the maximum number of bytes allowed for incoming packets to burst above the committed information rate.  
Range: 20 through 2147483647  
15. From the Dscp list, select the values for DSCP marking that the BSG uses for traffic that matches the service class term.  
Default: be |

Configuring Service Point (NSM Procedure)

To configure session policy decision function in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.  
2. Click the Device Tree tab, and then double-click the device to select it.  
3. Click the Configuration tab. In the configuration tree, expand Services > Border Signaling Gateway.  
4. Select Gateway.  
5. Add or modify settings as specified in Table 226 on page 397.  
6. Click one:  
   • OK—Saves the changes.  
   • Cancel—Cancels the modifications.
Table 226: Service Point Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure a service point. | 1. Click **Add new entry** next to Gateway.  
2. Click **Service Point** next to gateway.  
3. Click **Add new entry** next to Service Point.  
4. In the **Name** box, enter the name.  
5. In the **Comment** box, enter the comment.  
6. From the **Service Point Type** list, select the type of VoIP protocol for this service point.  
Values: sip  
7. From the **Service Interface** list, select the name of the service interface.  
8. From the **Default Media Realm** list, select the realm number used to match to a virtual interface  
Range: 0 through 1023 |
| Configure service classes for the embedded SPDF. | 1. Click **Service Class** next to Embedded Spdf.  
2. From the **Service Interface** list, select the name and logical unit number of the Multiservices PIC or DPC.  
3. Click **Add new entry** next to Service Class.  
4. In the **Name** box, enter the identifier for the service class.  
5. In the **Comment** box, enter the comment. |
| Assign new call usage policies or policy sets to the service point. | 1. Click **Service Policies** next to service-point.  
2. In the **Comment** box, enter the comment.  
3. Click **New Call Usage Policies** next to Service Policies.  
4. Click **Add new entry** next to New Call Usage Policies.  
5. In the **New new-call-usage-policies** window, enter the names of new call usage policies or policy sets.  
Syntax: If you specify more than one policy or policy set, you must enclose all policy names in brackets.  
7. Click **Add new entry** next to New Transaction Policies.  
8. In the **New new-transaction-policies** window, enter the names of new call usage policies or policy sets.  
Syntax: If you specify more than one policy or policy set, you must enclose all policy names in brackets.  
9. Click **Transport Details** next to service-point.  
10. In the **Comment** box, enter the comment.  
11. From the **Port Number** list, select the port number.  
12. In the **Ip Address** box, enter the IP address.  
13. Select the corresponding transport protocol. |

**Configuring SIP Policies and Timers (NSM Procedure)**

See the following topics:

- Configuring Message Manipulation Rules (NSM Procedure) on page 398
- Configuring New Call Usage Policy (NSM Procedure) on page 399
To configure message manipulation rules in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Services > Border Signaling Gateway.
4. Select Gateway.
5. Add or modify settings as specified in Table 227 on page 398.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

### Table 227: Message Manipulate Rules Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a message manipulation rule.</td>
<td>1. Click Add new entry next to Gateway.</td>
</tr>
<tr>
<td></td>
<td>2. Click Sip next to gateway.</td>
</tr>
<tr>
<td></td>
<td>3. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. Click Message Manipulation Rules next to Sip.</td>
</tr>
<tr>
<td></td>
<td>5. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td>Configure a manipulation rule.</td>
<td>1. Click Manipulation Rule next to Message Manipulation Rules.</td>
</tr>
<tr>
<td></td>
<td>2. Click Add new entry next to Manipulation Rule.</td>
</tr>
<tr>
<td></td>
<td>3. In the Name box, enter the name of the manipulation rule.</td>
</tr>
<tr>
<td></td>
<td>4. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. Click Actions next to manipulation-rule.</td>
</tr>
<tr>
<td></td>
<td>6. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>7. Click Request Uri next to Actions.</td>
</tr>
<tr>
<td></td>
<td>8. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>9. Click Field Value next to Request Uri.</td>
</tr>
<tr>
<td></td>
<td>10. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>11. Click Modify Regular Expression next to Field Value.</td>
</tr>
<tr>
<td></td>
<td>12. Click Add new entry next to Modify Regular Expression.</td>
</tr>
<tr>
<td></td>
<td>13. In the Name box, enter the regular expression that you want to modify.</td>
</tr>
<tr>
<td></td>
<td>14. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>15. In the With box, enter the regular expression that you want to replace the regular expression.</td>
</tr>
</tbody>
</table>
Table 227: Message Manipulate Rules Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Session Initiation Protocol (SIP) header.</td>
<td>1. Click <strong>Sip Header</strong> next to manipulation-rule.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Sip Header.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the name of the header field in SIP headers for which you want to define field values.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Field Value</strong> next to sip-header.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>7. Select the <strong>Remove All</strong> check box to remove all instances of the header field.</td>
</tr>
<tr>
<td></td>
<td>8. Click <strong>Add</strong> next to Field Value.</td>
</tr>
<tr>
<td></td>
<td>9. Select from the following field values:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Add</strong>—Adds an instance of the header field with the field value that you define. If the header field already exists, the software creates a new instance of the header field and inserts it before any existing instance of the header field. Having more than one field value is not allowed for some header fields.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Add Missing</strong>—Adds a new header field with the field value that you define if the header field is missing from the SIP header.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Add Overwrite</strong>—Adds a new header field with the field value that you define if the header field is missing from the SIP header. Its field value is overwritten with the new field value. The software overwrites the field value in all instances of the header field.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Modify Regular Expression</strong>—Changes the value of a regular expression.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Reject Regular Expression</strong>—Rejects SIP messages and terminates the usage that the message is part of if the header field contains the regular expression.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Remove Regular Expression</strong>—Removes all of the header fields that have field values that match this regular expression.</td>
</tr>
<tr>
<td></td>
<td>10. Enter the Name and Comment.</td>
</tr>
</tbody>
</table>

Configuring New Call Usage Policy (NSM Procedure)

To configure new call usage policy in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Services > Border Signaling Gateway**.
4. Select **Gateway**.
5. Add or modify settings as specified in Table 228 on page 400.
6. Click one:
• OK—Saves the changes.
• Cancel—Cancels the modifications.

Table 228: New Call Usage Policy Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a new call usage policy.</td>
<td>1. Click <strong>Add new entry</strong> next to Gateway.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Sip</strong> next to gateway.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>New Call Usage Policy</strong> next to Sip.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Add new entry</strong> next to New Call Usage Policy.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Name</strong> box, enter the identifier for the new call usage policy.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td>Define the new call usage policy term properties.</td>
<td>1. Click <strong>Term</strong> next to new-call-usage-policy.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Term.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the identifier for the term.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
</tbody>
</table>
### Table 228: New Call Usage Policy Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure match conditions for a new call usage policy. | 1. Click **From** next to term.  
2. In the **Comment** box, enter the comment.  
3. Click **Add new entry** next to Term.  
4. In the **Name** box, enter the identifier for the term.  
5. Click **Contact** next to From.  
6. Click **Add new entry** next to Contact.  
7. In the **Comment** box, enter the comment.  
8. Click **RegularExpression** next to contact.  
9. Click **Add new entry** next to Regular Expression.  
10. In the **New regular-expression** window, enter the regular expression used to match the contents of the contact field.  
   Syntax: To specify more than one regular expression, enclose the regular expressions in brackets.  
11. Click **Method** next to From.  
12. Click **Add new entry** next to Method.  
13. From the **Name** list, select **method-invite** to match the policy to SIP INVITE methods.  
14. In the **Comment** box, enter the comment.  
15. Click **Request Uri** next to From.  
16. Click **Add new entry** next to Request URI.  
17. In the **Comment** box, enter the comment.  
18. Click **RegularExpression** next to request-uri.  
19. In the **New regular-expression** window, enter the regular expression used to match the contents of the request URI field.  
   Syntax: To specify more than one regular expression, enclose the regular expressions in brackets.  
20. Click **Source Address** next to From.  
21. Click **Add new entry** next to Source Address.  
22. In the **New source-address** window, enter the IP addresses that you want to match.  
   Syntax: To specify more than one IP address, enclose the IP addresses in brackets.
Table 228: New Call Usage Policy Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Define the actions performed on incoming requests that match the new call usage policy. | 1. Click **Then** next to From.  
2. In the **Comment** box, enter the comment.  
3. Select one of the following check boxes:  
   - **accept**—To accept the traffic and send it to its destination.  
   - **reject**—To reject the traffic and return a rejection message. Rejected traffic can be logged or sampled.  
   - **trace**—To trace messages accepted by this policy.  
4. Click **Media Policy** next to Then.  
5. In the **Comment** box, enter the comment.  
6. Select the **No Anchoring** check box to disable or enable media anchoring for the policy.  
7. In the **Service Class** box, enter the name of the service class to be applied to traffic that matches the new call usage policy.  
8. Click **Data Inactivity Detection** next to Media Policy.  
9. In the **Comment** box, enter the comment.  
10. From the **Inactivity Duration** list, select the time interval that determines inactivity. Range: 30 through 3600 |

Configuring New Call Usage Policy Set (NSM Procedure)

To configure new call usage policy set in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.  
2. Click the **Device Tree** tab, and then double-click the device to select it.  
3. Click the **Configuration** tab. In the configuration tree, expand **Services > Border Signaling Gateway**.  
4. Select **Gateway**.  
5. Add or modify settings as specified in Table 229 on page 403.  
6. Click one:  
   - **OK**—Saves the changes.  
   - **Cancel**—Cancels the modifications.
### Table 229: New Call Usage Policy Set Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a new call usage policy set.</td>
<td>1. Click <strong>Add new entry</strong> next to Gateway.  &lt;br&gt;2. Click <strong>Sip</strong> next to gateway.  &lt;br&gt;3. In the <strong>Comment</strong> box, enter the comment.  &lt;br&gt;4. Click <strong>New Call Usage Policy Set</strong> next to Sip.  &lt;br&gt;5. Click <strong>Add new entry</strong> next to New Call Usage Policy Set.  &lt;br&gt;6. In the <strong>Name</strong> box, enter the identifier for the new call usage policy set.  &lt;br&gt;7. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
</tbody>
</table>

| Define the new call usage policies. | 1. Click **Policy Name** next to new-call-usage-policy-set.  <br>2. Click **Add new entry** next to Policy Name.  <br>3. In the **New policy-name** window, enter the names of one or more new call usage policies that you want to add to the set. Syntax: To specify a list of policies, enclose the policy names in brackets. |

### Configuring New Transaction Policy (NSM Procedure)

To configure new transaction policy in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Services > Border Signaling Gateway**.
4. Select **Gateway**.
5. Add or modify settings as specified in Table 230 on page 404.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

---

**NOTE:** For devices running JUNOS Release 9.5 and later, new transaction policy settings will be available in the device editor only when the policy-management mode is in-device mode. By default, new transaction policy settings can be created only in the Policy Manager and Object Manager.
Table 230: Transaction Policy Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure new transaction policy.</td>
<td>1. Click <strong>Add new entry</strong> next to Gateway.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Sip</strong> next to gateway.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>New Transaction Policy</strong> next to Sip.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Add new entry</strong> next to New Call Transaction Policy.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Name</strong> box, enter the identifier for the new transaction policy.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td>Define the new transaction policy term properties.</td>
<td>1. Click <strong>Term</strong> next to new-transaction-policy.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Term.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the identifier for the term.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td>Configure match conditions for a new transaction policy.</td>
<td>1. Click <strong>From</strong> next to term.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add new entry</strong> next to Term.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Name</strong> box, enter the identifier for the term.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Contact</strong> next to From.</td>
</tr>
<tr>
<td></td>
<td>6. Click <strong>Add new entry</strong> next to Contact.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>8. Click <strong>Regular Expression</strong> next to contact.</td>
</tr>
<tr>
<td></td>
<td>9. Click <strong>Add new entry</strong> next to Regular Expression.</td>
</tr>
<tr>
<td></td>
<td>10. In the <strong>New regular-expression</strong> window, enter the regular expression used to match the contents of the contact field.</td>
</tr>
<tr>
<td></td>
<td>Syntax: To specify more than one regular expression, enclose the regular expressions in brackets.</td>
</tr>
<tr>
<td></td>
<td>11. Click <strong>Method</strong> next to From.</td>
</tr>
<tr>
<td></td>
<td>12. Click <strong>Add new entry</strong> next to Method.</td>
</tr>
<tr>
<td></td>
<td>13. From the <strong>Name</strong> list, select the type of SIP method.</td>
</tr>
<tr>
<td></td>
<td>14. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>15. Click <strong>Request Uri</strong> next to From.</td>
</tr>
<tr>
<td></td>
<td>16. Click <strong>Add new entry</strong> next to Request Uri.</td>
</tr>
<tr>
<td></td>
<td>17. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>18. Click <strong>Regular Expression</strong> next to request-uri.</td>
</tr>
<tr>
<td></td>
<td>19. In the <strong>New regular-expression</strong> window, enter the regular expression used to match the contents of the request URI field.</td>
</tr>
<tr>
<td></td>
<td>Syntax: To specify more than one regular expression, enclose the regular expressions in brackets.</td>
</tr>
<tr>
<td></td>
<td>20. Click <strong>Source Address</strong> next to From.</td>
</tr>
<tr>
<td></td>
<td>21. Click <strong>Add new entry</strong> next to Source Address.</td>
</tr>
<tr>
<td></td>
<td>22. In the <strong>New source-address</strong> window, enter the IP addresses that you want to match.</td>
</tr>
<tr>
<td></td>
<td>Syntax: To specify more than one IP address, enclose the IP addresses in brackets.</td>
</tr>
</tbody>
</table>
Table 230: Transaction Policy Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Define the actions performed on incoming requests that match this policy. | 1. Click Then next to From.  
2. In the Comment box, enter the comment.  
3. Select the following check boxes:  
  - accept—To accept the traffic and send it to its destination  
  - reject—To reject the traffic and return a rejection message. Rejected traffic can be logged or sampled.  
  - trace—To trace messages accepted by this policy  
4. In the Admission Control box, enter the controller name.  
5. Click Message Manipulation next to Then.  
6. In the Comment box, enter the comment.  
7. Click Forward Manipulation next to Message Manipulation.  
8. Click Add new entry next to Forward Manipulation.  
9. In the Name box, enter the name of the forward message manipulation rules that you want to add to your new transaction policy.  
10. In the Comment box, enter the comment.  
11. Click Reverse Manipulation next to Message Manipulation.  
12. Click Add new entry next to Reverse Manipulation.  
13. In the Name box, enter the name of the reverse message manipulation rules that you want to add to your new transaction policy.  
14. In the Comment box, enter the comment. |
| Configure the next-hop destination and egress service point for a new transaction policy. | 1. Click Route next to Then.  
2. In the Comment box, enter the comment.  
3. In the Egress Service Point box, enter the name of the service point that you want to use as the egress service point.  
4. Click Next Hop next to Route.  
5. In the Comment box, enter the comment.  
6. Click Address next to Next Hop.  
7. Select the SIP entity towards which SIP requests are sent.  
  - address—To configure the destination IPv4 address of the next hop to contact  
    a. In the Comment box, enter the comment.  
    b. In the IPv4 Address box, enter the destination IPv4 address of the next hop to contact.  
    c. From the Port list, select the destination port of the next hop to contact. Default: 5060  
    d. Click Transport protocol next to Address.  
    e. In the Comment box, enter the comment.  
    f. Select the transport protocol for routing to the next hop.  
  - request-uri—To route all requests and responses on the dialog according to SIP. |

Configuring a New Transaction Policy Set (NSM Procedure)

To configure a new transaction policy set in NSM:
1. In the NSM navigation tree, select **Device Manager > Devices**.

2. Click the **Device Tree** tab, and then double-click the device to select it.

3. Click the **Configuration** tab. In the configuration tree, expand **Services > Border Signaling Gateway**.

4. Select **Gateway**.

5. Add or modify settings as specified in Table 231 on page 406.

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

---

**NOTE:** For devices running JUNOS Release 9.5 and later, new transaction policy set settings will be available in the device editor only when the policy-management mode is in-device mode. By default, new transaction policy set settings can be created only in the Policy Manager and Object Manager.

---

**Table 231: Transaction Policy Set Configuration Details**

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a new transaction policy set.</td>
<td>1. Click <strong>Add new entry</strong> next to Gateway.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Sip</strong> next to gateway.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>New Transaction Policy Set</strong> next to Sip.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Add new entry</strong> next to New Transaction Policy Set.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Name</strong> box, enter the identifier for the new transaction policy set.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
</tbody>
</table>

| Define the new transaction policies.    | 1. Click **Policy Name** next to new-transaction-policy-set.                |
|                                        | 2. Click **Add new entry** next to Policy Name.                             |
|                                        | 3. In the **New policy-name** window, enter the names of one or more new transaction policies that you want to add to the set. Syntax: To specify a list of policies, enclose the policy names in brackets. |

---

**Configuring Timers (NSM Procedure)**

You can configure timers used to issue SIP timeouts using the Sip option:

To configure timers in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.

