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, 1995, 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 DCC’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, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS is a trademark 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
Editing Joanne McClintock
Cover Design Edmonds Design

Revision History
24 August, 2009—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 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 hereunder. 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 access to the Software to Customer employees and contractors having a need to use the Software for Customer’s internal business purposes.

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

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

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

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

- Objectives .................................................................................................... xxv
- Audience ..................................................................................................... xxv
- Documentation Conventions ....................................................................... xxv
- Documentation .......................................................................................... xxvii
- Requesting Technical Support ................................................................... xxviii
  - Self-Help Online Tools and Resources .................................................. xxix
  - Opening a Case with JTAC ................................................................. xxix

## 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**

- M-series and MX-series Devices Supported by NSM ..........................15
- Considering the Device Status ..........................................................16
- Configuring a Deployed M-series or MX-series Device for Importing to NSM ..........................................................17
  - Configure an IP Address and a User with Full Administrative Privileges for the Device ..........................................................17
  - Check Network Connectivity .........................................................17
  - Check Connectivity to the NSM Server .........................................18
  - Configure a Static Route to the NSM Server ..................................18
  - Establish a Telnet or an SSHv2, and a NETCONF protocol over SSH Connection to the NSM Server .........................................20

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

#### Chapter 4  
**Adding M-series and MX-series Devices Overview**

- About Device Creation ......................................................................25
- Supported Add Device Workflows for M-series and MX-series Devices ..........................................................26
- Importing Devices Overview ..............................................................27
- Modeling Devices Overview ..............................................................28
- Adding Multiple Devices Using Automatic Discovery (JUNOS Software Devices Only) ..........................................................29
- Adding Device Groups Overview ......................................................29

#### Chapter 5  
**Updating M-series and MX-series Devices Overview**

- About Updating M-series and MX-series Devices .............................31
- How the Update Process Works ........................................................32
- Job Manager ..................................................................................33
- Tracking Updated Devices Using Job Manager ..................................34
- Reviewing Job Information Displayed in Job Manager .......................35
- Device States Displayed in Job Manager During Update .................36
- Understanding Updating Errors Displayed in the Job Manager ..........37
## Table of Contents

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

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

- About Device Configuration .................................................43
- M-series and MX-series Device Configuration Settings Supported in NSM .....44
- Configuring Device Features ................................................46
- Example: Configuration of Interfaces for MPLS in the CLI and NSM ..........47

### Chapter 7  
Configuring Access

- Configuring Access Profiles for L2TP or PPP Parameters (NSM Procedure) ..........................................................49
- Configuring Access Profile (NSM Procedure) ................................49
- Configuring Accounting Parameters for Access Profiles (NSM Procedure) ..........................................................50
- Configuring the Accounting Order (NSM Procedure) ..................51
- Configuring the Authentication Order (NSM Procedure) ..............52
- Configuring the Authorization Order (NSM Procedure) ..............52
- Configuring the L2TP Client (NSM Procedure) ..............................53
- Configuring the Client Filter Name (NSM Procedure) ..................54
- Configuring the RADIUS Options (NSM Procedure) ....................55
- Configuring the RADIUS Server (NSM Procedure) ......................56
- Configuring the Provisioning Order (NSM Procedure) ..................57
- Configuring RADIUS Parameters for AAA Subscriber Management (NSM Procedure) ..........................................................58
- Configuring the RADIUS Parameters (NSM Procedure) ..............60
- Configuring the RADIUS for Subscribers Access Management, L2TP, or PPP (NSM Procedure) .........................................................61
- Configuring Session Limit (NSM Procedure) ...............................62
- Configuring the Access Profile (NSM Procedure) ............................63

### Chapter 8  
Configuring Accounting Options

- Configuring Accounting Options (NSM Procedure) ......................65
- Configuring Class Usage Profiles (NSM Procedure) ....................65
- Configuring a Log File (NSM Procedure) .................................66
- Configuring the Filter Profile (NSM Procedure) ............................67
- Configuring the Interface Profile (NSM Procedure) ......................68
- Configuring the Policy Decision Statistics Profile (NSM Procedure) ....69
- Configuring the MIB Profile (NSM Procedure) ..............................70
- Configuring the Routing Engine Profile (NSM Procedure) ..............71