2. Click the **Device Tree** tab, and then double-click the device to select it.

3. Click the **Configuration** tab. In the configuration tree, expand **Services > Border Signaling Gateway**.
4. Select **Gateway**.

5. Add or modify settings as specified in Table 232 on page 407.

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

### Table 232: Timers Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure timers used to issue SIP timeouts.</td>
<td>1. Click <strong>Add new entry</strong> next to Gateway.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Sip</strong> next to gateway.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Timers</strong> next to Sip.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Inactive Call</strong> list, select the maximum time for signaling inactivity. Range: 300 through 86400</td>
</tr>
<tr>
<td></td>
<td>7. From the <strong>Timer C</strong> list, select the duration of the timeout period.    Range: 180 through 300</td>
</tr>
</tbody>
</table>

### Configuring Traceoptions (NSM Procedure)

You can configure border signaling gateway tracing operations using the Traceoptions option:

To configure traceoptions in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Services > Border Signaling Gateway**.
4. Select **Gateway**.
5. Add or modify settings as specified in Table 233 on page 408.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.
# Configure border signaling gateway (BSG) tracing operations

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Click <strong>Add new entry</strong> next to Gateway.</td>
<td></td>
</tr>
<tr>
<td>2. Click <strong>Traceoptions</strong> next to gateway.</td>
<td></td>
</tr>
<tr>
<td>3. Click <strong>Flag</strong> next to Traceoptions.</td>
<td></td>
</tr>
<tr>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
<td></td>
</tr>
<tr>
<td>5. From the <strong>Minimum</strong> list, select the severity of the event being traced.</td>
<td></td>
</tr>
<tr>
<td>- <strong>debug</strong>—Logging of all code flow of control.</td>
<td></td>
</tr>
<tr>
<td>- <strong>trace</strong>—Logging of program trace for START, and EXIT macros.</td>
<td></td>
</tr>
<tr>
<td>- <strong>info</strong>—Summary logs for normal operations. e.g. the policy decisions made for a call.</td>
<td></td>
</tr>
<tr>
<td>- <strong>warning</strong>—Failure-recovery or failure of an external entity.</td>
<td></td>
</tr>
<tr>
<td>- <strong>error</strong>—Failure with short-term effect, such as failed processing of a single call.</td>
<td></td>
</tr>
<tr>
<td>6. From the <strong>Session Trace</strong> list, select the minimum trace level for all session-trace messages.</td>
<td></td>
</tr>
</tbody>
</table>

# Configure trace level options for the datastore component of the BSG

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Click <strong>Add new entry</strong> next to Gateway.</td>
<td></td>
</tr>
<tr>
<td>2. Click <strong>Traceoptions</strong> next to gateway.</td>
<td></td>
</tr>
<tr>
<td>3. Click <strong>Flag</strong> next to Traceoptions.</td>
<td></td>
</tr>
<tr>
<td>4. Click <strong>Datastore</strong> next to Flag.</td>
<td></td>
</tr>
<tr>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
<td></td>
</tr>
<tr>
<td>6. From the <strong>Minimum</strong> list, select the minimum trace level for all datastore messages.</td>
<td></td>
</tr>
<tr>
<td>7. From the <strong>Data</strong> list, select the trace level for the data subcomponent.</td>
<td></td>
</tr>
<tr>
<td>8. From the <strong>Handle</strong> list, select the trace level for the access API for the database.</td>
<td></td>
</tr>
<tr>
<td>9. From the <strong>Db</strong> list, select the trace level for the wrapper layer around the database.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 233: Traceoption BSG Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure trace options for the BSG component that provides an infrastructure that enables incremental functionality implementation.</td>
<td>1. Click <strong>Add new entry</strong> next to Gateway.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Traceoptions</strong> next to gateway.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Flag</strong> next to Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Framework</strong> next to Flag.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Minimum</strong> list, select the minimum trace level for all framework messages.</td>
</tr>
<tr>
<td></td>
<td>7. From the <strong>Executor</strong> list, select the trace level for the framework subcomponent that executes configured actions for an event, handles any error states, delays processing, and so on.</td>
</tr>
<tr>
<td></td>
<td>8. From the <strong>Action</strong> list, select the trace level for the framework subcomponent that creates, initiates, and manipulates event actions.</td>
</tr>
<tr>
<td></td>
<td>9. From the <strong>Event</strong> list, select the trace level for the framework subcomponent that creates, modifies, and terminates event members.</td>
</tr>
<tr>
<td></td>
<td>10. From the <strong>Freezer</strong> list, select the trace level for the framework subcomponent that delays the execution of an event until certain conditions are met.</td>
</tr>
<tr>
<td></td>
<td>11. From the <strong>Memory Pool</strong> list, select the trace level for the framework subcomponent that creates, deletes, and manipulates memory pools and pool managers, and controls the check-in to and check-out from memory pools of memory objects.</td>
</tr>
</tbody>
</table>
Configure trace options for the Signaling Border Controller (SBC) utilities component of the BSG.

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Click <strong>Add new entry</strong> next to Gateway.</td>
<td></td>
</tr>
<tr>
<td>2. Click <strong>Traceoptions</strong> next to gateway.</td>
<td></td>
</tr>
<tr>
<td>3. Click <strong>Flag</strong> next to Traceoptions.</td>
<td></td>
</tr>
<tr>
<td>4. Click <strong>Sbc Util</strong>s next to Flag.</td>
<td></td>
</tr>
<tr>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
<td></td>
</tr>
<tr>
<td>6. From the <strong>Minimum</strong> list, select the minimum trace level for all sbc-util messages.</td>
<td></td>
</tr>
<tr>
<td>7. From the <strong>Configuration</strong> list, select the trace level for the configuration component of SBC utilities.</td>
<td></td>
</tr>
<tr>
<td>8. From the <strong>Ipc</strong> list, select the trace level for the IPC component of SBC utilities.</td>
<td></td>
</tr>
<tr>
<td>9. From the <strong>Device Monitor</strong> list, select the trace level for the device monitor component of SBC utilities.</td>
<td></td>
</tr>
<tr>
<td>10. From the <strong>Memory Management</strong> list, select the trace level for the memory management component of SBC utilities.</td>
<td></td>
</tr>
<tr>
<td>11. From the <strong>Message</strong> list, select the trace level for the message component of SBC utilities.</td>
<td></td>
</tr>
<tr>
<td>12. From the <strong>Common</strong> list, select the trace level for the common component of SBC utilities.</td>
<td></td>
</tr>
<tr>
<td>13. From the <strong>User Interface</strong> list, select the trace level for the user interface component of SBC utilities.</td>
<td></td>
</tr>
<tr>
<td>14. From the <strong>Memory Pool</strong> list, select the trace level for the message component of SBC utilities.</td>
<td></td>
</tr>
<tr>
<td>15. From the <strong>Memory Pool</strong> list, select the trace level for the memory pool component of SBC utilities.</td>
<td></td>
</tr>
</tbody>
</table>
Table 233: Traceoption BSG Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure trace options for the signaling component of the BSG.</td>
<td>1. Click <strong>Add new entry</strong> next to Gateway.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Traceoptions</strong> next to gateway.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Flag</strong> next to Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Signaling</strong> next to Flag.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Minimum</strong> list, select the minimum trace level for all signaling messages.</td>
</tr>
<tr>
<td></td>
<td>7. From the <strong>Sip Stack Wrapper</strong> list, select the trace options for the glue layer that receives events from the SIP stack and forwards them to the application and, conversely, receives events from the application and forwards them to the SIP stack.</td>
</tr>
<tr>
<td></td>
<td>8. From the <strong>b2b Wrapper</strong> list, select the trace options for entry and exit to the BSG signaling application.</td>
</tr>
<tr>
<td></td>
<td>9. From the <strong>Ua</strong> list, select the trace options for the signaling subcomponent that handles RECEIVE messages.</td>
</tr>
<tr>
<td></td>
<td>10. From the <strong>B2b</strong> list, select the trace options for the signaling component that implements the b2b logic (translating between dialogs, associating dialogs, creating new downstream dialogs, and so on).</td>
</tr>
<tr>
<td></td>
<td>11. From the <strong>Topology Hiding</strong> list, select the trace options for the signaling component that hides the network topology of a network by CONTACT replacement and removal or modification of certain headers.</td>
</tr>
<tr>
<td></td>
<td>12. From the <strong>Policy</strong> list, select the trace options for the signaling component that applies policies for call admission, routing decisions, security settings, and so on.</td>
</tr>
</tbody>
</table>
Table 233: Traceoption BSG Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set trace options for the SIP stack component of the BSG.</td>
<td>1. Click <strong>Add new entry</strong> next to Gateway. &lt;br&gt;2. Click <strong>Traceoptions</strong> next to gateway. &lt;br&gt;3. Click <strong>Flag</strong> next to Traceoptions. &lt;br&gt;4. Click <strong>Sip Stack</strong> next to Flag. &lt;br&gt;5. In the <strong>Comment</strong> box, enter the comment. &lt;br&gt;6. Select the <strong>Event Tracing</strong> check box to activate or deactivate the stack's event tracing. &lt;br&gt;7. Select the <strong>Event Tracing</strong> check box to activate or deactivate the stack's event tracing. &lt;br&gt;8. Select the <strong>Ips Tracing</strong> check box to activate or deactivate the stack's IPS tracing. &lt;br&gt;9. Select the <strong>Per Tracing</strong> check box to activate or deactivate the stack's performance tracing. &lt;br&gt;10. Select the <strong>Dev Logging</strong> check box to configure development tracing for the stack. &lt;br&gt;11. Select the <strong>Verbose Logging</strong> check box to configure verbose tracing for the stack. &lt;br&gt;12. From the <strong>Pd LogLevel</strong> list, select which types of PD logs are to be printed to the log file. Select one of the following: &lt;ul&gt;&lt;li&gt;<strong>problem</strong>—Problem log messages are sent to the log file. &lt;br&gt;<strong>exception</strong>—Exception and problem log messages are sent to the log file. &lt;/li&gt;&lt;/ul&gt;&lt;li&gt;<strong>audit</strong>—All log messages are sent to the log file. &lt;/li&gt;&lt;/ul&gt;13. From the <strong>Pd Log Detail</strong> list, select the amount of detail to be sent to the log file. Select one of the following: &lt;ul&gt;&lt;li&gt;<strong>full</strong>—All available information is sent to the log file. &lt;br&gt;<strong>summary</strong>—The type of logging, the identifier and the first line of the log message are sent to the log file. &lt;/li&gt;&lt;/ul</td>
</tr>
</tbody>
</table>

Configuring Class of Service (NSM Procedure)

The Class of Service (CoS) configuration available for the AS PIC enables you to configure Differentiated Services (DiffServ) code point (DSCP) marking and forwarding-class assignment for packets transiting the AS PIC.

To configure CoS in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > CoS**.
4. Add or modify the settings as specified in table Table 234 on page 413.
5. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.
Table 234: CoS Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define a CoS application profile.</td>
<td>1. Click Application profile next to CoS.</td>
</tr>
<tr>
<td></td>
<td>2. Click Add new entry next to Application Profile.</td>
</tr>
<tr>
<td></td>
<td>3. In the Name box, enter the profile name.</td>
</tr>
<tr>
<td></td>
<td>4. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. Expand application-profile.</td>
</tr>
<tr>
<td></td>
<td>6. Click Ftp next to application profile.</td>
</tr>
<tr>
<td></td>
<td>7. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>8. Expand Ftp.</td>
</tr>
<tr>
<td></td>
<td>9. Click Data next to Ftp.</td>
</tr>
<tr>
<td></td>
<td>10. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>11. In the Dscp box, enter the DSCP value or alias.</td>
</tr>
<tr>
<td></td>
<td>12. In the Forwarding Class box, enter the forwarding class.</td>
</tr>
<tr>
<td></td>
<td>13. Click Sip next to Ftp.</td>
</tr>
<tr>
<td></td>
<td>14. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>15. Expand Sip.</td>
</tr>
<tr>
<td></td>
<td>16. Click Video next to Sip.</td>
</tr>
<tr>
<td></td>
<td>17. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>18. In the Dscp box, enter the name assigned to a set of CoS markers.</td>
</tr>
<tr>
<td></td>
<td>19. In the Forwarding Class box, enter the name of the target application.</td>
</tr>
<tr>
<td></td>
<td>20. Click Voice next to Sip.</td>
</tr>
<tr>
<td></td>
<td>21. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>22. In the Dscp box, enter the DSCP mapping that is applied to the packets.</td>
</tr>
<tr>
<td></td>
<td>23. In the Forwarding Class box, enter the name of the target application.</td>
</tr>
</tbody>
</table>
Table 234: CoS Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify the rule the router uses when applying this service. | 1. Click **Rule** next to CoS.  
2. Click **Add new entry** next to rule.  
3. In the **Name** box, enter the rule the router uses when applying this service.  
4. In the **Comment** box, enter the comment.  
5. From the **Match Direction** list, select the direction in which the rule match is applied.  
   - **input**—Match on input to interface.  
   - **output**—Match on output from interface.  
   - **input–output**—Match on input to or output from interface.  
6. Expand **rule**.  
7. Click **Term** next to rule.  
8. Click **Add new entry** next to **Term**.  
9. In the **Name** box, enter the identifier for the term.  
10. In the **Comment** box, enter the comment.  
11. Expand **term**.  
12. Click **From** next to term.  
13. In the **Comment** box, enter the comment.  
14. Expand **From**.  
15. From the listed match conditions, select the ones that are applicable for CoS.  
   The match conditions listed are Application Sets, Applications, Destination Address, Destination Address Range, Destination Prefix List, Source Address, Source Address Range, and Source Prefix List.  
16. Expand **Then**.  
17. Click **Reflexive** next to Then.  
18. Select one of the following:  
   - **reflexive**—To apply the equivalent opposing CoS action to flows in the opposite direction.  
   - **reverse**—To define the CoS behavior for flows in the reverse direction.  
     a. In the **Comment** box, enter the comment.  
     b. In the **Dscp** box, enter the DSCP mapping that is applied to the packets.  
     c. In the **Forwarding Class**, enter the forwarding class to which packets are assigned  
     d. From the **Application Profile** list, select the identifier for the application profile.  
     e. Select the **Syslog** check box to enable system logging. |
Table 234: CoS Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify the rule set the router uses when applying this service. | 1. Click Rule-Set next to Cos.  
2. Click Add new entry next to Rule-Set.  
3. In the Name box, enter the identifier for the collection of rules that constitute this rule set.  
4. In the Comment box, enter the comment.  
5. Expand Rule-Set.  
6. Click Rule next to rule-set.  
7. Click Add new entry next to Rule.  
8. From the Name list, select the identifier for the collection of terms that constitute this rule.  
9. In the Comment box, enter the comment. |

Related Topics
- Configuring Service Interface Pools (NSM Procedure) on page 455
- Configuring a Service Set (NSM Procedure) on page 456

Configuring Intrusion Detection Service (NSM Procedure)

The Adaptive Services (AS) or Multiservices PIC supports a limited set of intrusion detection services (IDS) to perform attack detection. IDS enables you to focus attack detection and remedial actions on specific hosts or networks that you specify in the IDS terms. Signature detection is not supported.