### Chapter 9  
Configuring Applications

- Configuring the Application and Application Set (NSM Procedure) ........73
<table>
<thead>
<tr>
<th>Chapter 14</th>
<th>Configuring Event Options</th>
<th>147</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Destinations for File Archiving (NSM Procedure)</td>
<td>147</td>
<td></td>
</tr>
<tr>
<td>Configuring Event Script (NSM Procedure)</td>
<td>148</td>
<td></td>
</tr>
<tr>
<td>Generating Internal Events (NSM Procedure)</td>
<td>150</td>
<td></td>
</tr>
<tr>
<td>Configuring Event Policy (NSM Procedure)</td>
<td>151</td>
<td></td>
</tr>
<tr>
<td>Configuring Event Policy Tracing Operations (NSM Procedure)</td>
<td>154</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 15</th>
<th>Configuring Firewall</th>
<th>157</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the Firewall Filter for Any Family Type (NSM Procedure)</td>
<td>157</td>
<td></td>
</tr>
<tr>
<td>Configuring the Firewall Filter for Bridge Family Type (NSM Procedure)</td>
<td>159</td>
<td></td>
</tr>
<tr>
<td>Configuring the Firewall Filter for Ccc Family Type (NSM Procedure)</td>
<td>161</td>
<td></td>
</tr>
<tr>
<td>Configuring Filters for inet Family Type (NSM Procedure)</td>
<td>163</td>
<td></td>
</tr>
<tr>
<td>Configuring Firewall Filter for inet Family Type (NSM Procedure)</td>
<td>163</td>
<td></td>
</tr>
<tr>
<td>Configuring Prefix-specific Actions (NSM Procedure)</td>
<td>165</td>
<td></td>
</tr>
<tr>
<td>Configuring Service Filters (NSM Procedure)</td>
<td>166</td>
<td></td>
</tr>
<tr>
<td>Configuring Simple Filters (NSM Procedure)</td>
<td>167</td>
<td></td>
</tr>
<tr>
<td>Configuring Filters for inet6 Family Type (NSM Procedure)</td>
<td>168</td>
<td></td>
</tr>
<tr>
<td>Configuring Firewall Filter for inet6 Family Type (NSM Procedure)</td>
<td>169</td>
<td></td>
</tr>
<tr>
<td>Configuring Service Filters for inet6 (NSM Procedure)</td>
<td>171</td>
<td></td>
</tr>
<tr>
<td>Configuring the Firewall Filter for MPLS Family Type (NSM Procedure)</td>
<td>172</td>
<td></td>
</tr>
<tr>
<td>Configuring the Firewall Filter for VPLS Family Type (NSM Procedure)</td>
<td>175</td>
<td></td>
</tr>
<tr>
<td>Configuring a Policer for a Firewall Filter</td>
<td>178</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 16</th>
<th>Configuring Forwarding Options</th>
<th>181</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Accounting Options (NSM Procedure)</td>
<td>181</td>
<td></td>
</tr>
<tr>
<td>Configuring the Extended DHCP Agent (NSM Procedure)</td>
<td>183</td>
<td></td>
</tr>
<tr>
<td>Configuring Authentication Support for the DHCP Relay Agent (NSM Procedure)</td>
<td>183</td>
<td></td>
</tr>
<tr>
<td>Configuring Group (NSM Procedure)</td>
<td>184</td>
<td></td>
</tr>
<tr>
<td>Overriding the Default Configuration Settings for the Extended DHCP Relay Agent (NSM Procedure)</td>
<td>185</td>
<td></td>
</tr>
<tr>
<td>Configuring Relay Option 60 Information for Forwarding Client Traffic to Specific DHCP Servers (NSM Procedure)</td>
<td>186</td>
<td></td>
</tr>
<tr>
<td>Configuring Relay Option 82 for a DHCP Server (NSM Procedure)</td>
<td>188</td>
<td></td>
</tr>
<tr>
<td>Specifying the Name of a Group of DHCP Server Addresses for Use by the Extended DHCP Relay Agent (NSM Procedure)</td>
<td>189</td>
<td></td>
</tr>
<tr>
<td>Configuring Operations for Extended DHCP Relay Agent Processes (NSM Procedure)</td>
<td>190</td>
<td></td>
</tr>
<tr>
<td>Specifying Address Family for Filters (NSM Procedure)</td>
<td>191</td>
<td></td>
</tr>
</tbody>
</table>
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) ...................................... 209
  Configuring Receive Bucket Properties on Interfaces (NSM Procedure) .......... 210
  Configuring Tracing Operations of an Individual Router Interface (NSM Procedure) .......................................................... 210
  Configuring Transmit Leaky Bucket Properties (NSM Procedure) .............. 211
  Configuring Logical Interface Properties (NSM Procedure) .................... 212
    Configuring Logical Unit Properties (NSM Procedure) ......................... 212
    Configuring an IP Demux Underlying Interface (NSM Procedure) .............. 213
    Configuring the Logical Demux Source Family Type on the IP Demux Underlying Interface (NSM Procedure) ......................... 214
    Configuring Epd Threshold for the Logical Interface (NSM Procedure) ........ 214
  Configuring Protocol Family Information for the Logical Interface (NSM Procedure) .......................................................... 215
    Configuring Protocol Family (Ccc) Information for the Logical Interface (NSM Procedure) .................................................. 216
    Configuring Protocol Family (Inet) Information for the Logical Interface (NSM Procedure) .................................................. 217
    Configuring Protocol Family (Inet6) Information for the Logical Interface (NSM Procedure) .................................................. 223
    Configuring Protocol Family (ISO) Information for the Logical Interface (NSM Procedure) .................................................. 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) ......................... 233
  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
Configuring Maximum Prefixes (NSM Procedure) ........................................311
Configuring Multicast (NSM Procedure) .......................................................313
Configuring Options (NSM Procedure) .........................................................316
Configuring Routing Tables (NSM Procedure) ..............................................317
Configuring Routing Table Groups (NSM Procedure) .................................319
Configuring Source Routing (NSM Procedure) ..............................................320
Configuring Static Routes (NSM Procedure) .................................................321
Configuring Traceoptions (NSM Procedure) .................................................323

Chapter 22 Configuring Security 325
Configuring Authentication Key Updates (NSM Procedure) ..........................325

Chapter 23 Configuring Services 327
Configuring Adaptive Services PICs (NSM Procedure) ..................................327
Configuring Border Signaling Gateways (NSM Procedure) ............................328
Configuring Gateway Properties (NSM Procedure) ......................................328
Configuring Gateway (NSM Procedure) .......................................................329
Configuring an Admission Controller (NSM Procedure) ..............................329
Configuring Session Policy Decision Function (NSM Procedure) ................331
Configuring Service Point (NSM Procedure) ..............................................332
Configuring SIP Policies and Timers (NSM Procedure) ..................................334
Configuring Traceoptions (NSM Procedure) ................................................335
Configuring Class of Service (NSM Procedure) ..........................................350
Configuring Intrusion Detection Service (NSM Procedure) ..........................354
Tracing Services PIC Operations (NSM Procedure) ......................................358
Configuring Network Address Translation (NSM Procedure) ........................359
Configuring PGCP (NSM Procedure) .............................................................363
Configuring Gateway (NSM Procedure) .......................................................364
Configuring a Virtual Border Gateway Function on the Router (NSM Procedure) 364
Configuring Data Inactivity Detection (NSM Procedure) ................................365
Configuring Gateway Controller (NSM Procedure) ......................................366
Configuring Graceful Restart (NSM Procedure) ...........................................366
Configuring H248 Options Properties (NSM Procedure) ..............................367
Configuring H248 Options (NSM Procedure) ..............................................367
Changing Encoding Defaults (NSM Procedure) ...........................................368
Configuring Service Change (NSM Procedure) ............................................369
Configuring H248 Properties (NSM Procedure) ...........................................373
Configuring Application Data Inactivity Detection (NSM Procedure) .............374
Configuring Base Root (NSM Procedure) .....................................................374
Configuring Differentiated Services (NSM Procedure) .................................377
Configuring Event Timestamp Notification (NSM Procedure) ........................377
Hanging Termination Detection (NSM Procedure) .........................................378
Configuring Inactivity Timer (NSM Procedure) ...........................................379
Configuring Notification Behavior (NSM Procedure) ....................................380
Configuring Segmentation (NSM Procedure) ..............................................381
## Table of Contents

### Chapter 24 Configuring SNMP

- Configuring Basic System Identification for SNMP (NSM Procedure) ........... 401
- Configuring SNMP Communities (NSM Procedure) ................................ 402
- Configuring SNMP Trap Groups (NSM Procedure) .................................. 404
- Configuring SNMP Views (NSM Procedure) ........................................... 405

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

#### Chapter 25 Managing M-series and MX-series Devices Overview

Managing M-series and MX-series Device Software Versions ..................... 409

#### Chapter 26 Viewing the M-series and MX-series Device Inventory in NSM and the CLI

Viewing and Reconciling Device Inventory .............................................. 411
Comparing Device Inventory in NSM and the CLI .................................. 412
  - Viewing Device Inventory in NSM ...................................................... 412
  - Viewing Device Inventory from the CLI .............................................. 414

#### Chapter 27 Topology Manager

Overview of the NSM Topology Manager ............................................. 417
Requisites for a Topology Discovery .................................................... 417
About the NSM Topology Manager Toolbar ......................................... 418
Part 5  Monitoring M-series and MX-series Devices

Chapter 28  Real Time Monitoring of M-series and MX-series Devices

- About the Realtime Monitor .................................................................423
- Viewing Device Status ........................................................................424
- Viewing Device Monitor Alarm Status ..............................................427
- Setting the Polling Interval For Device Alarm Status ......................428

Part 6  Index

- Index ..................................................................................................431
# List of Figures

## Part 1  Getting Started

<table>
<thead>
<tr>
<th>Chapter 2</th>
<th>Understanding the JUNOS CLI and NSM</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Figure 1: Overview of the User Interface</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Figure 2: NSM Network Architecture</td>
<td>12</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Chapter 5</th>
<th>Updating M-series and MX-series Devices Overview</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Figure 3: Job Information Dialog Box</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>Figure 4: Failed Update Job Information Dialog Box</td>
<td>38</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Chapter 6</th>
<th>Configuring M-series and MX-series Devices Overview</th>
<th>43</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Figure 5: MPLS Configuration in the CLI</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>Figure 6: MPLS Configuration in NSM</td>
<td>48</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Chapter 26</th>
<th>Viewing the M-series and MX-series Device Inventory in NSM and the CLI</th>
<th>411</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Figure 7: The Device Inventory Window</td>
<td>413</td>
</tr>
<tr>
<td></td>
<td>Figure 8: Viewing the Hardware Inventory</td>
<td>413</td>
</tr>
<tr>
<td></td>
<td>Figure 9: Viewing the Software Inventory</td>
<td>414</td>
</tr>
</tbody>
</table>
# List of Tables

## About This Guide
- Table 1: Notice Icons ..................................................................................xxvi
- Table 2: Text Conventions ..........................................................................xxvi
- Table 3: Syntax Conventions .....................................................................xxvii
- Table 4: Network and Security Manager Publications .................................xxvii

## 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 31
  - Table 6: Device States During Update ............................................................36

## Part 3 Configuring M-series and MX-series Devices
- Chapter 6 Configuring M-series and MX-series Devices Overview 43
  - Table 7: The JUNOS Configuration Hierarchy and the NSM Configuration Tree ..............................................................................................................44
- Chapter 7 Configuring Access 49
  - Table 8: Access Profile Properties Configuration Details ..............................50
  - Table 9: Accounting Parameter Configuration Details ..................................51
  - Table 10: Accounting Order Configuration Details .......................................52
  - Table 11: Authentication Order Configuration Details ...................................52
  - Table 12: Authorization Order Configuration Details .....................................53
  - Table 13: Client Configuration Details ...........................................................53
  - Table 14: Client Filter Name Configuration Details .......................................55
  - Table 15: Ldap Options Configuration Details ...............................................55
  - Table 16: Ldap Server Configuration Details ..................................................57
  - Table 17: Provisioning Order Configuration Details .......................................57
  - Table 18: Radius Parameter Configuration Details .........................................58
  - Table 19: Radius Parameters Configuration Details .......................................61
  - Table 20: Radius Server Configuration Details ...............................................62
  - Table 21: Session Limit Configuration Details .................................................63
  - Table 22: Access Profile Configuration Details ...............................................63
- Chapter 8 Configuring Accounting Options 65
  - Table 23: Class Usage Profile Configuration Details .......................................66
Table 24: Log File Configuration Details ........................................................67
Table 25: Filter Profile Configuration Details .................................................68
Table 26: Interface Profile Configuration Details ...........................................69
Table 27: Policy Decision Statistics Profile Configuration Details .................70
Table 28: MIB Profile Configuration Details ...................................................71
Table 29: Routing Engine Profile Configuration Details .................................72

Chapter 9 Configuring Applications 73
Table 30: Applications Configuration Details .................................................74

Chapter 10 Configuring Bridge Domains 75
Table 31: Bridge Domain Configuration Details .............................................76
Table 32: Bridge Options Configuration Details .............................................77
Table 33: Forwarding Options Configuration Details .....................................78
Table 34: Logical Interface Configuration Details .........................................80
Table 35: Multicast Snooping Options Configuration Details .........................81
Table 36: Igmp Snooping Configuration Details .............................................83
Table 37: VLAN ID Configuration Details ....................................................88

Chapter 11 Configuring Chassis 89
Table 38: Aggregated Devices Configuration Details ....................................90
Table 39: Chassis Alarms Configuration Details ...........................................91
Table 40: Container Interfaces Configuration Details ....................................91
Table 41: FPC Configuration Details ............................................................92
Table 42: Lcc Configuration Details .............................................................99
Table 43: Chassis Redundancy Configuration Details ..................................105
Table 44: Chassis Routing Engine Configuration Details ..............................106

Chapter 12 Configuring Authentication 107
Table 45: RADIUS Authentication Configuration Details ..............................107
Table 46: TACACS+ Authentication Configuration Details ..........................108
Table 47: Login Class Authentication Configuration Details .........................110
Table 48: User Authentication Configuration Details ...................................111
Table 49: Remote Template Account Details ...............................................112
Table 50: Local Template Account Details ...................................................113