To configure IDS in NSM:

1. In the navigation tree select Device Manager > Devices.
2. Click the Device tree tab and then double-click the device to select it.
3. In the Configuration tab, expand Services > Ids.
4. Add or modify the settings as specified in Table 235 on page 416.
5. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
### Table 235: IDS Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the rule the router uses when applying this service.</td>
<td>1. Click <strong>Rule</strong> next to Ids.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Rule.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the identifier for the collection of terms that constitute this rule.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. From the <strong>Match Direction</strong> list, select the direction in which the rule match is applied.</td>
</tr>
<tr>
<td></td>
<td>- <strong>input</strong>—To apply the rule match on input.</td>
</tr>
<tr>
<td></td>
<td>- <strong>output</strong>—To apply the rule match on output.</td>
</tr>
<tr>
<td></td>
<td>- <strong>input-output</strong>—To apply the rule match bidirectionally.</td>
</tr>
<tr>
<td></td>
<td>6. Expand rule.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>Term</strong> next to rule.</td>
</tr>
<tr>
<td></td>
<td>8. Click Add new entry next to Term.</td>
</tr>
<tr>
<td></td>
<td>9. In the <strong>Name</strong> box, enter the Identifier for the term.</td>
</tr>
<tr>
<td></td>
<td>10. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
</tbody>
</table>

| Specify input conditions for the IDS term.                           | 1. Expand **term**.                                                       |
|                                                                     | 2. Click **From** next to term.                                           |
|                                                                     | 3. In the **Comment** box, enter the comment.                             |
|                                                                     | 4. Expand **From**.                                                      |
|                                                                     | 5. From the listed match conditions, select the ones that are applicable for ids. |
|                                                                     | The match conditions listed are Application Sets, Applications, Destination Address, Destination Address Range, Destination Prefix List, Source Address, Source Address Range, and Source Prefix List. |

| Define the IDS term actions.                                        | 1. Click **Then** next to term.                                           |
|                                                                     | 2. In the **Comment** box, enter the comment.                             |
|                                                                     | 3. Expand **Then**.                                                      |
Table 235: IDS Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify the type of data to be aggregated. | 1. Click **Aggregation** next to Then.  
2. In the **Comment** box, enter the comment.  
3. From the **Source Prefix** list, select the prefix value for source IPv4 address aggregation.  
   Range: 1 through 32  
4. From the **Destination Prefix** list, select the prefix value for destination IPv4 address aggregation.  
   Range: 1 through 32  
5. From the **Source Prefix IPv6** list, select the prefix value for source IPv6 address aggregation.  
   Range: 1 through 128.  
6. From the **Destination Prefix IPv6** list, select the prefix value for destination IPv6 address aggregation.  
   Range: 1 through 128 |
| Specify handling of entries in the IDS events cache. | 1. Click **Force Entry** next to Then.  
2. Select one of the following:  
   - **force-entry**—To ensure that the entry has a permanent place in the IDS cache after one event is registered.  
   - **ignore-entry**—To ensure that all IDS events are ignored. |
| Set logging values for this IDS term. | 1. Click **Logging** next to Then.  
2. In the **Comment** box, enter the comment.  
3. From the **Threshold** list, select the logging threshold number of events per second.  
4. Select the **Syslog** check box to enable system logging. |
Table 235: IDS Configuration Details *(continued)*

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| **Configuring session limit.** | 1. Click **Session Limit** next to Then.  
2. In the **Comment** box, enter the comment.  
3. Expand **Session Limit**.  
4. Click **By Destination**, **By Source** or **By Pair** next to **Session Limit**.  
5. In the **Comment** box, enter the comment.  
6. In the **Maximum** box, enter the maximum number of open sessions per IP address or subnet per application.  
   Range: 1 through 32,767  
7. In the **Rate** box, enter the maximum number of sessions per second per IP address or subnet per application.  
   Range: 4 through 32,767  
8. In the **Packets** box, enter the maximum peak packets per second per application or IP address.  
   Range: 4 through 2147483647  
9. From the **Hold Time** list, select the length of time for which to stop all new flows once the rate of events exceeds the threshold set by one or more of the maximum, packets, or rate statements.  
   Range: 0 through 60 |
| **Enable SYN-cookie defenses against SYN attacks.** | 1. Click **Syn Cookie** next to Then.  
2. In the **Comment** box, enter the comment.  
3. From the **Threshold** list, select the SYN-cookie defense number of SYN attacks per second.  
4. From the **Mss** list, select the maximum segment size value used in TCP delayed binding.  
   Default: 1500  
   Range: 128 through 8192 |
| **Specify the rule set the router uses when applying this service.** | 1. Click **Rule Set** next to **Ids**.  
2. Click **Add new entry** next to **Rule Set**.  
3. In the **Name** box, enter the rule the router uses when applying this service.  
4. In the **Comment** box, enter the comment.  
5. Expand **rule-set**.  
6. Click **Rule** next to **rule-set**.  
7. Click **Add new entry** next to **Rule**.  
8. In the **Name** box, enter the rule the router uses when applying this service.  
9. In the **Comment** box, enter the comment. |
Tracing Services PIC Operations (NSM Procedure)

Tracing operations track all adaptive services operations and record them in a log file. The logged error descriptions provide detailed information to help you solve problems faster.

To configure tracing services PIC operations in NSM:

1. In the navigation tree select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. In the Configuration tab, expand Services.
4. Select Logging.
5. Add or modify the settings as specified in Table 236 on page 420.
6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
### Table 236: Traceoptions Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure Adaptive Services or Multiservices PIC tracing operations. | 1. Click **Traceoptions** next to **Logging**.  
2. In the **Comment** box, enter the comment.  
3. Select the **No Remote Trace** check box to disable remote tracing globally or for a specific tracing operation. |
| Specify the name of the file to receive the output of the tracing operation and specifies the maximum number of trace files. | 1. Click **File** next to **Traceoptions**.  
2. In the **Comment** box, enter the comment for the file.  
3. In the **Filename** box, enter the name of the file to receive the output of the tracing operation.  
4. In the **Size** box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).  
5. From the **Files** list, select the maximum number of trace files.  
Range: 2 through 1000  
Default: 3 files  
6. Select one of the following:  
• **world-readable**—To enable unrestricted file access.  
• **no-world-readable**—To restrict file access to owner. This is the default setting.  
7. In the **Match** box, enter the regular expression. |
| Specify the tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. | 1. Click **Flag** next to **Traceoptions**.  
2. Click **Add new entry** next to **Flag**.  
3. From the **Name** list, select the flag.  
4. In the **Comment** box, enter the comment for the flag. |

**Related Topics**
- Configuring Adaptive Services PICs (NSM Procedure) on page 391
- Configuring a Service Set (NSM Procedure) on page 456
- Configuring Service Interface Pools (NSM Procedure) on page 455

**Configuring Network Address Translation (NSM Procedure)**

Network Address Translation (NAT) is a mechanism for concealing a set of host addresses on a private network behind a pool of public addresses. It can be used as a security measure to protect the host addresses from direct targeting in network attacks.

To configure NAT in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Nat**.
4. Add or modify the settings as specified in Table 237 on page 422.
5. Click one:
• **OK**—To save the changes.

• **Cancel**—To cancel the modifications.
Table 237: NAT Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable multicast filters on Ethernet interfaces when IPv6 NAT is used for neighbor discovery.</td>
<td>1. Click <strong>Ipv6 Multicast Interfaces</strong> next to Nat.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Ipv6 Multicast Interfaces.</td>
</tr>
<tr>
<td></td>
<td>3. From the <strong>Name list</strong>, select <strong>All</strong> to enable filters on all interfaces.</td>
</tr>
<tr>
<td></td>
<td>4. Select <strong>Interface name</strong> to enable filters on a specific interface only.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. Select the <strong>Disable</strong> check box to disable filters on the specified interfaces.</td>
</tr>
</tbody>
</table>

Specify the NAT name and properties.                                                                 |
| 1. Click **Pool** next to Nat.                                                                 |
| 2. Click **Add new entry** next to Pool.                                                       |
| 3. In the **Name** box, enter the identifier for the Nat address pool.                        |
| 4. In the **Comment** box, enter the comment.                                                 |
| 5. Expand **pool**.                                                                           |
| 6. Click **Address** next to pool.                                                             |
| 7. Click **Add new entry** next to Address.                                                    |
| 8. In the **Name** box, enter an IPv4 or IPv6 prefix value.                                    |
| 9. In the **Comment** box, enter the comment.                                                 |

Configure the NAT pool address range.                                                              |
| 1. Click **Address Range** next to pool.                                                       |
| 2. Click **Add new entry** next to Address Range.                                              |
| 3. In the **Low** box, enter the lower boundary for the IPv4 or IPv6 address range.            |
| 4. In the **High** box, enter the upper boundary for the IPv4 or IPv6 address range.           |
| 5. In the **Comment** box, enter the comment.                                                   |
Table 237: NAT Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure Packet gateway Control Protocol (PGCP). | 1. Click **Pgcp** next to pool.  
2. In the **Comment** box, enter the comment.  
3. Click the **Remotely Controlled** check box to configure the addresses and ports in a NAT pool to be remotely controlled by the gateway controller.  
4. From the **Ports Per Session** list, select the number of ports to be enabled.  
NOTE: The ports per session should be either 2 or 4.  
5. Expand **Pgcp**.  
6. Click **Hint** next to **Pgcp**.  
7. Click **Add new entry** next to **Hint**.  
8. In the dialog box, enter an alphanumeric string of up to 3 characters that the BGF uses to match with a termination hint located in the Direction field of a nonstandard termination ID. |

| Configure addresses and ports for use in NAT Rules. | 1. Click **Port** next to pool.  
2. In the **Comment** box, enter the comment.  
3. Expand **Port**.  
4. Click **Automatic** next to **Port**.  
5. Select one of the following:  
  - **automatic**—To configure Router-assigned port.  
  - **range**—To specify a range with minimum and maximum values.  
    Range: 0 through 65535 |
### Table 237: NAT Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify the rule the router uses when applying this service. | 1. Click **Rule** next to Nat.  
2. Click **Add new entry** next to Rule.  
3. In the **Name** box, enter the identifier for the collection of terms that comprise this rule.  
4. In the **Comment** box, enter the comment.  
5. From the **Match Direction** list, select the direction in which the rule match is applied.  
6. Expand **Rule**.  
7. Click **Term** next to Rule.  
8. Click **Add new entry** next to Term.  
9. In the **Name** box, enter the identifier for the term.  
10. In the **Comment** box, enter the comment.  
11. Expand **term**.  
12. Click **From** next to term.  
13. In the **Comment** box, enter the comment.  
14. Expand **From**.  
15. From the listed match conditions, select the ones that are applicable for Nat.  
   The match conditions listed are Application Sets, Applications, Destination Address, Destination Address Range, Destination Prefix List, Source Address, Source Address Range, and Source Prefix List.  
16. Click **Then** next to From.  
17. Expand **Then**.  
18. In the **Comment** box, enter the comment.  
19. Select the **Syslog** check box to enable system logging.  
20. Click **No Translation** next to Then.  
21. Select one of the following:  
   - **no-translation**—To specify that traffic is not to be translated.  
   - **translated**—To define properties for translated traffic.
Table 237: NAT Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the rule set the router uses when applying this service.</td>
<td>1. Click <strong>Rule Set</strong> next to Nat.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Rule Set.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter an identifier for the collection of rules</td>
</tr>
<tr>
<td></td>
<td>that constitute this rule set.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. Expand <strong>rule-set</strong>.</td>
</tr>
<tr>
<td></td>
<td>6. Click <strong>Rule</strong> next to rule-set.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>Add new entry</strong> next to Rule.</td>
</tr>
<tr>
<td></td>
<td>8. From the <strong>Name</strong> list, select the identifier for the collection of</td>
</tr>
<tr>
<td></td>
<td>terms that comprise this rule.</td>
</tr>
<tr>
<td></td>
<td>9. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Configuring Adaptive Services PICs (NSM Procedure) on page 391
- Configuring Service Interface Pools (NSM Procedure) on page 455
- Configuring PGCP (NSM Procedure) on page 425

**Configuring PGCP (NSM Procedure)**

You can use the Packet Gateway Control Protocol (PGCP) options to configure the Border Gateway Function. See the following topics:

- Configuring Gateway (NSM Procedure) on page 426
- Configuring H248 Options Properties (NSM Procedure) on page 430
- Configuring H248 Properties (NSM Procedure) on page 436
- Configuring H248 Timers (NSM Procedure) on page 447
- Configuring the Monitor (NSM Procedure) on page 448
- Configuring Overload Control (NSM Procedure) on page 449
- Configuring Session Mirroring (NSM Procedure) on page 450
- Configuring Media Service (NSM Procedure) on page 450
- Configuring a Rule (NSM Procedure) on page 451
- Configuring Rule Set (NSM Procedure) on page 452
- Configuring Session Mirroring (NSM Procedure) on page 452
- Configuring Traceoptions (NSM Procedure) on page 453
- Configuring Virtual Interface (NSM Procedure) on page 454
Configuring Gateway (NSM Procedure)

You can configure a virtual Border gateway Function (BGF) on the router by configuring gateway. See the following topics:

- Configuring a Virtual Border Gateway Function on the Router (NSM Procedure) on page 426
- Configuring Data Inactivity Detection (NSM Procedure) on page 427
- Configuring Gateway Controller (NSM Procedure) on page 428
- Configuring Graceful Restart (NSM Procedure) on page 429

Configuring a Virtual Border Gateway Function on the Router (NSM Procedure)

You can configure a virtual BGF on the router using the Gateway option.

To configure a virtual BGF on the router in NSM:

1. In the navigation tree select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. In the Configuration tab, expand Services > Pgcp.
4. Select Gateway.
5. Add or modify the settings as specified in Table 238 on page 426.
6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.

Table 238: Virtual BGF Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure a virtual BGF on the router     | 1. In the Name box, enter the identifier of the virtual BGF.  
2. In the Comment box, enter the comment.  
3. In the Gateway Address box, enter the IP address of the virtual BGF that you are configuring on the router.  
4. From the Gateway Port list, select the port number of the virtual BGF that you are configuring on the router.  
Range: 0 through 65,535  
5. From the Cleanup Timeout list, select the interval before inactivity detection starts.  
Range: 0 through 65,535 seconds  
6. From the Service State list, select the service state of the virtual BGF.  
7. From the Max Concurrent Calls list, select the Maximum number of concurrent calls on the virtual BGF.  
Range: 0 through 10,000 |
Configuring Data Inactivity Detection (NSM Procedure)

You can configure data inactivity detection to detect latch deadlocks or other media inactivity on a gate.

To configure data inactivity detection on the router in NSM:

1. In the navigation tree select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. In the Configuration tab, expand Services > Pgcp.
4. Select Gateway.
5. Add or modify the settings as specified in Table 239 on page 428.
6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
Table 239: Data Inactivity Detection Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure data inactivity detection.</td>
<td>1. Expand Gateway.</td>
</tr>
<tr>
<td></td>
<td>2. Click Data Inactivity Detection next to Gateway.</td>
</tr>
<tr>
<td></td>
<td>3. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. From the Inactivity Delay list, select the time interval before checking for media inactivity.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 3600 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 5</td>
</tr>
<tr>
<td></td>
<td>5. From the Latch Deadlock delay list, select the time interval before checking for data packets.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 3600 seconds</td>
</tr>
<tr>
<td></td>
<td>6. Select the Send Notification on Delay check box to send an inactivity notification immediately when no media packets are detected during a delay period that precedes checking for media inactivity.</td>
</tr>
<tr>
<td></td>
<td>7. From the Inactivity Duration list, select the time during which no packets are received.</td>
</tr>
<tr>
<td></td>
<td>Range: 5 through 86400 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 30</td>
</tr>
<tr>
<td></td>
<td>8. Select the Stop Detection On Drop check box to configure the BGf to stop inactivity detection when a gate action is set to drop.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Change the service state of inactive terminations.</th>
<th>1. Expand Data Inactivity Detection.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Click Report Service Change next to Data Inactivity Detection.</td>
</tr>
<tr>
<td></td>
<td>3. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. From the Service Change Type list, select the method and reason used in changing the service state of the termination to active in order to curtail sending of inactivity messages.</td>
</tr>
<tr>
<td></td>
<td>• forced-906—If the service is to be terminated using a forced termination method with reason code 906 (loss of lower layer connectivity).</td>
</tr>
<tr>
<td></td>
<td>• forced-910—If the service is to be terminated using a forced termination with reason code 910 (media capability failure).</td>
</tr>
</tbody>
</table>

Configuring Gateway Controller (NSM Procedure)
You can configure a gateway controller either as a remote controller or as a local controller. Configure the gateway controller as a remote controller if you are using an external gateway controller and configure the gateway controller as a local controller if you are using a border signaling gateway (BSG).

To configure gateway controller in NSM:

1. In the navigation tree select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. In the Configuration tab, expand Services > Pgcp.
4. Select **Gateway**.

5. Add or modify the settings as specified in Table 240 on page 429.

6. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.

### Table 240: Gateway Controller Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure a gateway controller. | 1. Click **Add new entry** next to Gateway.  
| 2. Click **Gateway Controller** next to gateway.  
| 3. Click **Add new entry** next to Gateway Controller.  
| 4. In the **Name** box, enter the name of the gateway controller or BSG.  
| 5. In the **Comment** box, enter the comment.  
| 6. In the **Controller Address** box, enter the IP address of the gateway controller.  
| 7. From the **Controller Port** list, select the port number of the gateway controller.  
| | Range: 0 through 65535  
| 8. Expand **gateway-controller**.  
| 9. Click **Interim Ah Scheme**.  
| 10. In the **Comment** box, enter the comment.  
| 11. From the **Algorithm** list, select the algorithm used for the interim AH scheme.  
| | **HMAC null** is currently the only algorithm supported |

### Configuring Graceful Restart (NSM Procedure)

You can configure graceful restart properties that are used during synchronization between the pgcpd process and the Multiservices PIC or DPC.

To configure graceful restart in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in Table 241 on page 430.
6. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.
Table 241: Graceful Restart Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure graceful restart properties.</td>
<td>1. Click <strong>Add new entry</strong> next to Gateway.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Graceful Restart</strong> next to gateway.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. From the <strong>Maximum Synchronization Time</strong> list, select the maximum time allowed for the synchronization procedure with the PIC or DPC.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 300</td>
</tr>
<tr>
<td></td>
<td>5. From the <strong>Maximum Synchronization Mismatches</strong> list, select the maximum number of mismatches allowed during the synchronization procedure with the PIC or DPC.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 20000</td>
</tr>
<tr>
<td></td>
<td>6. Select the <strong>No Synchronization</strong> check box to disable the synchronization procedure with the PIC.</td>
</tr>
</tbody>
</table>

Configuring H248 Options Properties (NSM Procedure)

You can configure properties for the H.248 options. See the following topics:

- Configuring H248 Options (NSM Procedure) on page 430
- Changing Encoding Defaults (NSM Procedure) on page 431
- Configuring Service Change (NSM Procedure) on page 431

**Configuring H248 Options (NSM Procedure)**

You can configure options that affect virtual BGF H.248 behavior.

To configure H248 options in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in Table 242 on page 431.
6. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.
### Table 242: H248 Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure options that affect virtual BGF H.248 behavior.</td>
<td>1. Click <strong>Add new entry</strong> next to Gateway.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>H248 Options</strong> next to gateway.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. Select the <strong>Audit Observed Events Returns</strong> option to enable a history of media inactivity events to be viewed by the gateway controller.</td>
</tr>
</tbody>
</table>

### Changing Encoding Defaults (NSM Procedure)

You can change the encoding defaults using this option.

To configure encoding defaults in NSM:

1. In the navigation tree select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. In the Configuration tab, expand Services > Pgcp.
4. Select Gateway.
5. Add or modify the settings as specified in Table 243 on page 431.
6. Click one:
   - OK—To save the changes
   - Cancel—To cancel the modifications

### Table 243: Encoding Defaults Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change encoding defaults.</td>
<td>1. Click <strong>Add new entry</strong> next to Gateway.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>H248 Options</strong> next to gateway.</td>
</tr>
<tr>
<td></td>
<td>3. Expand <strong>H248 Options</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Encoding</strong> next to H248 Options.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. Select the <strong>No Dscp Bit Mirroring</strong> check box to disable mirroring of DSCP bits.</td>
</tr>
<tr>
<td></td>
<td>7. Select the <strong>Use Lower Case</strong> check box to configure upper-case encoding for H.248 messages.</td>
</tr>
</tbody>
</table>

### Configuring Service Change (NSM Procedure)

Service change specifies the method and reason that the virtual BGF includes in ServiceChange commands that it sends to the gateway controller when the state of a control association, virtual interface, or context changes. See the following topics:

- Configuring Context Indications (NSM Procedure) on page 432
- Configure Control Association Indications (NSM Procedure) on page 432
- Configuring Virtual Interface Indications (NSM Procedure) on page 435
Configuring Context Indications (NSM Procedure)
Context indications specify the method and reason that the virtual BGF includes in Service- Interruption ServiceChange commands that it sends to the gateway controller when the gates of a context no longer provide their configured services. When the virtual BGF sends a Service- Interruption message, both terminations in the context become Out-of-Service.

To configure context indications in NSM:

1. In the navigation tree select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. In the Configuration tab, expand Services > Pgcp.
4. Select Gateway.
5. Add or modify the settings as specified in Table 244 on page 432.
6. Click one:
   • OK—To save the changes.
   • Cancel—To cancel the modifications.

Table 244: Context indication Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure context indications.</td>
<td>1. Click Add new entry next to Gateway.</td>
</tr>
<tr>
<td></td>
<td>2. Click H248 Options next to gateway.</td>
</tr>
<tr>
<td></td>
<td>3. Expand H248 Options.</td>
</tr>
<tr>
<td></td>
<td>4. Click Service Change next to H248 Options.</td>
</tr>
<tr>
<td></td>
<td>5. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. Select the Use Wildcard Response check box to enable the virtual BGF to issue service change commands as wildcard-response commands, which trigger a short response from the gateway controller.</td>
</tr>
<tr>
<td></td>
<td>7. Expand Service Change.</td>
</tr>
<tr>
<td></td>
<td>8. Click Context Indications next to Service Change.</td>
</tr>
<tr>
<td></td>
<td>9. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>10. From the State Loss list, select the method and reason that the virtual BGF includes in Service- Interruption ServiceChange commands that it sends to the gateway controller after a state loss on a specific context.</td>
</tr>
</tbody>
</table>

Configure Control Association Indications (NSM Procedure)
Specify the method and reason that the virtual BGF includes in ServiceChange commands that it sends to the gateway controller when the state of the control association changes.

To configure control associations indications in NSM:

1. In the navigation tree select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services**.

4. Select **Pgcp**.

5. Add or modify the settings as specified in Table 245 on page 434.

6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
Table 245: Control Association Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify the method and reason that the virtual BGF includes in Registration Request ServiceChange commands when it attempts to reregister with the gateway controller or register with a new gateway controller after the control association is disconnected. | 1. Click **Add new entry** next to Gateway.  
2. Click **H248 Options** next to gateway.  
3. Expand **H248 Options**.  
4. Click **Service Change** next to H248 Options.  
5. Expand **Service Change**.  
6. Click **Control Association Indications** next to Service Change.  
7. In the **Comment** box, enter the comment.  
8. Expand **Control Association Indications**.  
9. Click **Disconnect** next to Control Association Indications.  
10. In the **Comment** box, enter the comment.  
11. From the **Reconnect** list, select the method and reason that the virtual BGF includes in Registration Request ServiceChange commands when it attempts to reregister with the gateway controller or register with a new gateway controller after the control association is disconnected.  
12. From the **Controller Failure** list, select the method and reason that the virtual BGF includes in Registration Request ServiceChange commands when it attempts to reregister with the gateway controller or register with a new gateway controller after the control association is disconnected. |

| Specify the method and reason that the virtual BGF includes in Unregistration Messages in ServiceChange commands that it sends to the gateway controller when a control association transitions to Out-of-Service because of a failure. | 1. Click **Down** next to Control Association.  
2. In the **Comment** box, enter the comment.  
3. From the **Administrative** list, select the method and reason that the virtual BGF includes in Unregistration Messages in ServiceChange commands that it sends to the gateway controller when a control association transitions to Out-of-Service because of an administrative operation.  
4. From the **Failure** list, select the method and reason that the virtual BGF includes in Unregistration or Notification Messages in ServiceChange commands when a control association transitions to Out-of-Service.  
5. From the **Graceful** list, select the method and reason that the virtual BGF includes in Notification ServiceChange commands that it sends to the gateway controller when the control association transitions from In-Service to Out-of-Service-Graceful. |
Table 245: Control Association Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify the method and reason that the virtual BGF includes in Notification Messages or Registration commands when a control association transitions to In-Service. | 1. Click **Up** next to Control Association.  
2. In the **Comment** box, enter the comment.  
3. From the **Failover Cold** list, select the method and reason that the virtual BGF includes in Registration ServiceChange commands when it attempts to register with a new gateway controller following a cold failover.  
4. From the **Failover Warm** list, select the method and reason that the virtual BGF includes in Registration ServiceChange commands when it attempts to register with a new gateway controller following a warm failover.  
5. From the **Cancel Graceful** list, select the method and reason that the virtual BGF includes in Notification ServiceChange commands that it sends to the gateway controller when the control association transitions from the Draining state to the Forwarding state. |

**Configuring Virtual Interface Indications (NSM Procedure)**

Virtual interface indications specify the method and reason that the virtual BGF includes in ServiceChange commands that it sends to the gateway controller when the state of the virtual interface changes.

To configure virtual interface indications in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in Table 246 on page 436.
6. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.
Table 246: Virtual Interface Indications Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify the method and reason that the virtual BGF includes in ServiceChange commands that it sends to the gateway controller when the state of the virtual interface changes to Out-of-Service. | 1. Click Add new entry next to Gateway.  
2. Click H248 Options next to gateway.  
3. Expand H248 Options.  
4. Click Service Change next to H248 Options.  
5. Expand Service Change.  
6. Click Virtual Interface Indications next to Service Change.  
7. In the Comment box, enter the comment.  
8. Expand Virtual Interface Indications.  
9. Click Virtual Interface Down next to Virtual Interface Indications.  
10. In the Comment box, enter the comment.  
11. From the Graceful list, select the method and reason that the virtual BGF includes in Notification ServiceChange commands that it sends to the gateway controller when the control association transitions from In-Service to Out-of-Service-Graceful.  
12. From the Administrative list, select the method and reason that the virtual BGF includes in Unregistration Messages in ServiceChange commands that it sends to the gateway controller when a control association transitions to Out-of-Service because of an administrative operation.  
13. From the Failure list, select the method and reason that the virtual BGF includes in Unregistration or Notification Messages in ServiceChange commands when a control association transitions to Out-of-Service.  
14. From the Link Loss list, select the method and reason that the virtual BGF includes in Service-Interruption ServiceChange commands that it sends to the gateway controller when the virtual interface transitions to Out-of-Service because of a link loss. |

| Specifying the ServiceChange command that the virtual BGF sends to the gateway controller when the state of the virtual interface changes to In-Service. | 1. Click Virtual Interface Up next to Virtual Interface Indications.  
2. In the Comment box, enter the comment.  
3. From the Warm list, select the method and reason that the virtual BGF includes in Service-Restoration ServiceChange commands that it sends to the gateway controller when a virtual interface transitions to In-Service.  
4. From the Cancel Graceful list, select the method and reason that the virtual BGF includes in Notification ServiceChange commands that it sends to the gateway controller when the control association transitions from the Draining state to the Forwarding state. |

Configuring H248 Properties (NSM Procedure)

You can configure default values for H248 properties using the following options. See the following topics:

- Configuring Application Data Inactivity Detection (NSM Procedure) on page 437
- Configuring Base Root (NSM Procedure) on page 437
Configuring Application Data Inactivity Detection (NSM Procedure)

You can activate or deactivate regulated notification of media inactivity events.

To configure application data inactivity detection in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in Table 247 on page 437.
6. Click one:
   - OK—To save the changes
   - Cancel—To cancel the modifications

### Table 247: Data Inactivity Detection Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Activate or deactivate regulated notification of media inactivity events. | 1. Click **Add new entry** next to Gateway.  
2. Click **H248 Properties** next to gateway.  
3. In the **Comment** box, enter the comment.  
4. Expand **H248 Properties**.  
5. Click **Application Data Inactivity Detection** next to H248 Properties.  
6. In the **Comment** box, enter the comment.  
7. From the **Ip Flow Stop Detection** list, select the regulated or non-regulated (immediate) notification of media inactivity events. |

Configuring Base Root (NSM Procedure)

You can configure default values for properties in the base root package using the Base Root option:

To configure base root package in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.

4. Select **Gateway**.

5. Add or modify the settings as specified in Table 248 on page 439.

6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
Table 248: Base Root Package Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Set default, maximum, and minimum values for the MG originated pending limit property of the base root package. | 1. Click **Add new entry** next to Gateway.  
2. Click **H248 Properties** next to gateway.  
3. Expand **H248 Properties**.  
4. Click **Base Root** next to H248 Properties.  
5. In the **Comment** box, enter the comment.  
6. Expand **Base Root**.  
7. Click **Mg Originated Pending Limit** next to Base Root.  
8. In the **Comment** box, enter the comment.  
9. From the **Default** list, select the default number of transaction pending messages that the gateway controller can receive from the virtual BGF.  
   Range: 1 through 512 |

| Set default, maximum, and minimum values for the MG provisional response timer property of the base root package. | 1. Click **Mg Provisional Response Value Timer** next to Base Root.  
2. In the **Comment** box, enter the comment.  
3. From the **Default** list, select the default time within which the gateway controller waits for a pending response from the virtual BGF if a transaction cannot be completed.  
   Range: 500 through 3000 milliseconds |

| Set default, maximum, and minimum values for the MGC originated pending limit property of the base root package. | 1. Click **Mgc Originated Pending Limit** next to Base Root.  
2. In the **Comment** box, enter the comment.  
3. From the **Default** list, select the default number of transaction pending messages that the virtual BGF can receive from the gateway controller.  
   Range: 1 through 512 |

| Set default, maximum, and minimum values for the MGC provisional response timer value property of the base root package. | 1. Click **Mgc Provisional Response Timer Value** next to Base Root.  
2. In the **Comment** box, enter the comment.  
3. From the **Default** list, select the default time within which the virtual BGF waits for a pending response from the gateway controller if a transaction cannot be completed.  
   Range: 500 through 3000 milliseconds |

| Set default, maximum, and minimum values for the normal MG execution time property of the base root package. | 1. Click **Normal Mg Execution Time** next to Base Root.  
2. In the **Comment** box, enter the comment.  
3. From the **Default** list, select the default interval within which the gateway controller waits for a response to transactions from the virtual BGF.  
   Range: 500 through 29000 milliseconds |
Table 248: Base Root Package Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Set default, maximum, and minimum values for the normal MGC execution time property of the base root package. | 1. Click **Normal Mgc Execution Time** next to Base Root.  
2. In the **Comment** box, enter the comment.  
3. From the **Default** list, select the default interval within which the virtual BGF waits for a response to transactions from the gateway controller. Range: 500 through 29,000 milliseconds. |

Configuring Differentiated Services (NSM Procedure)

You can configure default values for properties in the Differentiated Services (DiffServ) package using the DiffServ option.

To configure DiffServ in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in Table 249 on page 440.
6. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.

Table 249: Diffserv Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure default values for properties in the Differentiated Services (DiffServ) package. | 1. Click **Add new entry** next to Gateway.  
2. Click **H248 Properties** next to gateway.  
3. Expand **H248 Properties**.  
4. Click **Diffserv** next to H248 Properties.  
5. In the **Comment** box, enter the comment.  
6. Click **Dscp** next to Diffserv.  
7. In the **Comment** box, enter the comment.  
8. From the **Default** list, select the default values for Differentiated Services Code Point (DSCP) marking that the virtual BGF uses for outgoing traffic when the DSCP value is not already defined by the gateway controller. |
Configuring Event Timestamp Notification (NSM Procedure)

You can enable or disable the gateway controller to access timestamp information for media inactivity event notifications.

To configure event timestamp notification in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in Table 250 on page 441.
6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure event timestamp notification.</td>
<td>1. Click <strong>Add new entry</strong> next to Gateway.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>H248 Properties</strong> next to gateway.</td>
</tr>
<tr>
<td></td>
<td>3. Expand <strong>H248 Properties</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Event Timestamp Notification</strong> next to H248 Properties.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Request Timestamp</strong> list, select whether time stamp information is made available to the gateway controller or is suppressed.</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>requested</strong> to enable gateway controller access to time stamp information for notifications.</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>suppressed</strong> to disable gateway controller access to time stamp information for notifications.</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>autonomous</strong> which is equivalent to suppressed.</td>
</tr>
</tbody>
</table>

Hanging Termination Detection (NSM Procedure)

You can enable and configure hanging termination detection using this option.

To configure hanging termination detection in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in Table 251 on page 442.
6. Click one:
• OK—To save the changes.
• Cancel—To cancel the modifications.

Table 251: Hanging Termination Detection Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure hanging termination detection</td>
<td>1. Click Add new entry next to Gateway.</td>
</tr>
<tr>
<td></td>
<td>2. Click H248 Properties next to gateway.</td>
</tr>
<tr>
<td></td>
<td>4. Click Hanging Termination Detection next to H248 Properties.</td>
</tr>
<tr>
<td></td>
<td>5. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. From the Timerx list, select the number of seconds between the last message exchanged for this termination and when the BGF sends a notification to the gateway controller. Range: 0 through 2,147,480</td>
</tr>
</tbody>
</table>

Configuring Inactivity Timer (NSM Procedure)

You can configure the inactivity timer package, which allows the BGF to use message inactivity to detect that its active gateway controller has failed using this option.

To configure Inactivity Timer in NSM:

1. In the navigation tree select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. In the Configuration tab, expand Services > Pgcp.
4. Select Gateway.
5. Add or modify the settings as specified in Table 252 on page 443.
6. Click one:
   • OK—To save the changes.
   • Cancel—To cancel the modifications.
Configure the inactivity timeout event.

1. Click Add new entry next to Gateway.
2. Click H248 Properties next to gateway.
4. Click Inactivity Timer next to H248 Properties.
5. In the Comment box, enter the comment.
6. Expand Inactivity Timer.
7. Click Inactivity Timeout next to Inactivity Timer.
8. In the Comment box, enter the comment.
9. Select the Detect check box to specify the BGF detects inactivity timeout events received from the BGF by default.
10. Expand Inactivity Timeout.