Chapter 13 Configuring Class of Service Features 115
Table 51: Configuring and Applying Behavior Aggregate Classifiers ............116
Table 52: Configuring Code Point Aliases ....................................................119
Table 53: Drop Profile Configuration Fields ................................................120
Table 54: Assigning Forwarding Classes to Output Queues ..........................122
Table 55: Forwarding Policy Configuration Details ......................................123
Table 56: Fragmentation Maps Configuration Details ..................................125
Table 57: Host Outbound Traffic Configuration Details ................................126
Table 58: Interfaces Configuration Fields ....................................................127
Table 59: Routing Instances Configuration Details .......................................132
Table 60: Configuring Schedulers ..............................................................134
Table 61: Assigning Forwarding Classes to Output Queues ..........................136
Table 62: Restricted Queue Configuration Details ........................................137
Table 63: Traceoptions Configuration Details .............................................158
Table 64: Traffic Control profile Configuration Details .................................140
Table 65: Translation Table Configuration Details .......................................142

Chapter 14 Configuring Event Options 147
Table 66: Destination Configuration Details ...............................................147
Table 114: Traffic Shaping Configuration Details .............................................234
Table 115: Interface Set Configuration Details .............................................235
Table 116: Traceoption Configuration Details .............................................236

Chapter 18 Configuring Multicast Snooping Options ..................................237
Table 117: Multicast Snooping Options Configuration Details ......................238

Chapter 19 Configuring Policy Options .....................................................241
Table 118: AS Path Configuration Details ...................................................242
Table 119: AS Path Group Configuration Details .........................................243
Table 120: Community Configuration Details .............................................244
Table 121: Condition Configuration Details ................................................245
Table 122: Damping Configuration Details ..................................................246
Table 123: Configuring Policy Statement Fields .........................................247
Table 124: Configuring Prefix List Fields ...................................................249

Chapter 20 Configuring Protocols ..............................................................251
Table 125: Configuring Bfd Fields ...............................................................252
Table 126: BGP Configuration Fields ...........................................................253
Table 127: Trace Options Configuration Details .........................................255
Table 128: L2 Learning Configuration Details ...........................................257
Table 129: Local Switching Configuration Details ......................................258
Table 130: Neighbor Interface Configuration Details ..................................260
Table 131: Layer2 Circuit Traceoption Configuration Details ......................263
Table 132: Layer2 Circuit Configuration Details .........................................265
Table 133: LDP Configuration Details .........................................................268
Table 134: Link Management Protocol Configuration Details .....................278
Table 135: MSTP Configuration Fields .......................................................280
Table 136: OSPF Configuration Fields .......................................................282
Table 137: RIP Configuration Fields ..........................................................286
Table 138: RSVP Configuration Details ......................................................288
Table 139: VRRP Configuration Fields .......................................................294
Table 140: VSTP Configuration Fields .......................................................296

Chapter 21 Configuring Routing Options ..................................................297
Table 141: Confederation Fields .................................................................298
Table 142: Dynamic Tunnels Configuration Details ......................................299
Table 143: Fate Sharing Fields .................................................................301
Table 144: Flow Route Fields .................................................................303
Table 145: Forwarding Table Fields ...........................................................304
Table 146: Generated Routes Fields ............................................................306
Table 147: Interface Routes Fields ...............................................................308
Table 148: Configuring Martian Address Fields .........................................309
Table 149: Configuring Maximum Paths Fields ........................................311
Table 150: Configuring Maximum Prefixes Fields ....................................312
Table 151: Configuring Multicast Fields ....................................................313
Table 152: Configuring Options Fields ......................................................316
Table 153: Rib Fields .................................................................................318
Table 154: Rib Group Fields .......................................................................320
Table 155: Source Routing Fields ..............................................................321
Table 156: Static Fields .............................................................................322
Table 157: Traceoption Fields ...................................................................323

Chapter 22 Configuring Security ..............................................................325
Chapter 23 Configuring Services 327
Table 158: Security Authentication Key Configuration Details ..........326
Table 159: Adaptive Services Pics Configuration Details ......................328
Table 160: Gateway Configuration Details ...........................................329
Table 161: Admission Controller Configuration Details .........................330
Table 162: Session Policy Decision Configuration Details ......................331
Table 163: Service Point Configuration Details ......................................333
Table 164: Message Manipulate Rules Configuration Details ...................334
Table 165: New Call Usage Policy Configuration Details .........................337
Table 166: New Call Usage Policy Set Configuration Details .................340
Table 167: Transaction Policy Configuration Details ...............................341
Table 168: Transaction Policy Set Configuration Details .........................344
Table 169: Timers Configuration Details ..............................................345
Table 170: Traceoption BSG Configuration Details .................................346
Table 171: CoS Configuration Details ..................................................352
Table 172: IDS Configuration Details ...................................................355
Table 173: Traceoptions Configuration Details .......................................359
Table 174: NAT Configuration Details ..................................................361
Table 175: Virtual BGF Configuration Details .......................................364
Table 176: Data Inactivity Detection Configuration Details ......................365
Table 177: Gateway Controller Configuration Details ...............................366
Table 178: Graceful Restart Configuration Details ....................................367
Table 179: H248 Configuration Details ..................................................368
Table 180: Encoding Defaults Configuration Details ...............................368
Table 181: Context Indication Configuration Details .................................369
Table 182: Control Association Configuration Details ..............................371
Table 183: Virtual Interface Indications Configuration Details .................373
Table 184: Data Inactivity Detection Configuration Details ......................374
Table 185: Base Root Package Configuration Details ...............................376
Table 186: Diffserv Configuration Details .............................................377
Table 187: Event Timestamp Notification Configuration Details ...............378
Table 188: Hanging Termination Detection Configuration Details ..............379
Table 189: Inactivity Timer Configuration Details ...................................380
Table 190: Notification Behavior Configuration Details .........................381
Table 191: Segmentation Package Configuration Details .........................382
Table 192: Traffic Management Configuration Details .............................384
Table 193: H248 Timers Configuration Details ........................................386
Table 194: Monitor Configuration Details .............................................387
Table 195: Overload Control Configuration Details ...................................387
Table 196: Session Mirroring Configuring Details ...................................388
Table 197: Media Service Configuration Details ......................................389
Table 198: Configuring Rule ...............................................................389
Table 199: Configuring Rule Set ...........................................................390
Table 200: Session Mirroring Configuration Details .................................391
Table 201: Traceoptions Configuration Details ......................................392
Table 202: Virtual Interface Configuration Details .................................393
Table 203: Service Interface Pools Configuration Details .........................394
Table 204: Service Set Configuration Details .........................................395
Table 205: Stateful Firewall Configuration Details ...................................399

Chapter 24 Configuring SNMP 401

Table 206: Security Authentication Key Configuration Details ..................402
Table 207: Adaptive Services Pics Configuration Details .........................403
Table 208: Gateway Configuration Details ............................................404
Table 209: Admission Controller Configuration Details .........................405
Table 210: Session Policy Decision Configuration Details ......................406
Table 211: Service Point Configuration Details ......................................407
Table 212: Message Manipulate Rules Configuration Details ...................408
Table 213: New Call Usage Policy Configuration Details .........................411
Table 214: New Call Usage Policy Set Configuration Details .................414
Table 215: Transaction Policy Configuration Details ...............................415
Table 216: Transaction Policy Set Configuration Details .........................418
Table 217: Timers Configuration Details ...............................................419
Table 218: Traceoption BSG Configuration Details ...................................420
Table 219: CoS Configuration Details ....................................................426
Table 220: IDS Configuration Details ....................................................427
Table 221: Traceoptions Configuration Details .......................................431
Table 222: NAT Configuration Details ..................................................433
Table 223: Virtual BGF Configuration Details .......................................436
Table 224: Data Inactivity Detection Configuration Details ......................437
Table 225: Gateway Controller Configuration Details ...............................438
Table 226: Graceful Restart Configuration Details ....................................439
Table 227: H248 Configuration Details ..................................................440
Table 228: Encoding Defaults Configuration Details ...............................440
Table 229: Context Indication Configuration Details .................................441
Table 230: Control Association Configuration Details ..............................444
Table 231: Virtual Interface Indications Configuration Details .................446
Table 232: Data Inactivity Detection Configuration Details ......................447
Table 233: Base Root Package Configuration Details ...............................449
Table 234: Diffserv Configuration Details .............................................450
Table 235: Event Timestamp Notification Configuration Details ...............451
Table 236: Hanging Termination Detection Configuration Details ..............452
Table 237: Inactivity Timer Configuration Details ...................................453
Table 238: Notification Behavior Configuration Details .........................454
Table 239: Segmentation Package Configuration Details .........................455
Table 240: Traffic Management Configuration Details .............................457
Table 241: H248 Timers Configuration Details ........................................459
Table 242: Monitor Configuration Details .............................................460
Table 243: Overload Control Configuration Details ...................................460
Table 244: Session Mirroring Configuring Details ...................................461
Table 245: Media Service Configuration Details ......................................462
Table 246: Configuring Rule ...............................................................462
Table 247: Configuring Rule Set ...........................................................463
Table 248: Session Mirroring Configuration Details .................................464
Table 249: Traceoptions Configuration Details ......................................465
Table 250: Virtual Interface Configuration Details .................................466
Table 251: Service Interface Pools Configuration Details .........................467
Table 252: Service Set Configuration Details .........................................468
Table 253: Stateful Firewall Configuration Details ...................................469
Part 5

Monitoring M-series and MX-series Devices

Chapter 28

Real Time Monitoring of M-series and MX-series 423

Table 210: Device Status Information ..........................................................424
About This Guide

- Objectives on page xxv
- Audience on page xxv
- Documentation Conventions on page xxv
- Documentation on page xxvii
- Requesting Technical Support on page xxviii

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.

Audience

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 xxvi defines notice icons used in this guide.

### Table 1: Notice Icons

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

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

### Table 2: Text Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><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#</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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><strong>Key names linked with a plus (+) sign</strong></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</code>, <code>ipAddress</code></td>
</tr>
<tr>
<td><strong>The angle bracket (&gt;)</strong></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 xxvii 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 xxvii 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. 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.

- **JTAC policies**—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at [http://www.juniper.net/customers/support/downloads/7100059-EN.pdf](http://www.juniper.net/customers/support/downloads/7100059-EN.pdf).

- **Product warranties**—For product warranty information, visit [http://www.juniper.net/support/warranty/](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/](http://www.juniper.net/customers/support/)
- Search for known bugs: [http://www2.juniper.net/kb/](http://www2.juniper.net/kb/)
- Find product documentation: [http://www.juniper.net/techpubs/](http://www.juniper.net/techpubs/)
- Find solutions and answer questions using our Knowledge Base: [http://kb.juniper.net/](http://kb.juniper.net/)
- Download the latest versions of software and review release notes: [http://www.juniper.net/customers/csc/software/](http://www.juniper.net/customers/csc/software/)
- Search technical bulletins for relevant hardware and software notifications: [https://www.juniper.net/alerts/](https://www.juniper.net/alerts/)
- Join and participate in the Juniper Networks Community Forum: [http://www.juniper.net/company/communities/](http://www.juniper.net/company/communities/)
- Open a case online in the CSC Case Management tool: [http://www.juniper.net/cm/](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/](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/](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](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
M-series and MX-series Devices
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
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 co-management using other methods. To manage the device configuration, you can also use the XML files import and export feature, or you can manage from the device’s admin console.

Related Topics

- 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
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;
```
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**

![User Interface Diagram]
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
How NSM Works with the CLI and Distributed Data Collection

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

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

- **configlet**—A configlet is a small, static configuration file that contains information 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.

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.
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 17

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 17
Considering the Device Status

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

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

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

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

- **Undeployed devices**—Undeployed devices are devices that you are not currently using in your network and, typically, for which you do not have IP addresses, zones, or other basic network information. For undeployed devices, you can model a new device configuration and later install that configuration on the device. For more information 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 17
Configuring a Deployed M-series or MX-series Device for Importing to NSM

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

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

To configure these parameters, perform the following tasks:

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

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

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

**Action**
Generally when you install the JUNOS 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:
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@>
```

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.

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 hierarchy mode, go to the following hierarchy level:

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

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

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

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

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

4. Verify the configuration:

   ```
   user@host# show
   ```

5. Commit the configuration:
user@host# commit

6. Verify the connection to the NSM server:

user@host# run ping destination

Sample Output

user@host> edit
Entering configuration mode

[edit]
user@host# edit routing-options

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

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

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

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

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

[edit routing-options]
user@host# run ping 192.193.60.181
PING 192.193.60.181 (192.193.60.181): 56 data bytes
64 bytes from 192.193.60.181: icmp_seq=0 ttl=64 time=23.050 ms
64 bytes from 192.193.60.181: icmp_seq=1 ttl=64 time=18.129 ms
64 bytes from 192.193.60.181: icmp_seq=2 ttl=64 time=0.304 ms
^C
--- 192.193.60.181 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.304/13.828/23.050/9.771 ms