Configure maximum inactivity time.

1. Click Maximum Inactivity Time next to Inactivity Timeout.
2. In the Comment box, enter the comment.
3. From the Default list, select the default value for the maximum inactivity time.
   Range: 100 through 65,535 (10-millisecond units)

Configuring Notification Behavior (NSM Procedure)

You can configure the default frequency for regulated media inactivity notifications sent by the BGF using the Notification Behavior option.

To configure notification behavior in NSM:

1. In the navigation tree select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. In the Configuration tab, expand Services > Pgcp.
4. Select Gateway.
5. Add or modify the settings as specified in Table 253 on page 444.
6. Click one:
   • OK—To save the changes.
   • Cancel—To cancel the modifications.
Table 253: Notification Behavior Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure the default frequency for sending media inactivity notifications for regulated events. | 1. Click **Add new entry** next to Gateway.  
2. Click **H248 Properties** next to gateway.  
3. Expand **H248 Properties**.  
4. Click **Notification Behavior** next to H248 properties.  
5. In the **Comment** box, enter the comment.  
6. Expand **Notification Behavior**.  
7. Click **Notification Regulation** next to Notification Behavior.  
8. In the **Comment** box, enter the comment.  
9. In the **Default** box, enter the default frequency for sending media inactivity notifications for regulated events. |

Configuring Segmentation (NSM Procedure)

You can configure default values for properties in the segmentation package using this option.

To configure segmentation in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in Table 254 on page 445.
6. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.
Table 254: Segmentation Package Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Set default, maximum, and minimum values for the MG maximum PDU size property of the segmentation package. | 1. Click **Add new entry** next to Gateway.  
2. Click **H248 Properties** next to gateway.  
3. Expand **H248 Properties**.  
4. Click **Segmentation** next to H248 properties.  
5. In the **Comment** box, enter the comment.  
6. Expand **Segmentation**.  
7. Click **Mg Maximum Pdu Size** next to Segmentation.  
8. In the **Comment** box, enter the comment.  
9. From the **Default** list, select the default maximum size of messages that the gateway controller sends to the BGF. Range: 512 through 65,507 bytes |
| Set default, maximum, and minimum values for the MG segmentation timer value property of the segmentation package. | 1. Click **Mg Segmentation Timer** next to Segmentation.  
2. In the **Comment** box, enter the comment.  
3. From the **Default** list, select the default time within which the gateway controller waits to receive outstanding message segments from the virtual BGF after it receives the SegmentationCompleteToken. Range: 500 through 30,000 milliseconds |
| Set default, minimum, and maximum values for the MGC maximum Protocol Data Unit (PDU) size property of the segmentation package. | 1. Click **Mgc Maximum Pdu Size** next to Segmentation.  
2. In the **Comment** box, enter the comment.  
3. From the **Default** list, select the default maximum size of messages that the virtual BGF sends to the gateway controller. Range: 512 through 65,507 bytes |

**Configuring Traffic Management (NSM Procedure)**

You can configure traffic management of the gate stream and the RTP Control Protocol (RTCP) stream. The parameters for the RTCP stream take effect only when the gate is an Real-time Transport Protocol (RTP)/RTCP gate.

To configure traffic management in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in Table 255 on page 446.
6. Click one:
   • OK—To save the changes.
   • Cancel—To cancel the modifications.

Table 255: Traffic Management Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure the maximum burst size for RTP/RTCP gate streams. | 1. Click **Add new entry** next to Gateway.  
2. Click **H248 Properties** next to gateway.  
3. Expand **H248 Properties**.  
4. Click **Traffic Management** next to H248 properties.  
5. In the **Comment** box, enter the comment.  
6. Click **Max Burst Size** next to Traffic Management.  
7. In the **Comment** box, enter the comment.  
8. From the **Default** list, select the default maximum burst size. Range: 20 through 2147483647 bytes  
9. Expand **Maximum Burst Size**.  
10. Click **Rtcp** next to Maximum Burst Size.  
11. In the **Comment** box, enter the comment.  
12. Expand **Rtcp**.  
13. Click **Percentage** next to Rtcp.  
14. Select one of the following:  
   • percentage—if the value entered is a percentage of the RTP gate's rate.  
   • fixed-value—if the value entered is a fixed number of bytes per second. Range: 20 through 2147483647 bytes-per-second |

| Configure the peak data rate for RTP/RTCP gate streams. | 1. Click **Peak Data Rate** next to Traffic Management.  
2. In the **Comment** box, enter the comment.  
3. From the **Default** list, select the default peak data rate. Range: 125 through 2147483647 bytes per second  
4. Expand **Peak Data Rate**.  
5. Click **Rtcp** next to Peak Data Rate.  
6. In the **Comment** box, enter the comment.  
7. Expand **Rtcp**.  
8. Click **Percentage** next to Rtcp.  
9. Select one of the following:  
   • percentage—if the value entered is a percentage of the RTP's gate rate.  
   • fixed-value—if the value entered is a fixed number of bits per second. Range: 0 through 2147483647 |
Table 255: Traffic Management Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the sustained data rate for streams of any protocol, including RTP.</td>
<td>1. Click Sustained Data Rate next to Traffic Management.</td>
</tr>
<tr>
<td></td>
<td>2. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. From the Default list, select the default value for sustained data rate.</td>
</tr>
<tr>
<td></td>
<td>Range: 125 through 4,294,967,295 bytes per second</td>
</tr>
<tr>
<td></td>
<td>4. Expand Sustained Data Rate.</td>
</tr>
<tr>
<td></td>
<td>5. Click Rtcp next to Sustained Data Rate.</td>
</tr>
<tr>
<td></td>
<td>6. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>7. Expand Rtcp.</td>
</tr>
<tr>
<td></td>
<td>8. Click Percentage next to Rtcp.</td>
</tr>
<tr>
<td></td>
<td>9. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• percentage—if the value entered is a percentage of the RTP's gate rate.</td>
</tr>
<tr>
<td></td>
<td>• fixed-value—if the value entered is a fixed number of bits per second.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 2147483647</td>
</tr>
</tbody>
</table>

Configuring H248 Timers (NSM Procedure)

You can configure H.248 timers for the PGCP connection using the H248 Timers option.

To configure H248 timers in NSM:

1. In the navigation tree select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. In the Configuration tab, expand Services > Pgcp.
4. Select Gateway.
5. Add or modify the settings as specified in Table 256 on page 448.
6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
Table 256: H248 Timers Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure H248 Timers.</td>
<td>1. Click Add new entry next to Gateway.</td>
</tr>
<tr>
<td></td>
<td>2. Click H248 Timers next to gateway.</td>
</tr>
<tr>
<td></td>
<td>3. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. From the Maximum Waiting Delay list, select the maximum time the virtual</td>
</tr>
<tr>
<td></td>
<td>BGF waits before contacting a new gateway controller when the connection to</td>
</tr>
<tr>
<td></td>
<td>the controlling gateway controller is lost.</td>
</tr>
<tr>
<td></td>
<td>Range: 100 through 300000 milliseconds</td>
</tr>
<tr>
<td></td>
<td>Default: 3000</td>
</tr>
<tr>
<td></td>
<td>5. From the Tmax Retransmission Delay list, select the duration of the delay</td>
</tr>
<tr>
<td></td>
<td>before the BGF considers the gateway controller to be down.</td>
</tr>
<tr>
<td></td>
<td>Range: 1000 through 60000 milliseconds</td>
</tr>
<tr>
<td></td>
<td>Default: 25000</td>
</tr>
<tr>
<td></td>
<td>6. From the Initial Average Ack Delay list, select the assumed initial</td>
</tr>
<tr>
<td></td>
<td>average delay.</td>
</tr>
<tr>
<td></td>
<td>Range: 500 through 4000 milliseconds</td>
</tr>
<tr>
<td></td>
<td>Default: 1000</td>
</tr>
<tr>
<td></td>
<td>7. From the Maximum Net Propagation Delay list, select the duration of the</td>
</tr>
<tr>
<td></td>
<td>maximum network propagation delay time.</td>
</tr>
<tr>
<td></td>
<td>Range: 500 through 100000 milliseconds</td>
</tr>
<tr>
<td></td>
<td>Default: 5000</td>
</tr>
</tbody>
</table>

Configuring the Monitor (NSM Procedure)

You can enable Real-Time Control Protocol (RTCP) and Real-Time Transport Protocol (RTP) application-level gateways (ALGs) for media flows and monitor packets using the Monitor option.

To configure the monitor in NSM:

1. In the navigation tree select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. In the Configuration tab, expand Services > Pgcp.
4. Select Gateway.
5. Add or modify the settings as specified in Table 257 on page 449.
6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
Table 257: Monitor Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure the monitor.        | 1. Click **Add new entry** next to Gateway.  
|                               | 2. Click **Monitor** next to gateway.       
|                               | 3. In the **Comment** box, enter the comment. |
|                               | 4. Expand **Monitor**.                      |
|                               | 5. Click **Media** next to Monitor.         |
|                               | 6. In the **Comment** box, enter the comment. |
|                               | 7. Select the **Rtp** check box to enable Real-Time Transport Protocol (RTP) application-level gateway (ALG) on media flows created when the gateway controller installs media gates on the virtual BGF. |
|                               | 8. Select the **Rtcp** check box to enable Real-Time Control Protocol (RTCP) application-level gateway (ALG) on media flows created when the gateway controller installs media gates on the virtual BGF. |

Configuring Overload Control (NSM Procedure)

You can configure the BGF to send overload messages to the gateway controller based on the status of its work queue. The overload messages cause the gateway controller to lower the rate at which it admits packets for processing.

To configure overload control in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in Table 258 on page 449.
6. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.

Table 258: Overload Control Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure the BGF to send overload messages. | 1. Click **Add new entry** next to Gateway.  
|                               | 2. Click **Overload Control** next to gateway.       |
|                               | 3. In the **Comment** box, enter the comment.       |
|                               | 4. From the **Queue Limit Percentage** list, select the percentage of the overload control work queue in use that triggers creation of an overload notification. |
|                               | Range: 1 through 100 |
Configuring Session Mirroring (NSM Procedure)

You can configure the session mirroring feature using the Session Mirroring option.

To configure session mirroring in NSM:

1. In the navigation tree select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. In the Configuration tab, expand Services > Pgcp.
4. Select Gateway.
5. Add or modify the settings as specified in Table 259 on page 450.
6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure the delivery function that receives the session mirroring information. | 1. Click Add new entry next to Gateway.  
2. Click Session Mirroring next to gateway.  
3. In the Comment box, enter the comment.  
4. Select the Disable Session Mirroring check box to disable the session mirroring feature.  
5. Expand Session Mirroring.  
6. Click Delivery Function next to Session Mirroring.  
7. Click Add new entry next to Delivery Function.  
8. In the New delivery-function window, enter the name of the delivery function that receives the session mirroring information. |

Configuring Media Service (NSM Procedure)

You can configure media services for the Border gateway Function (BGF) configuration. Media services are applied to Packet Gateway Control Protocol (PGCP) packets.

To configure media service in NSM:

1. In the navigation tree select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. In the Configuration tab, expand Services > Pgcp.
4. Select Media Service.
5. Add or modify the settings as specified in Table 260 on page 451.
6. Click one:
   - OK—To save the changes.
• Cancel—To cancel the modifications.

Table 260: Media Service Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure media service. | 1. Click **Add new entry** next to Media Service.  
2. In the **Name** box, enter the identifier for the media service name.  
3. In the **Comment** box, enter the comment.  
4. In the **Nat Pool** box, enter the identifier for the NAT address pool. |

Configuring a Rule (NSM Procedure)

You can specify the rule that the router uses when it applies the media service.

To configure a rule in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Rule**.
5. Add or modify the settings as specified in Table 261 on page 451.
6. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.

Table 261: Configuring Rule

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure a rule.     | 1. Click **Add new entry** next to Rule.  
2. In the **Name** box, enter the identifier for the rule.  
3. In the **Comment** box, enter the comment.  
4. From the **Gateway** list, select the identifier of the virtual BGF.  
5. Expand rule.  
6. Click **Media Service** next to rule.  
7. Click **Add new entry** next to Media Service.  
8. In the **New media-service** window, enter the identifier for the media service name. |
Configuring Rule Set (NSM Procedure)

You can specify the rule set the router uses when applying this service.

To configure Rule Set in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Rule Set**.
5. Add or modify the settings as specified in Table 262 on page 452.
6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.

Table 262: Configuring Rule Set

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure a rule set. | 1. Click **Add new entry** next to Rule Set.  
2. In the **Name** box, enter the identifier for the collection of rules that make up this rule set.  
3. In the **Comment** box, enter the comment.  
4. Expand **rule-set**.  
5. Click **Rule** next to rule-set.  
6. Click **Add new entry** next to Rule.  
7. From the **Name** list, select the identifier for the rule.  
8. In the **Comment** box, enter the comment. |

Configuring Session Mirroring (NSM Procedure)

You can configure the session mirroring feature using the session mirroring option.

To configure session mirroring in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Session Mirroring**.
5. Add or modify the settings as specified in Table 263 on page 453.
6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
Table 263: Session Mirroring Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure session mirroring. | 1. In the Comment box, enter the comment.  
| | 2. Select the Disable Session Mirroring check box to disable session mirroring on the BGF.  
| | 3. Expand Session Mirroring.  
| | 4. Click Delivery Function next to Session Mirroring.  
| | 5. Click Add new entry next to Delivery Function.  
| | 6. In the Name box, enter the name of the delivery function that receives the session mirroring information.  
| | 7. In the Comment box, enter the comment.  
| | 8. In the Destination Address box, enter the address of the server to which the BGF sends session-mirroring information.  
| | 9. From the Destination Port list, select the port on the delivery function server that receives session-mirroring information. Range: 0 through 65535  
| | 10. In the Network Operator Id box, enter the network operator ID. The ID can be up to five characters.  
| | 11. In the Source Address box, enter the address of the interface on which the BGF sends session-mirroring data to the delivery function.  
| | 12. From the Source Port list, select the port on which the BGF sends session-mirroring data to the delivery function. Range: 0 through 65,535  
| | 14. Click Memory Management next to delivery-function.  
| | 15. In the Comment box, enter the comment.  
| | 16. From the Operational Mode list, select the operational mode.

Configuring Traceoptions (NSM Procedure)

You can configure Packet Gateway Control Protocol (PGCP) trace options using the traceoptions option.

To configure traceoptions in NSM:

1. In the navigation tree select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. In the Configuration tab, expand Services > Pgcp.
4. Select Traceoptions.
5. Add or modify the settings as specified in Table 264 on page 454.
6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
Configure PGCP trace options.

1. In the Comment box, enter the comment.
2. Select the No Remote Trace check box to disable remote tracing.
3. Expand Traceoptions.
4. Click File next to Traceoptions.
5. In the Comment box, enter the comment.
6. In the Filename box, enter the name of the file to which the tracing messages are written.
7. In the Size box, enter the size parameter (in bytes) to trigger rotation of files.
8. From the Files list, select the number of trace files.
9. Select one of the following:
   • world-readable—To allow all users to use the log file.
   • no-world-readable—To disallow all users from using the log file.
10. In the Match box, enter the regular expression.
11. Click Flag next to Traceoptions.
12. Click Add new entry next to Flag.
13. In the Comment box, enter the comment.

Configuring Virtual Interface (NSM Procedure)

You can configure a virtual interface for the BGF using the Virtual Interface option.

To configure virtual interface in NSM:

1. In the navigation tree select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. In the Configuration tab, expand Services > Pgc.
4. Select Virtual Interface.
5. Add or modify the settings as specified in Table 265 on page 455.
6. Click one:
   • OK—To save the changes.
   • Cancel—To cancel the modifications.
Table 265: Virtual Interface Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a virtual interface</td>
<td>1. Click <strong>Add new entry</strong> next to Virtual Interface.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Name</strong> box, enter the identifier number for the interface.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 1023</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. From the <strong>Service State</strong> list, select the service state of the virtual</td>
</tr>
<tr>
<td></td>
<td>interface.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Interface</strong> box, enter the interface name.</td>
</tr>
<tr>
<td></td>
<td>6. Expand <strong>virtual-interface</strong>.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>Media Service</strong> next to virtual-interface.</td>
</tr>
<tr>
<td></td>
<td>8. Click <strong>Add new entry</strong> next to Media Service.</td>
</tr>
<tr>
<td></td>
<td>9. In the dialog box, enter the identifier for the media service name.</td>
</tr>
<tr>
<td></td>
<td>10. Click <strong>Routing Instance</strong> next to virtual-interface.</td>
</tr>
<tr>
<td></td>
<td>11. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>12. From the <strong>Routing Instance Name</strong> list, select the name of a routing</td>
</tr>
<tr>
<td></td>
<td>instance.</td>
</tr>
<tr>
<td></td>
<td>13. In the <strong>Service Interface</strong> box, enter the name and logical interface</td>
</tr>
<tr>
<td></td>
<td>number of the service Interface in <strong>interface-name.unit-number</strong> form.</td>
</tr>
</tbody>
</table>

Configuring Service Interface Pools (NSM Procedure)

You can configure service interface pools used for Virtual Private Network (VPN) aggregation using the Service Interface Pools option. Up to 1000 logical interfaces can be configured in a service interface pool. All interfaces in a pool must belong to the same service PIC or DPC. All interfaces assigned to the same service must be in the same pool.