Meaning The sample output shows that a static route (192.193.60.181/32) to the NSM server is configured and committed, and that there is a connection between the router and the server because the ping command shows that three packets were transmitted and received.
Establish a Telnet or an SSHv2, and a NETCONF protocol over SSH Connection to the NSM Server

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

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

   [edit system services]

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

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

4. Verify the configuration:

   user@host# show

5. Commit the configuration:

   user@host# commit

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

[edit system services]
Establish a Telnet or an SSHv2, and a NETCONF protocol over SSH Connection to the NSM Server
Establish a Telnet or an SSHv2, and a NETCONF protocol over SSH Connection to the NSM Server
Part 2

Integrating M-series and MX-series Devices

- Adding M-series and MX-series Devices Overview on page 25
- Updating M-series and MX-series Devices Overview on page 31
Chapter 4
Adding M-series and MX-series Devices
Overview

About Device Creation on page 25
Supported Add Device Workflows for M-series and MX-series Devices on page 26
Importing Devices Overview on page 27
Modeling Devices Overview on page 28
Adding Multiple Devices Using Automatic Discovery (JUNOS Software Devices Only) on page 29
Adding Device Groups Overview on page 29

About Device Creation

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

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

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

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

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

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

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

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

**Related Topics**
- Supported Add Device Workflows for M-series and MX-series Devices on page 26
- Importing Devices Overview on page 27
- Modeling Devices Overview on page 28
- Adding Multiple Devices Using Automatic Discovery (JUNOS Software Devices Only) on page 29
- Adding Device Groups Overview on page 29

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

An M-series or MX-series device can be added using the following methods or workflows:
- Import device with static IP address
- Import device with dynamic IP address
- Model and activate device
- Rapid deployment (configlets)
- Device discovery
Import many devices (CSV file) with static IP addresses

Import many devices (CSV file) with dynamic IP addresses

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

**Related Topics**
- About Device Creation on page 25
- Importing Devices Overview on page 27
- Modeling Devices Overview on page 28
- Adding Multiple Devices Using Automatic Discovery (JUNOS Software Devices Only) on page 29
- Adding Device Groups Overview on page 29

---

**Importing Devices Overview**

NSM can import device configurations from M-series and MX-series devices running JUNOS 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 25
- Supported Add Device Workflows for M-series and MX-series Devices on page 26
- Modeling Devices Overview on page 28
- Adding Multiple Devices Using Automatic Discovery (JUNOS Software Devices Only) on page 29
- Adding Device Groups Overview on page 29

Modeling Devices Overview

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

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

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

Related Topics
- About Device Creation on page 25
- Supported Add Device Workflows for M-series and MX-series Devices on page 26
- Importing Devices Overview on page 27
- Adding Multiple Devices Using Automatic Discovery (JUNOS Software Devices Only) on page 29
- Adding Device Groups Overview on page 29

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 25
- Supported Add Device Workflows for M-series and MX-series Devices on page 26
- Importing Devices Overview on page 27
- Modeling Devices Overview on page 28
- Adding Device Groups Overview on page 29

Adding Device Groups Overview

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

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

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

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

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

**Related Topics**

- About Device Creation on page 25
- Supported Add Device Workflows for M-series and MX-series Devices on page 26
- Importing Devices Overview on page 27
- Modeling Devices Overview on page 28
- Adding Multiple Devices Using Automatic Discovery (JUNOS Software Devices Only) on page 29
Chapter 5

Updating M-series and MX-series Devices

Overview

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

About Updating M-series and MX-series Devices

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

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

Updating a device is a three-step process.

1. Ensure that you have configured the device correctly, created and assigned a policy to the device, and established a connection between the device and the management server.
2. From the Device Manager launchpad, select Update Device. The launchpad displays the Update Device(s) dialog box.
   All connected and managed devices appear in the device list. Modeled devices and devices awaiting import for the first time do not appear.
3. Select the devices or device groups you want to update and click Apply Changes. NSM updates the selected devices or device groups with the modeled configuration.
NSM uses centralized control and tracking to indicate when you need to update a device, and to follow the progress of the device configuration you are updating. Before updating your managed devices, you can use other NSM modules and tools to identify devices that need to be updated, validate their modeled configurations, and preview how those devices accept the new configuration. After updating, you can use the same tools to verify a successful update. These tools include:

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

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

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

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

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

### How the Update Process Works

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

1. Using the NSM monitoring tools, you learn of the attack and locate the cause of the event. Using NSM modules such as the Realtime Monitor and Log Viewer, you determine the exact attack that penetrated the device. From the Report Manager, you also determine what rule in the security policy was ineffective in blocking the attack.

2. You update the modeled device configuration, editing the configuration to detect and prevent the attack from entering your network again.
3. Before updating the running configuration, you review the modeled device configuration. Using a delta configuration summary, compare the modeled configuration with the running configuration on the device to confirm the differences. Fine-tune the modeled configuration, if needed.

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

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

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

---

**Related Topics**

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

---

**Job Manager**

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

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

- Name of the command
- Date and time the command was sent
- Completion status for each device that received the command
- Detailed description of command progress
- Command output, such as a configuration list or command-line interface (CLI) changes on the device
NOTE: Job Manager configuration summaries and job information details do not display passwords in the list of CLI commands for administrators that do not have the assigned activity “View Device Passwords.” By default, only the super administrator has this assigned activity.

Related Topics
- About Updating M-series and MX-series Devices on page 31
- How the Update Process Works on page 32
- Tracking Updated Devices Using Job Manager on page 34
- Reviewing Job Information Displayed in Job Manager on page 35
- Device States Displayed in Job Manager During Update on page 36
- Understanding Updating Errors Displayed in the Job Manager on page 37

Tracking Updated Devices Using Job Manager

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

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

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

Related Topics
- About Updating M-series and MX-series Devices on page 31
- How the Update Process Works on page 32
- Job Manager on page 33
- Reviewing Job Information Displayed in Job Manager on page 35
Reviewing Job Information Displayed in Job Manager

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

Figure 3: Job Information Dialog Box

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

The job information includes:

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

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

**NOTE:** If the Job Information dialog box might contain Chinese, Japanese, or Korean characters, you must 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 31
- How the Update Process Works on page 32
- Job Manager on page 33
- Tracking Updated Devices Using Job Manager on page 34
- Device States Displayed in Job Manager During Update on page 36
- Understanding Updating Errors Displayed in the Job Manager on page 37

### Device States Displayed in Job Manager During Update

During an update, the managed device changes device state. You can view the current device state in real time in the State Description field of the Job Information dialog box. Table 6 on page 36 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>
</tbody>
</table>
Table 6: Device States During Update (continued)

<table>
<thead>
<tr>
<th>Device State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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</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>Device Data Model</td>
<td></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 31
- How the Update Process Works on page 32
- Job Manager on page 33
- Tracking Updated Devices Using Job Manager on page 34
- Reviewing Job Information Displayed in Job Manager on page 35
- Understanding Updating Errors Displayed in the Job Manager on page 37

Understanding Updating Errors Displayed in the Job Manager

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

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

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

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

Figure 4: Failed Update Job Information Dialog Box

In the Job Information dialog box, the update:

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

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

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

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

**Related Topics**
- About Updating M-series and MX-series Devices on page 31
- How the Update Process Works on page 32
- Job Manager on page 33
- Tracking Updated Devices Using Job Manager on page 34
- Reviewing Job Information Displayed in Job Manager on page 35
- Device States Displayed in Job Manager During Update on page 36
Part 3
Configuring M-series and MX-series Devices

- Configuring M-series and MX-series Devices Overview on page 43
- Configuring Access on page 49
- Configuring Accounting Options on page 65
- Configuring Applications on page 73
- Configuring Bridge Domains on page 75
- Configuring Chassis on page 89
- Configuring Authentication on page 107
- Configuring Class of Service Features on page 115
- Configuring Event Options on page 147
- Configuring Firewall on page 157
- Configuring Forwarding Options on page 181
- 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 297
- Configuring Security on page 325
- Configuring Services on page 327
- Configuring SNMP on page 401
Chapter 6

Configuring M-series and MX-series Devices Overview

About Device Configuration on page 43
M-series and MX-series Device Configuration Settings Supported in NSM on page 44
Configuring Device Features on page 46
Example: Configuration of Interfaces for MPLS in the CLI and NSM on page 47

About Device Configuration

This topic does not provide extensive details for configuring features on M-series and MX-series devices in Network and Security Manager (NSM). For detailed information about configuring specific features for M-series and MX-series devices, see the following JUNOS 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
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 44 provides a general guideline of the CLI hierarchy levels that are supported in the NSM configuration tree. For the exact parameters available, double-click the device in the Device Manager and select the Configuration tab. The configuration tree appears in the main display area with all parameters viewable or configurable from NSM.

**Table 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 43
- Configuring Device Features on page 46
- Example: Configuration of Interfaces for MPLS in the CLI and NSM on page 47

Configuring Device Features

You can configure JUNOS 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**.

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

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

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

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

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

Figure 6 on page 48 shows the NSM UI with the same information as in the CLI example. On the left, the Navigation tree is expanded at Protocols, and then further expanded at MPLS, similar to the CLI hierarchy levels. Within MPLS, Interface is highlighted, indicating that the information 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.
In addition, Figure 6 on page 48 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 43
- M-series and MX-series Device Configuration Settings Supported in NSM on page 44
- Configuring Device Features on page 46
Chapter 7
Configuring Access

- Configuring Access Profiles for L2TP or PPP Parameters (NSM Procedure) on page 49
- Configuring the Access Profile (NSM Procedure) on page 63

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 49
2. Configuring Accounting Parameters for Access Profiles (NSM Procedure) on page 50
3. Configuring the Accounting Order (NSM Procedure) on page 51
4. Configuring the Authentication Order (NSM Procedure) on page 52
5. Configuring the Authorization Order (NSM Procedure) on page 52
6. Configuring the L2TP Client (NSM Procedure) on page 53
7. Configuring the Client Filter Name (NSM Procedure) on page 54
8. Configuring the LDAP Options (NSM Procedure) on page 55
9. Configuring the LDAP Server (NSM Procedure) on page 56
10. Configuring the Provisioning Order (NSM Procedure) on page 57
11. Configuring RADIUS Parameters for AAA Subscriber Management (NSM Procedure) on page 58
12. Configuring the RADIUS Parameters (NSM Procedure) on page 60
13. Configuring the RADIUS for Subscriber Access Management, L2TP, or PPP (NSM Procedure) on page 61
14. Configuring Session Limit (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 8 on page 50.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

### Table 8: 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 9 on page 51.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.
Table 9: 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 RADIUS accounting to send an Acct-Stop message when client access fails 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 RADIUS accounting to send an Acct-Stop message when the AAA server denies a client access.</td>
</tr>
<tr>
<td></td>
<td>6. Select the <strong>Immediate Update</strong> check box to configure the router to send an Acct-Update message to the RADIUS accounting server on receipt of a response (for example, an ACK or timeout) to the Acct-Start message.</td>
</tr>
<tr>
<td></td>
<td>7. From the <strong>Update Interval</strong> list, select the amount of time between updates, in minutes. Range: 10 through 1440 minutes Default: no updates</td>
</tr>
<tr>
<td></td>
<td>8. From the <strong>Statistics</strong> list, select the time statistics for the 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 LT2P 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 10 on page 52.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.
Table 10: 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. |

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

Table 11: 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. |

Configuring the Authorization Order (NSM Procedure)

To configure authorization order in NSM:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Access.
4. Select Profile.
5. Add or modify settings as specified in Table 12 on page 53.
6. Click one:
   ■ OK—Saves the changes.
   ■ Cancel—Cancels the modifications.

### Table 12: Authorization Order Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the authorization order.</td>
<td>1. Click Add new entry next to Profile.</td>
</tr>
<tr>
<td></td>
<td>2. Click Authorization Order next to Profile.</td>
</tr>
<tr>
<td></td>
<td>3. Click Add new entry next to Authorization Order.</td>
</tr>
<tr>
<td></td>
<td>4. In the New authorization-order 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 13 on page 53.
6. Click one:
   ■ OK—Saves the changes.
   ■ Cancel—Cancels the modifications.