To configure service interface pools in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services**.
4. Select **Service Interface Pools**.
5. Add or modify the settings as specified in Table 266 on page 456.
6. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.
Table 266: Service Interface Pools Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure a service interface pool for VPN aggregation for the BGF feature. | 1. In the Comment box, enter the comment.  
2. Expand Service Interface Pools.  
3. Click Pool next to Service Interface Pools.  
4. Click Add new entry next to Pool.  
5. In the Name box, enter the name of the service interface pool.  
6. In the Comment box, enter the comment.  
7. Click Interface next to pool.  
8. Click Add new entry next to interface.  
9. In the Name box, enter the name and logical unit number of the service interface.  
10. In the Comment box, enter the comment. |

Related Topics
- Configuring a Service Set (NSM Procedure) on page 456
- Configuring Stateful Firewall (NSM Procedure) on page 460

Configuring a Service Set (NSM Procedure)

A service set is a collection of services to be performed by an Adaptive Services (AS) or Multiservices PIC.

To configure a service set in NSM:

1. In the navigation tree select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. In the Configuration tab, expand Services.
4. Select Service Set.
5. Add or modify the settings as specified in Table 267 on page 457.
6. Click one:
   - OK—Save the changes.
   - Cancel—Cancel the modifications.
### Table 267: Service Set Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define the service set.</td>
<td>1. Click <strong>Add new entry</strong> next to Service Set.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Name</strong> box, enter the name that identifies the service set.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Max Flows</strong> box, enter the maximum number of flows.</td>
</tr>
<tr>
<td></td>
<td>5. From the <strong>Tcp Mss</strong> list, select the TCP Maximum Segment Size (MSS) allowed for the service set.</td>
</tr>
<tr>
<td></td>
<td>Range: 536 to 65535</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Application Identification Profile</strong> list, select the application identification method.</td>
</tr>
<tr>
<td></td>
<td>7. From the <strong>Idp Profile</strong> list, select the Idp profile.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: The IDP profile is a list of IDP policies as defined in the Security &gt; Idp &gt; Idp policy assigned to this device.</td>
</tr>
</tbody>
</table>

**Configuring AACL rule and AACL rule set.**

|                                           | 1. Click **Aacl Rules** next to service-set.                                                          |
|                                           | 2. Select one of the following:                                                                      |
|                                           |   - **aacl-rules**—To specify the rule the router uses when applying this service.                  |
|                                           |   - **aacl-rule-set**—To specify the rule set the router uses when applying this service.           |
|                                           | 3. Click **Add new entry**.                                                                          |
|                                           | 4. From the **Name** list, select the identifier for the collection of terms that constitute this rule set. |
|                                           | 5. In the **Comment** box, enter the comment.                                                        |

**Allow multicast traffic to be sent to the Adaptive Services or Multiservices PIC.**

|                                           | 1. Click **Allow Multicast** next to service-set.                                                     |
|                                           | 2. In the **Comment** box, enter the comment.                                                        |

**Specify the Class of Service (CoS) service rule or rule set included in this service.**

|                                           | 1. Click **Cos Rules** next to service-set.                                                          |
|                                           | 2. Select one of the following:                                                                      |
|                                           |   - **cos-rules**—To specify cos-rules.                                                             |
|                                           |   - **cos-rule-set**—To specify cos-rules set.                                                       |
|                                           | 3. Click **Add new entry**.                                                                         |
|                                           | 4. From the **Name** list, select the rule or rule set name.                                         |

**Define JUNOS SDK service set.**

|                                           | 1. Click **Extension Service** next to service-set.                                                  |
|                                           | 2. Click **Add new entry** next to Extension Service.                                                |
|                                           | 3. In the **Name** box, enter the identifier for a provider-specific service.                       |
|                                           | 4. In the **Comment** box, enter the comment.                                                        |
Table 267: Service Set Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify the intrusion detection service (IDS) rules or rule set included in this service set. | 1. Click **Ids Rules** next to service-set.  
2. Select one of the following:  
   - **ids—rules**—To specify the ids rules.  
   - **ids-rule-sets**—To specify the ids-rule-sets.  
3. Click **Add new entry**.  
4. From the **Name** list, select the rule or rule set name. |
| Specify the device name for the interface service PIC. | 1. Click **Interface Service** next to service-set.  
2. Select one of the following:  
   - **interface-service**—To specify the device name for the interface service Physical Interface Card.  
     a. In the **Comment** box, enter the comment.  
     b. In the **Services Interface** box, enter the name of the service device associated with the interface-wide service set.  
   - **next-hop-service**—To specify interface names or a service interface pool for the forwarding next-hop service set. You cannot specify both a service interface pool and an inside or outside interface.  
     a. In the **Comment** box, enter the comment.  
     b. In the **Inside Service Interface** box, enter the name and logical unit number of the service interface associated with the service set applied inside the network.  
     c. In the **Outside Service Interface** box, enter the name and logical unit number of the service interface associated with the service set applied outside the network  
     d. From the **Service Interface Pool** list, select the name of the pool of logical interfaces. |
| Specify the Network Address Translation (NAT) rules or rule set included in this service set. | 1. Click **Nat Rules** next to service-set.  
2. Select one of the following:  
   - **nat-rules**—To specify the NAT rules included in this service set.  
   - **nat-rule-sets**—To specify the NAT rule set included in this service set.  
3. Click **Add new entry**.  
4. From the **Name** list, select the rule or rule set name.  
5. In the **Comment** box, enter the comment. |
Table 267: Service Set Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify the Packet Gateway Control Protocol (PGCP) rules or rule set included in this service set. | 1. Click **Pgcp Rules** next to service-set.  
2. Select one of the following:  
• **pgcp-rules**—To specify the pgcp rules included in this service set.  
• **pgcp-rule-set**—To specify the pgcp rule set included in this service set.  
3. Click **Add new entry**.  
4. From the **Name** list, select the rule or rule set name.  
5. In the **Comment** box, enter the comment. |
| Configuring the policy decision statistics profile. | 1. Click **Policy Decision Statistics Profile** next to service-set.  
2. In the **Comment** box, enter the comment.  
3. From the **Profile Name** list, select the policy decision statistics profile. |
| Define the order in which services are applied for this service set. | 1. Click **Service Order** next to service-set.  
2. In the **Comment** box, enter the comment.  
3. Click **Forward Flow** next to Service Order.  
4. Click **Add new entry** next to Forward Flow.  
5. In the **New forward-flow** window, enter the service order for forward flow.  
6. Click **Reverse Flow** next to Service Order.  
7. Click **Add new entry** next to Reverse Flow.  
8. In the **New reverse-flow** window, enter the service order for reverse flow. |
| Specify the stateful firewall rules or rule set included in this service set. | 1. Click **Stateful Firewall Rules** next to service-set.  
2. Select one of the following:  
• **stateful-firewall-rules**—To specify the stateful firewall rules.  
• **stateful-firewall-rule-sets**—To specify the stateful firewall rule set.  
3. Click **Add new entry**.  
4. From the **Name** list, select the rule or rule set name.  
5. In the **Comment** box, enter the comment. |
### Related Topics
- Configuring Service Interface Pools (NSM Procedure) on page 455
- Configuring Stateful Firewall (NSM Procedure) on page 460
- Configuring Intrusion Detection Service (NSM Procedure) on page 415

### Configuring Stateful Firewall (NSM Procedure)

Stateful firewall is a type of firewall filter that considers state information derived from previous communications and other applications when evaluating traffic. Contrasted with a stateless firewall that inspects packets in isolation, a stateful firewall provides an extra layer of security by using state information derived from past communications and other applications to make dynamic control decisions for new communication attempts.

To configure stateful firewall in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Stateful Firewall**.
4. Add or modify the settings as specified in Table 268 on page 461.
5. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.

---

**Table 267: Service Set Configuration Details (continued)**

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure generation of system log messages for the service set. | 1. Click **Syslog** next to service-set.  
2. In the **Comment** box, enter the comment.  
3. Click **Host** next to Syslog.  
4. Click **Add new entry** next to Host.  
5. In the **Name** box, enter the name of the system logging utility host machine.  
6. In the **Comment** box, enter the comment.  
7. From the **Facility Override** list, select the name of the facility that overrides the default assignment.  
8. In the **Log Prefix** box, enter the system logging prefix value.  
9. Click **Contents** next to host.  
10. From the **Name** list, select the service set.  
11. In the **Comment** box, enter the comment.  
12. From the **Any** list, select the system logging severity level. |
### Table 268: Stateful Firewall Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| **Define the rule.**        | 1. Click **Rule** next to Stateful Firewall.  
2. Click **Add new entry** next to Rule.  
3. In the **Name** box, enter the identifier for the collection of terms that constitute this rule.  
4. In the **Comment** box, enter the comment.  
5. From the **Match Direction** list, select the direction in which the rule match is applied.  
   - Select **input** to apply the rule match on the input side of the interface.  
   - Select **output** to apply the rule match on the output side of the interface.  
   - Select **input-output** to apply the rule match bidirectionally.  |
| **Define a term.**          | 1. Click **Term** next to rule.  
2. Click **Add new entry** next to Term.  
3. In the **Name** box, enter the identifier for the term.  
4. In the **Comment** box, enter the comment.  
5. Expand **term**.  
6. Click **From** next to term.  
7. In the **Comment** box, enter the comment.  
8. Expand **From**.  
9. From the listed match conditions, select the match condition for stateful firewall.  
   - The match conditions listed are Application Sets, Applications, Destination Address, Destination Address Range, Destination Prefix List, Source Address, Source Address Range, and Source Prefix List.  
10. Click **Then** next to term.  
11. In the **Comment** box, enter the comment.  
12. Select the **Syslog** check box to enable system logging.  
13. Expand **Then**.  
14. Click **Accept** next to Then.  
   - Select **Accept** to accept the traffic and send it on to its destination.  
   - Select **discard** to not accept traffic or process it further.  
   - Select **reject** to accept the traffic and return a rejection message.  |
| **Define Ip option.**       | 1. Click **Allow Ip Options** next to Then.  
2. Click **Add new entry** next to Allow Ip Options.  
3. From the dropdown list, select the IP option name. |
### Table 268: Stateful Firewall Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define the rule set.</td>
<td>1. Click <strong>Rule Set</strong> next to Stateful Firewall.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Rule Set.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the identifier for the collection of rules</td>
</tr>
<tr>
<td></td>
<td>that constitute this rule set.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Rule</strong> next to rule-set.</td>
</tr>
<tr>
<td></td>
<td>6. Click <strong>Add new entry</strong> next to Rule.</td>
</tr>
<tr>
<td></td>
<td>7. From the <strong>Name</strong> list, select the identifier for the collection of</td>
</tr>
<tr>
<td></td>
<td>terms that constitute this rule.</td>
</tr>
<tr>
<td></td>
<td>8. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Configuring Service Interface Pools (NSM Procedure) on page 455
- Configuring a Service Set (NSM Procedure) on page 456
CHAPTER 24

Configuring SNMP

- Configuring Basic System Identification for SNMP (NSM Procedure) on page 463
- Configuring SNMP Communities (NSM Procedure) on page 464
- Configuring SNMP Trap Groups (NSM Procedure) on page 466
- Configuring SNMP Views (NSM Procedure) on page 467

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 269 on page 463.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 269: 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>
<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>
</tbody>
</table>
Table 269: Basic System Identification Details (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snmp &gt; Engine Id</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use Mac Address</td>
<td>Sets the engine ID to use the MAC address.</td>
<td>Select this option.</td>
</tr>
</tbody>
</table>

Related Topics

- Configuring SNMP Communities (NSM Procedure) on page 464
- Configuring SNMP Trap Groups (NSM Procedure) on page 466
- Configuring SNMP Views (NSM Procedure) on page 467

Configuring SNMP Communities (NSM Procedure)

You can configure an SNMP community to authorize access to the SNMP server by SNMP clients, based on the source IP address of incoming SNMP request packets. A community also defines which MIB objects are available and the operations (read-only or read-write) allowed on those objects. The SNMP client application specifies an SNMP community name in Get, GetNext, GetBulk, and Set SNMP requests. If a community is not configured, all SNMP requests are denied.

To configure SNMP communities in NSM:

1. In the navigation tree, select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. Click the Configuration tab.
4. In the configuration tree, expand SNMP.
5. Select Community.
6. Click the Add or Edit icon.
7. Enter the parameters as specified in Table 270 on page 465.
8. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
   - Apply—To apply the SNMP settings.

NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the Updating Devices section in the Network and Security Manager Administration Guide for more information.
### Table 270: Configuring Community 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 community.</td>
<td>Enter a name for the community.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for the community.</td>
<td>Enter a comment.</td>
</tr>
<tr>
<td>View</td>
<td>Specifies the view associated with the community.</td>
<td>Enter a name for the view.</td>
</tr>
</tbody>
</table>
| Authorization  | Specifies the type of access granted to the community. Access is authorized for SNMP Get, GetBulk, GetNext, and Set requests. | Select an access type for the community:  
  - None—No requests are enabled.  
  - read-only—Enable Get, GetNext, and GetBulk requests. This option is enabled by default.  
  - read-write—Enable all requests, including Set requests.  
  You must configure a view to enable Set requests. |
| Client List Name| Specifies a client list or prefix list to be assigned to an SNMP community.| 1. Expand the Community tree and select Client List Name.                
  2. Select a name. |
| Routing Instance| Specifies a routing instance for a community.                           | 1. Expand the Community tree and select Routing Instance.                    
  2. Click the New button or select an entry and click the Edit button. 
  3. Configure the following to create and define a routing instance:  
    - Name—Enter a name for the routing instance.  
    - Comment—Enter a comment for the routing instance.  
  NOTE: On routers, to configure a routing instance within a logical system, specify the logical system name followed by the routing instance name. Use a slash (/) to separate the two names. To configure the default routing instance on a logical system, specify the logical system name followed by “default.” |

**Related Topics**  
- Configuring Client Lists (NSM Procedure)
Configuring SNMP Trap Groups (NSM Procedure)

You can create and name a group of one or more types of SNMP traps and then define which systems receive the group of SNMP traps. The trap group must be configured for SNMP traps to be sent. The trap group name can be any string and is embedded in the community name field of the trap. To configure your own trap group port, use the Destination Port option. The default destination port is port 162. For each trap group that you define, specify:

- At least one system as the recipient of the SNMP traps in the trap group
- The types of traps the trap group can receive
- Routing instance used by the trap group

To configure trap groups in NSM:

1. In the navigation tree, select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. Click the Configuration tab.
4. In the configuration tree, expand SNMP.
5. Select Trap Group.
6. Select the Enable Feature check box.
7. Enter the parameters as specified in Table 271 on page 466.
8. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
   - Apply—To apply the SNMP settings.

Table 271: Configuring SNMP Trap Group Fields

<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 the SNMP trap group.</td>
<td>Select the version number for the SNMP trap group from the list.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Specifies the SNMP trap group port number.</td>
<td>Enter a trap group 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>
Table 271: Configuring SNMP Trap Group Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Categories | Defines the types of traps that are sent to the targets of the named trap group. | 1. Expand the **trap-group** tree and select **Categories**.  
2. Select the trap type.  
**NOTE:** If you do not configure categories, all trap types are included in trap notifications.  
3. On routers, choose an Otn Alarm and a Sonet Alarm for your trap category. |

| Targets   | Specifies the IPv4 or IPv6 address of the systems to receive traps.         | 1. Expand the **trap-group** tree and select **Targets**.  
2. Click the New button or select an OID and click the Edit button.  
3. Enter the IPv4 or IPv6 addresses of the system (do not enter hostnames). |

**Related Topics**
- Configuring Basic System Identification for SNMP (NSM Procedure) on page 463
- Configuring SNMP Communities (NSM Procedure) on page 464
- Configuring SNMP Views (NSM Procedure) on page 467

**Configuring SNMP Views (NSM Procedure)**

By default, an SNMP community grants read access and denies write access to all supported MIB objects, including communities configured for read-write authorization. To restrict or grant read or write access to a set of MIB objects, configure a MIB view and associate the view with a community. Each MIB object of a view has a common object identifier (OID) prefix. Each OID represents a subtree of the MIB object hierarchy. The subtree can be represented either by a sequence of integers separated by periods (such as 1.3.6.1.2.1.2) or by its subtree name (such as interfaces). Use a view to specify a group of MIB objects on which to define access. You can also use the wildcard character asterisk (*) to include OIDs that match a particular pattern in the SNMP view. To enable a view, associate it with a community.

To configure SNMP views in NSM:

1. In the navigation tree, select **Device Manager** > **Devices**.  
2. In the **Devices** list, double-click the device to select it.  
3. Click the **Configuration** tab.  
4. In the configuration tree, expand **SNMP**.  
5. Select **View**.
6. Select the **Enable Feature** check box.

7. Enter the parameters as specified in Table 272 on page 468.

8. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.
   - **Apply**—To apply the SNMP settings.

### Table 272: Configuring SNMP View Fields

<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>
<tr>
<td>Oid</td>
<td>Specifies an OID used to represent a subtree of MIB objects.</td>
<td>1. Expand the <strong>View</strong> tree and select <strong>oid</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the New button or select an OID and click the Edit button.</td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the MiB for the view.</td>
<td>Enter the OID of the MiB in either dotted-integer format or subtree-name format.</td>
</tr>
<tr>
<td>Include or Exclude</td>
<td>Specifies whether the view includes or excludes the set of MIB objects.</td>
<td>Select <strong>exclude</strong> to exclude the subtree of MIB objects represented by the specified OID. Select <strong>include</strong> to include the subtree of MIB objects represented by the specified OID.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Configuring Basic System Identification for SNMP (NSM Procedure) on page 463
- Configuring SNMP Communities (NSM Procedure) on page 464
- Configuring SNMP Trap Groups (NSM Procedure) on page 466
PART 4

Managing M-series and MX-series Devices

- Managing M-series and MX-series Devices Overview on page 471
- Viewing the M-series and MX-series Device Inventory in NSM and the CLI on page 473
- Topology Manager on page 479
Managing M-series and MX-series Devices

Overview

- Managing M-series and MX-series Device Software Versions on page 471

Managing M-series and MX-series Device Software Versions

You can use Network and Security Manager (NSM) to upgrade or adjust the software on managed M-series and MX-series devices running JUNOS Release 9.3 or later.

When a software upgrade is applied to an M-series or MX-series device with dual Routing Engines, the upgraded software is applied to both Routing Engines. The backup is upgraded first. The router then reboots and the backup becomes the master. Then the former master is upgraded, as is the standard procedure for upgrading M-series and MX-series devices with dual Routing Engines.

For more information and steps about updating the device software version, see “Upgrading the Device Software” in the Network and Security Manager Administration Guide.

Related Topics
- Viewing and Reconciling Device Inventory on page 473
- Comparing Device Inventory in NSM and the CLI on page 474
CHAPTER 26

Viewing the M-series and MX-series Device Inventory in NSM and the CLI

- Viewing and Reconciling Device Inventory on page 473
- Comparing Device Inventory in NSM and the CLI on page 474

Viewing and Reconciling Device Inventory

Device inventory management in Network and Security Manager (NSM) allows you to display information about the hardware, software, and license components of each device. It also provides features to update the NSM database with the most current inventory information from the device. In addition, you can use Device Monitor, Device List, and the device tooltip to view the status of inventory synchronization.

These inventory management features are available for all M-series and MX-series devices. You can use these features to make the NSM database match the device inventory, but you cannot write new inventory information to the device.

Initially, the device inventory in the NSM database is generated when the device is first imported into NSM. Immediately after import, the device inventory in the NSM database matches exactly the inventory on the device itself.

If the hardware on the device is changed, the software is upgraded through the WebUI or CLI, new software packages are installed, and then the inventory on the device is no longer synchronized with the NSM database.

The Device Monitor, Device List, and tooltip shows the hardware and software inventory status for each device. Possible states include:

- In Sync—Inventory in the NSM database matches the device.
- Out of Sync—Inventory in the NSM database does not match the device.
- N/A—Either the device is not yet connected and managed by NSM, or the device is a ScreenOS security device or IDP sensor.

Changes to the device inventory are not automatically updated in the NSM database.
For detailed information about comparing and reconciling device inventory, see the *Network and Security Manager Administration Guide*.

**Related Topics**
- Managing M-series and MX-series Device Software Versions on page 471
- Comparing Device Inventory in NSM and the CLI on page 474

### Comparing Device Inventory in NSM and the CLI

NSM and the JUNOS command-line interface (CLI) display similar information about the device inventory, although screens rendered in NSM look different than the JUNOS CLI. This topic provides an introduction to viewing software and hardware inventory using NSM and compares the NSM view with the CLI output for the same device.

- Viewing Device Inventory in NSM on page 474
- Viewing Device Inventory from the CLI on page 476

#### Viewing Device Inventory in NSM

**Purpose**

NSM displays the hardware and software inventory for each device according to the information it has in its database. For a device with dual Routing Engines, NSM collects the inventory data from the master Routing Engine.

To view the device inventory, the device must be in the Managed state.

**Action**

To view the device inventory, follow these steps:

1. In the navigation tree, select **Device Manager > Devices**.
2. Right-click the device whose inventory you want to view.
3. Select **View/Reconcile Inventory**.

   The Device Inventory window opens, similar to the example shown in Figure 7 on page 474.

**Figure 7: The Device Inventory Window**
4. Select the **Hardware** tab to display information about hardware modules in the device, including the I/O module, the Routing Engine, and so on. (See Figure 8 on page 475.)

Figure 8: Viewing the Hardware Inventory

5. Select the **Software** tab to display information about the software packages installed in the device, including the installed OS and its version, and any other installed packages. (See Figure 9 on page 475.)

Figure 9: Viewing the Software Inventory

---

**NOTE:** The License tab not supported for M-series or MX-series devices.
Viewing Device Inventory from the CLI

Purpose  The information displayed in the Device Inventory window, as shown in “Viewing Device Inventory in NSM” on page 474 can also be viewed from the device (router) using the CLI operational mode. Generally, the hardware and software information displayed in the Device Inventory window and the CLI command output is similar.

Action  To view device hardware and software inventory, from the device enter the following JUNOS CLI operational mode commands:

    show chassis hardware
    show version

Sample Output  The following sample output shows hardware and software inventory for the same router used in “Viewing Device Inventory in NSM” on page 474.

    user@host> show chassis hardware
    Hardware inventory:
    Item                        Version     Part number       Serial number     Description
    Chassis                                39097             M10i
    Midplane         REV 04   710-008920   CM0805            M10i Midplane
    Power Supply 0   Rev 06   740-008537   5384103           AC Power Supply
    Power Supply 1   Rev 06   740-008537   5384265           AC Power Supply
    HCM 0            REV 03   710-010580   CM1272            M10i HCM
    HCM 1            REV 03   710-010580   CM1187            M10i HCM
    Routing Engine 0 REV 09   740-009459   1000602468        RE-5.0
    CFEB 0           REV 09   750-010465   DK6820            Internet Processor II
    FPC 0                                                    E-FPC
    PIC 0          REV 10   750-002971   CL0219            4x OC-3 SONET, MM
    PIC 1          REV 11   750-002992   CM4540            4x F/E, 100 BASE-TX
    PIC 2          REV 08   750-005724   CL9082            2x OC-3 ATM-II IQ, MM
    PIC 3          REV 08   750-005724   CL9078            2x OC-3 ATM-II IQ, MM
    FPC 1                                                    E-FPC
    PIC 2          REV 12   750-008425   CG1204            Adaptive Services
    PIC 3          REV 12   750-012838   DJ0049            4x 1GE(LAN), IQ2
    Xcvr 0       REV 01   740-013111   7303532           SFP-T
    Xcvr 1       REV 01   740-013111   7314215           SFP-T
    Xcvr 2       REV 01   740-013111   7303398           SFP-T
    Xcvr 3       REV 01   740-013111   7303376           SFP-T
    Fan Tray 1                                               Rear Right Fan Tray

    user@host> show version
    Hostname: host
    Model: m10i
    JUNOS Base OS boot [9.3B2.7]
    JUNOS Base OS Software Suite [9.3B2.7]
    JUNOS Kernel Software Suite [9.3B2.7]
    JUNOS Crypto Software Suite [9.3B2.7]
    JUNOS Packet Forwarding Engine Support (M/T Common) [9.3B2.7]
    JUNOS Packet Forwarding Engine Support (M7i/M10i) [9.3B2.7]
    JUNOS Online Documentation [9.3B2.7]
    JUNOS Routing Software Suite [9.3B2.7]

Meaning  The sample output for the show chassis hardware command shows the hardware installed on the M10i device. The row of output showing the midplane is in bold to illustrate that the midplane information in this example is identical to the midplane information in the NSM UI example.
The sample output for the `show version` command shows the version of JUNOS software installed on the M10i device. In this instance, the CLI output provides more information than is provided by the NSM UI.

**Related Topics**
- Managing M-series and MX-series Device Software Versions on page 471
- Viewing and Reconciling Device Inventory on page 473
CHAPTER 27

Topology Manager

- Overview of the NSM Topology Manager on page 479
- Requisites for a Topology Discovery on page 479
- About the NSM Topology Manager Toolbar on page 480

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 on page 479
- About the NSM Topology Manager Toolbar on page 480

Requisites for a Topology Discovery

To use the Topology Manager, first add one or more EX-series switches to the Device Manager in NSM. You can then use an added device as a seed device in initiating a topology discovery.

Alternatively, if there are no devices added or managed in NSM, you can initiate a topology discovery by configuring preferred subnets. All the IP addresses in the included subnets range are discovered. Therefore, you need to have either seed devices and/or preferred subnets to initiate topology discovery. You also need:

1. The management IP address of the EX-series switch that acts as the seed IP address
2. SNMP credentials:
   - For SNMPv1 and SNMPv2c: Community string
For SNMPv3: Username, security level, authentication type, privacy type, privacy password, and authentication password

3. Enabled Layer 2 protocols like LLDP, STP, RSTP in the switched network, because network discovery depends on these as well as on the Address Forwarding Table information.

For more information about the Topology Manager, see the Network and Security Manager Administration Guide.

Related Topics
- Overview of the NSM Topology Manager on page 479
- About the NSM Topology Manager Toolbar on page 480

About the NSM Topology Manager Toolbar

You can use the Topology Manager toolbar to perform the following actions:

- **Zoom in and Zoom out**: Use these tools to view the network topology according to the detail required. These tools are only of use in the map view.

- **Save to file**: Use this tool to save the network topology map as an image file and the devices and links tables as text files from their respective views.

- **Print**: From different views, you can use this tool to print a network topology map as an image file and the devices and links tables as text files.

- **Manage Devices**: Use this tool to select one or more devices from a topology map and manage them in NSM. This tool is applicable only to map views and not the different table views. To add a device:
  a. Click the **Manage Devices** icon. A dialog box opens.
  b. Enter the SSH user name and password.
  c. Click **OK**.

- **Set Preferences**: Use this tool to set preferences according to which the discovery engine can perform a topology discovery. You can set preferences for default SNMP credentials, topology discovery intervals, and subnets to be included or excluded.

- **Start and Stop Topology Discovery**: Use these tools to initiate and stop a topology discovery based on the set of seed devices and credentials specified in the topology preferences.

- **Search**: You can search for a device, end-point device, link, or port in any of the table views by providing a string in the search text box. NSM performs a substring match against all attributes of the particular view and displays the results in the same table. If you navigate to another tab, your search results are lost. You can save the search output in a text file as comma-separated values.

The Topology Manager status bar at the bottom of the screen indicates the timestamp of the last completed topology discovery and whether a discovery is in progress.
For more information about the Topology Manager, see the Network and Security Manager Administration Guide.

**Related Topics**
- Overview of the NSM Topology Manager on page 479
- Requisites for a Topology Discovery on page 479
PART 5

Monitoring M-series and MX-series Devices

- Real Time Monitoring of M-series and MX-series on page 485
CHAPTER 28

Real Time Monitoring of M-series and MX-series

About the Realtime Monitor

The Realtime Monitor module in Network and Security Manager (NSM) enables you to monitor real-time status and statistics about all the managed devices in your network at a glance. Features of Realtime Monitor enabled for M-series and MX-series include viewing device status, viewing monitor alarm status, and setting the polling interval for device alarm status. You can use the Realtime Monitor to identify problems and discover trends across multiple geographic regions and functional areas from a central management location.

The Realtime Monitor can also help you quickly identify potential device, network, and system-level problems, such as:

- Configuration status—At the device level, you can monitor the changing status of one or more security devices in real time.
- Connection status—At the network level, you can monitor problems that could lead to failed devices.

The Realtime Monitor does the work of a management expert by first gathering information about specific processes and network activity, then color-coding each event to organize problems.

Related Topics

- Viewing Device Status on page 486
- Viewing Device Monitor Alarm Status on page 488
- Setting the Polling Interval For Device Alarm Status on page 489
Viewing Device Status

Table 273 on page 486 lists and describes device information that you can view through the Device Monitor.

Table 273: 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>
<tr>
<td>Config Status</td>
<td>Current configuration status of the device in NSM:</td>
</tr>
<tr>
<td></td>
<td>• None—No state has been set (does not show in Device Monitor).</td>
</tr>
<tr>
<td></td>
<td>• Modeled—The device exists in NSM, but a connection to the device has not yet been established.</td>
</tr>
<tr>
<td></td>
<td>• RMA—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></td>
<td>• Waiting for 1st connect—NSM is waiting for the device to connect. You must enter a command on the device to make it connect to NSM.</td>
</tr>
<tr>
<td></td>
<td>• Import Needed—You must import the configuration of the device into NSM. When you add a device for the first time, verify that your status indicates “Import Needed” before you attempt to import the device. During migration, this state indicates that import of the security device configuration is still required.</td>
</tr>
<tr>
<td></td>
<td>• OS Version Adjustment Needed—The firmware version detected running on the device is different than what was previously detected in NSM. This could happen in the event that the automatic adjustment option was cleared during a change device firmware directive or an Update Device directive was issued to an IDP device with a firmware version mismatch.</td>
</tr>
<tr>
<td></td>
<td>• Platform Mismatch—The device platform selected when adding the DMI device in NSM does not match the device itself. A device in this state cannot connect to NSM.</td>
</tr>
<tr>
<td></td>
<td>• Device Firmware Mismatch—The OS version selected when adding a DMI device does not match the OS version running on the device itself.</td>
</tr>
<tr>
<td></td>
<td>• Device Type Mismatch—The type of device specified when adding the device in NSM does not match the device itself. The device type might indicate whether the device is part of a vsys device, part of a cluster, or part of a virtual chassis. A device in this state cannot connect to NSM.</td>
</tr>
<tr>
<td></td>
<td>• Detected duplicate serial number—The device has the same sequence number as another managed device. A device in this state cannot connect to NSM.</td>
</tr>
<tr>
<td></td>
<td>• Update Needed—An update to this device is required.</td>
</tr>
<tr>
<td></td>
<td>• Managed—The device is currently being managed by NSM.</td>
</tr>
<tr>
<td></td>
<td>• Managed, In Sync—The physical device configuration is synced with the modeled configuration in NSM.</td>
</tr>
</tbody>
</table>
Table 273: Device Status Information (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
</table>
| Config Status (continued) | - Managed, Device Changed—The physical device configuration is out of sync with the modeled configuration in NSM. Changes were made to the physical device configuration (the configuration on the physical device is newer than the modeled configuration).
  For M-series and MX-series devices with redundant Routing Engines, this status can indicate that a routing engine switchover has occurred.
  - Managed, NSM Changed—The modeled device configuration is out of sync with the physical device configuration. Changes were made to the modeled configuration (the configuration on the NSM is newer than the physical device configuration).
  - Managed, NSM and Device Changed—Both device configurations (physical and modeled) are out of sync with each other. Changes were made to the physical device configuration and to the modeled configuration.
  - Managed, Sync Pending—Completion of the Update Device directive is suspended and waiting for the device to reconnect. This state occurs only for ScreenOS devices that have the Update When Device Connects option selected during the device update. |
| Connection Status | Connection status of the device in NSM:
  - Up—Device is currently connected to NSM.
  - Down—Device is not currently connected to NSM but has connected in the past.
  - Never Connected—Device has never connected to NSM.
    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.
    NOTE: If the network connection goes down for a period longer than six to eight minutes, the device connection will permanently time out. If this occurs and the device goes down for any reason, the device still appears as Up in the Device Monitor. |
| Alarm | Displays the current alarm status for each device in NSM:
  - If device has any alarms, the most severe alarm severity is displayed (either Major or Minor).
  - None—The device has no alarms.
  - Unknown—The device status is unknown. For example, the device might not be connected.
  - N/A—The device’s alarm is not pollable or discoverable, for example, this column shows “N/A” for ScreenOS and IDP devices.
    Alarm is colored:
    - Red for Major.
    - Orange for Minor.
    - Green for Ignore, None, Unknown, or N/A. |
### Table 273: Device Status Information (continued)

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

**Related Topics**  
- About the Realtime Monitor on page 485  
- Viewing Device Monitor Alarm Status on page 488  
- Setting the Polling Interval For Device Alarm Status on page 489

### Viewing Device Monitor Alarm Status

**Purpose**  
Alarms refresh automatically through periodic polling.

**Action**  
To view the Alarm status and time:

1. From Device Monitor, right-click the device row entry and select the View Alarm option.  
   The device Alarm Status dialog box displays the alarm list and polling time for the device.
2. To retrieve the current alarm status in the device, click the **Refresh** button.

The poll time is derived from the device server time.

**Related Topics**
- About the Realtime Monitor on page 485
- Viewing Device Status on page 486
- Setting the Polling Interval For Device Alarm Status on page 489

### Setting the Polling Interval For Device Alarm Status

The default polling interval is 900 seconds (15 minutes). To configure polling intervals for Alarm Status:

1. From **Device Manager > Devices**, double-click the device to open it.
   
   The Info tab dialog box is displayed.

2. Select the **Device Admin** page to set the polling interval for the device.
   
   The minimum polling interval is 60 seconds. The maximum interval is 2,147,483,647 seconds. You cannot disable polling.

**Related Topics**
- About the Realtime Monitor on page 485
- Viewing Device Status on page 486
- Viewing Device Monitor Alarm Status on page 488
PART 6

Index

• Index on page 493
Index

A
access address pools, configuring..........................50
access profile, configuring.................................70
access profiles, L2TP
  AAA subscriber management
    RADIUS parameters, configuring..................63
  access profile, configuring..........................55
accounting order, configuring..........................56
accounting parameters, configuring......................55
authentication order, configuring.........................57
authorization order, configuring..........................57
client filter name, configuring............................59
configuring..................................................54
L2TP client, configuring...................................58
LDAP options, configuring..................................60
LDAP server, configuring...................................61
provisioning order, configuring...........................62
RADIUS parameters, configuring...........................66
session limit, configuring..................................67
subscriber access management
  RADIUS, configuring......................................67
accounting options
  class usage profile, configuring.......................71
  filter profile, configuring..............................73
  interface profile, configuring...........................74
  log file, configuring.......................................72
  MIB profile, configuring..................................76
policy decision statistics profile,
  configuring................................................75
routing engine profile, configuring.......................77
accounting options, configuring.........................71
adaptive services PICs, configuring......................391
address assignment pools, configuring....................47
address family, specifying..................................193
aggregated devices, configuring...........................97
alarm status
  setting polling intervals..................................489
  viewing.....................................................488
API...........................................................................12
application, application set
  configuring......................................................79
authentication key updates, configuring...............389
B
BGP
  configuring.....................................................252
border signaling gateways, configuring...............392
bridge domain
  forwarding options, configuring.......................84
  IGMP snooping, configuring.............................89
  layer 2 learning, forwarding, configuring...........82
  logical interfaces, configuring........................85
  multicast snooping options, configuring..............86
  VLAN ID, configuring......................................94
bridge domain, configuring................................81
bridge domains properties
  configuring..................................................81
C
chassis alarms, configuring.............................98
chassis FPC, configuring................................100
classifiers
  CoS...............................................................122
  CLI
    about..........................................................7
  code point aliases..........................................124
  communities
    configuring.................................................464
  confederation
    configuring................................................362
  configuring, access group profile......................51
  container interfaces, configuring......................99
  CoS classifiers................................................122
  CoS code point aliases.....................................124
  CoS drop profiles..........................................125
  CoS forwarding classes....................................127
  CoS forwarding policy, configuring.....................129
  CoS fragmentation maps, configuring..................130
  CoS host outbound traffic, configuring..............131
  CoS interfaces..............................................132
<table>
<thead>
<tr>
<th>Category</th>
<th>Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoS routing instances</td>
<td>configuring 138</td>
</tr>
<tr>
<td>CoS scheduler maps</td>
<td>configuring 141</td>
</tr>
<tr>
<td>CoS schedulers</td>
<td>configuring 139</td>
</tr>
<tr>
<td>CoS tracing operations</td>
<td>configuring 143</td>
</tr>
<tr>
<td>CoS traffic control profiles</td>
<td>configuring 144</td>
</tr>
<tr>
<td>CoS translation table</td>
<td>configuring 145</td>
</tr>
<tr>
<td>customer support</td>
<td>contacting JTAC xxx</td>
</tr>
<tr>
<td>D</td>
<td>data model, defined 11</td>
</tr>
<tr>
<td>device</td>
<td>status 16</td>
</tr>
<tr>
<td>device configuration</td>
<td>about 41</td>
</tr>
<tr>
<td>device groups</td>
<td>modeling 26</td>
</tr>
<tr>
<td>device groups</td>
<td>planning for 27</td>
</tr>
<tr>
<td>device groups</td>
<td>using 27</td>
</tr>
<tr>
<td>device inventory</td>
<td>reconciling 473</td>
</tr>
<tr>
<td>device inventory</td>
<td>viewing 473</td>
</tr>
<tr>
<td>Device Monitor</td>
<td>alarm status 488</td>
</tr>
<tr>
<td>device status information</td>
<td>486</td>
</tr>
<tr>
<td>device schemas</td>
<td>about 12</td>
</tr>
<tr>
<td>devices</td>
<td>adding multiple with discovery rules 27</td>
</tr>
<tr>
<td>devices</td>
<td>importing with dynamic IP address 16</td>
</tr>
<tr>
<td>devices</td>
<td>managed 23</td>
</tr>
<tr>
<td>devices</td>
<td>modeling 26</td>
</tr>
<tr>
<td>DHCP agent</td>
<td>authentication support, configuring 185</td>
</tr>
<tr>
<td>DHCP agent</td>
<td>default configuration settings, overriding 187</td>
</tr>
<tr>
<td>DHCP agent</td>
<td>group, configuring 186</td>
</tr>
<tr>
<td>DHCP agent</td>
<td>name of a group, configuring 191</td>
</tr>
<tr>
<td>DHCP agent</td>
<td>operations, configuring 192</td>
</tr>
<tr>
<td>DHCP agent, configuring</td>
<td>relay option 60, configuring 189</td>
</tr>
<tr>
<td>DHCP agent, configuring</td>
<td>relay option 82, configuring 190</td>
</tr>
<tr>
<td>DMI</td>
<td>See distributed data collection</td>
</tr>
<tr>
<td>drop profiles</td>
<td>configuring 125</td>
</tr>
<tr>
<td>dynamic tunnels</td>
<td>configuring 363</td>
</tr>
<tr>
<td>E</td>
<td>edit routing-options command 18</td>
</tr>
<tr>
<td>E</td>
<td>event policy tracing, configuring 157</td>
</tr>
<tr>
<td>E</td>
<td>event policy, configuring 154</td>
</tr>
<tr>
<td>E</td>
<td>event script, configuring 152</td>
</tr>
<tr>
<td>F</td>
<td>fate sharing</td>
</tr>
<tr>
<td>F</td>
<td>configuring 364</td>
</tr>
<tr>
<td>F</td>
<td>firewall filter</td>
</tr>
<tr>
<td>F</td>
<td>any family type, configuring 159</td>
</tr>
<tr>
<td>F</td>
<td>bridge family type, configuring 161</td>
</tr>
<tr>
<td>F</td>
<td>ccc family type, configuring 163</td>
</tr>
<tr>
<td>F</td>
<td>inet family type, configuring 165</td>
</tr>
<tr>
<td>F</td>
<td>inet6 family type, configuring 170</td>
</tr>
<tr>
<td>F</td>
<td>mpls family type, configuring 174</td>
</tr>
<tr>
<td>F</td>
<td>policer 180</td>
</tr>
<tr>
<td>F</td>
<td>VPLS family type, configuring 177</td>
</tr>
<tr>
<td>G</td>
<td>flow</td>
</tr>
<tr>
<td>G</td>
<td>configuring 366</td>
</tr>
<tr>
<td>G</td>
<td>forwarding</td>
</tr>
<tr>
<td>G</td>
<td>accounting options, configuring 183</td>
</tr>
<tr>
<td>G</td>
<td>forwarding classes 127</td>
</tr>
<tr>
<td>G</td>
<td>forwarding table</td>
</tr>
<tr>
<td>G</td>
<td>configuring 368</td>
</tr>
<tr>
<td>G</td>
<td>gateway</td>
</tr>
<tr>
<td>G</td>
<td>admission controller, configuring 393</td>
</tr>
<tr>
<td>G</td>
<td>message manipulation rules, configuring 398</td>
</tr>
<tr>
<td>G</td>
<td>new call usage policy set, configuring 402</td>
</tr>
<tr>
<td>G</td>
<td>new call usage policy, configuring 399</td>
</tr>
<tr>
<td>G</td>
<td>new transaction policy set, configuring 405</td>
</tr>
<tr>
<td>G</td>
<td>new transaction policy, configuring 403</td>
</tr>
<tr>
<td>G</td>
<td>service point, configuring 403</td>
</tr>
<tr>
<td>G</td>
<td>session policy decision function, configuring 396</td>
</tr>
<tr>
<td>G</td>
<td>SIP policies and timers, configuring 397</td>
</tr>
<tr>
<td>G</td>
<td>timers, configuring 406</td>
</tr>
<tr>
<td>G</td>
<td>traceoptions, configuring 407</td>
</tr>
<tr>
<td>G</td>
<td>gateway properties, configuring 392</td>
</tr>
<tr>
<td>G</td>
<td>gateway, configuring 393</td>
</tr>
<tr>
<td>G</td>
<td>generated routes</td>
</tr>
<tr>
<td>G</td>
<td>configuring 369</td>
</tr>
<tr>
<td>G</td>
<td>group specific properties RIPng, configuring 339</td>
</tr>
<tr>
<td>G</td>
<td>group, device 27</td>
</tr>
</tbody>
</table>

494 Copyright © 2010, Juniper Networks, Inc.
H
H248 options
  encoding defaults, configuring.................................431
  service change, configuring........................................431
H248 options, configuring..............................................430
H248 properties
  application data inactivity detection, configuring........437
  base root, configuring.............................................437
  differentiated services, configuring..........................440
  event timestamp notification, configuring....................441
  hanging termination detection, configuring....................441
  inactivity timer, configuring....................................442
  notification behavior, configuring.............................443
  segmentation, configuring........................................444
  traffic management, configuring................................445
Helpers
  DNS packet forwarding, enabling................................199
  port, configuring....................................................201
  router/interface, configuring....................................196
  tracing operations, configuring..................................202
  configuring..................................................................195
I
ILMI protocol, configuring...........................................255
inet family type
  firewall filter, configuring......................................165
  prefix-specific actions, configuring...........................167
  service filters, configuring.......................................168
  simple filters, configuring.......................................169
inet6 family type
  firewall filter, configuring......................................171
  service filters, configuring.......................................173
Instance export
  configuring................................................................430
Instance import
  configuring................................................................430
Interface routes
  configuring................................................................430
Interface set, configuring.............................................234
Interface trace options, configuring...............................235
Interfaces
  logical interface properties, configuring......................212
  properties, configuring.............................................207
  receive bucket properties, configuring.......................209
  tracing operations, configuring................................209
  traffic shaping profile, configuring............................232
  transitions, damping..............................................208
  transmit leaky bucket, configuring.............................211
Interfaces
  MPLS, configuring..................................................285
  interfaces, configuring..........................................207
  intrusion detection service, configuring......................415
  inventory See device inventory
IP addresses
  configuring.............................................................17
J
Job Manager
  about........................................................................31
  displaying updating errors.......................................35
  reviewing..................................................................33
JUNOS software devices
  adding multiple with discovery rules.........................27
  configuring............................................................42
  JUNOS software, upgrading........................................471
L
label distribution protocol, configuring.........................264
label switched path
  administrative group, configuring.............................290
  automatic bandwidth, configuring.............................291
  BFD, configuring.....................................................296
  fast reroute, configuring.........................................293
  LSP related routes, adding.......................................294
  MPLS LSPs, configuring...........................................295
  label switched path, configuring..............................287
  layer 2 address learning, configuring.........................256
  layer 2 circuit
    local interface switching, configuring......................257
    neighbor interface, configuring..............................258
    tracing.............................................................261
  layer 2 circuit, configuring....................................257
  LDAP options, configuring........................................52
  LDAP server, configuring..........................................53
  link management protocol, configuring.......................275
  load balancing
    per-flow/per-prefix, configuring.............................203
  load balancing, configuring.....................................194
  logical interface
    demux source family type, configuring......................214
    epd threshold, configuring....................................214
    IP demux, configuring...........................................213
    unit properties, configuring................................212


Index
logical interfaces
  ccc family information, configuring..........................215
  inet family information, configuring..........................217
  inet6 family information, configuring..........................223
  ISO family information, configuring.............................229
  MPLS family information, configuring..............................230
  protocol family information, configuring..........................215
  TCC family information, configuring...............................232

LSP
  administrative group, configuring..............................301
  BFD, configuring..........................................................303, 309, 314
  class-type bandwidth, configuring..................................302
  egress router, configuring..............................................311
  packets, tracing.............................................................312
  primary paths, configuring.............................................300
  secondary paths, configuring.........................................305
  system log messages, configuring....................................313

M
  M-series devices
    adding multiple with discovery rules..............................27
    configuring...............................................................42
    supported Internet routers.............................................15
  managed devices.............................................................23
  martian addresses
    configuring.................................................................373
  maximum paths
    configuring.................................................................374
  maximum prefixes
    configuring.................................................................375
  MPLS
    administrative group, configuring..............................282
    administrative groups, configuring..............................282
    bandwidth, configuring..................................................283
    diffserv-aware, configuring..........................................284
    packets, tracing.............................................................320
  MPLS statistics, configuring.............................................319
  MPLS, enabling...............................................................279
  MSDP
    active source limit, configuring....................................322
    export policy, configuring.............................................323
    MSDP peers, configuring................................................325
    per-source active source limit,
      configuring...............................................................328
    routing table group, configuring....................................327
    traceoptions, configuring..............................................328
  MSDP peer group, configuring............................................324
  MSDP, configuring...........................................................321
  MSTP.................................................................329
  MTU signaling, configuring................................................317
  multicast
    configuring.................................................................377
  multiclass LSP
    class-type bandwidth constraints,
      configuring...............................................................308
  MX-series devices
    adding multiple with discovery rules..............................27
    configuring.................................................................42
    supported Internet Services routers..............................15

N
  named paths, configuring..................................................316
  navigation tree..............................................................7
  NetConf.................................................................13
  network
    connectivity, checking.................................................17
    ping command..............................................................17
  network address translation, configuring..........................420
  no-readvertise
    option.................................................................18
  NSM API.................................................................12
  NSM architecture
    distributed data collection.............................................7
  NSM modules
    Log Viewer...............................................................30
    Realtime Monitor.........................................................30, 485
  NSM UI
    about.................................................................7

O
  option
    no-readvertise..........................................................18
    retain........................................................................18
  Options
    configuring.................................................................380
  OSPF.................................................................331

P
  PGCP
    gateway, configuring.....................................................426
    H248 options, configuring.............................................430
    H248 properties, configuring..........................................436
    H248 timers, configuring.................................................447
    media service, configuring.............................................450
    monitor, configuring.....................................................448
    overload control, configuring.........................................449
    rule set, configuring.....................................................452
scheduler maps .......................................................... 141
schedulers .................................................................. 139
schema
See device schema
secondary paths
administrative group, configuring .......................... 307
SecurID server, configuring ..................................... 69
service interface pools, configuring ...................... 455
service set, configuring ............................................. 456
services
class of service, configuring ................................... 412
show route command ................................................ 17, 18
SNMP
communities ................................................................ 464
trap groups .................................................................. 466
views ........................................................................... 467
source routing
configuring ................................................................. 384
stateful firewall, configuring ...................................... 460
static LSP, configuring ............................................... 318
static route .................................................................. 18
Static Routes
configuring ................................................................. 385
status
device ......................................................................... 16
support, technical See technical support
T
T640 router, configuring ............................................. 105
TCP
See Transmission Control Protocol
technical overview ...................................................... 3
technical support
contacting JTAC ......................................................... xxx
topologies, configuring ............................................... 386
Traceoptions
configuring ................................................................. 387
Transmission Control Protocol ................................. 13
trap groups
configuring ................................................................. 466
U
unreachable workflow
importing device ...................................................... 16
V
views
configuring ................................................................. 467
VRRP ........................................................................... 358
VSTP ........................................................................... 359