### Table 13: Client Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the client.</td>
<td>1. Click Add new entry next to Profile.</td>
</tr>
<tr>
<td></td>
<td>2. Click Client next to Profile.</td>
</tr>
<tr>
<td></td>
<td>3. Click Add new entry next to Client.</td>
</tr>
<tr>
<td></td>
<td>4. In the Name box, enter the client name.</td>
</tr>
<tr>
<td></td>
<td>5. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. In the Chap Secret box, enter the secret key associated with a peer.</td>
</tr>
<tr>
<td></td>
<td>7. In the pap password box, enter the Password Authentication Protocol (PAP) password.</td>
</tr>
<tr>
<td>Configure a client group.</td>
<td>1. Click Client Group next to client.</td>
</tr>
<tr>
<td></td>
<td>2. Click Add new entry next to Client Group.</td>
</tr>
<tr>
<td></td>
<td>3. In the New client-group window, enter the client group.</td>
</tr>
</tbody>
</table>
Table 13: 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 17 on page 57.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.
Table 14: 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 15 on page 55.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 15: Ldap Options Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure lightweight directory</td>
<td>1. Click <strong>Add new entry</strong> next to Profile.</td>
</tr>
<tr>
<td>access protocol options.</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</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>distinguished name (DN) or base DN under which to search for user DN.</td>
</tr>
</tbody>
</table>
Table 15: 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. |

---

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

To configure Lightweight Directory Access Protocol (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 **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.
Table 16: Ldap Server Configuration Details

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

Configuring the Provisioning Order (NSM Procedure)

To configure the provisioning order in NSM:
1. In the NSM navigation tree, select Device Manager > Devices.  
2. Click the Device Tree tab, and then double-click the device to select it.  
3. Click the Configuration tab. In the configuration tree, expand Access.  
4. Select Profile.  
5. Add or modify settings as specified in Table 17 on page 57.  
6. Click one:  
   ■ OK—Saves the changes.  
   ■ Cancel— Cancels the modifications.

Table 17: Provisioning Order Configuration Details

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

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

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

Table 18: 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 for Dynamic Host Configuration Protocol (DHCP), Layer 2 Tunneling Protocol (L2TP), and Point-to-Point Protocol (PPP) clients.</td>
<td>1. Click Attributes next to Radius.</td>
</tr>
<tr>
<td></td>
<td>2. In the Comment box, enter the comment.</td>
</tr>
</tbody>
</table>
### Table 18: Radius Parameter Configuration Details (continued)

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

### Configuring the RADIUS Parameters (NSM Procedure)

#### Task
Configure the options used by RADIUS authentication and accounting servers.

#### Your Action
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 Nas Identifier box, enter a string in the range from 1 to 64 characters.
6. From the Accounting Session Id Format list, select the format the router uses to identify the accounting session. Select one of the following:
   - 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.

#### Task
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.

#### Your Action
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 5VLAN ID field.
7. From the Vlan Width list, select the number of bits in the VLAN ID field.

### Table 18: Radius Parameter Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the options used by RADIUS authentication and accounting</td>
<td>1. Click Options next to Radius.</td>
</tr>
<tr>
<td>servers.</td>
<td>2. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td>3. Select the Ethernet Port Type Virtual check box to specify a port</td>
<td>4. From the Interface Description Format list, select the information that</td>
</tr>
<tr>
<td>type of virtual.</td>
<td>is included in or omitted from the interface description that the router</td>
</tr>
<tr>
<td></td>
<td>passes to RADIUS for inclusion in the RADIUS attribute 87 (NAS-Port-Id).</td>
</tr>
<tr>
<td>4. From the Interface Description Format list, select the information</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td>is included in or omitted from the interface description that the</td>
<td>- sub-interface—To specify the subinterface.</td>
</tr>
<tr>
<td>router passes to RADIUS for inclusion in the RADIUS attribute 87</td>
<td>- adapter—To specify the adapter.</td>
</tr>
<tr>
<td>(NAS-Port-Id).</td>
<td>5. In the Nas Identifier box, enter a string in the range from 1 to 64</td>
</tr>
<tr>
<td></td>
<td>characters.</td>
</tr>
<tr>
<td>6. From the Accounting Session Id Format list, select the format</td>
<td>7. From the Revert Interval list, select the amount of time the router</td>
</tr>
<tr>
<td>the router uses to identify the accounting session. Select one of</td>
<td>waits after a server has become unreachable.</td>
</tr>
<tr>
<td>the following:</td>
<td>- Range: 60 through 4294967295 seconds</td>
</tr>
<tr>
<td>- decimal—To use the decimal format.</td>
<td>- Default: 600 seconds</td>
</tr>
<tr>
<td>- description—To use the generic format, in the form jnpr</td>
<td>8. Select the vlan-nas-port-stacked-format check box to configure RADIUS</td>
</tr>
<tr>
<td>interface-specifier:subscriber-session-id.</td>
<td>attribute 5 (NAS-Port) to include the S-VLAN ID, in addition to the VLAN ID,</td>
</tr>
<tr>
<td></td>
<td>for subscribers on Ethernet interfaces.</td>
</tr>
</tbody>
</table>
5. Add or modify settings as specified in Table 19 on page 61.
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 19: Radius Parameters 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 Options next to Profile.</td>
</tr>
<tr>
<td></td>
<td>3. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. From the Revert Interval list, select the amount of time the router waits after a server has become unreachable. Default: 600 seconds</td>
</tr>
</tbody>
</table>

### 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 20 on page 62.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
### Table 20: Radius Server Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure the RADIUS servers.</td>
<td>Click <strong>Add new entry</strong> next to Profile</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Radius Server</strong> next to Profile.</td>
</tr>
<tr>
<td>3.</td>
<td>In the <strong>Name</strong> box, enter the profile name.</td>
</tr>
<tr>
<td>4.</td>
<td>In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td>5.</td>
<td>From the <strong>Port</strong> list, select the port number on which to contact the RADIUS server. Default: 1812 (as specified in RFC 2865)</td>
</tr>
<tr>
<td>6.</td>
<td>In the <strong>Secret</strong> 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>7.</td>
<td>From the <strong>Timeout</strong> 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>8.</td>
<td>From the <strong>Retry</strong> 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>9.</td>
<td>In the <strong>Source Address</strong> box, enter a valid IPv4 address configured on one of the router interfaces.</td>
</tr>
<tr>
<td>10.</td>
<td>From the <strong>Routing Instance</strong> 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 21 on page 63.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.
Table 21: Session Limit Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the timeout interval.</td>
<td>1. Click <strong>Add new entry</strong> next to Profile.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Session 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>Client Idle Timeout</strong> list, select the time in minutes of idleness after which access is denied.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 255 minutes</td>
</tr>
<tr>
<td></td>
<td>5. From the <strong>Client Session Timeout</strong> list, select the time in minutes since initial access after which access is denied.</td>
</tr>
</tbody>
</table>

Configure a client group.

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Click <strong>Client Group</strong> next to Session Option.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Client Group.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>New client-group</strong> window, enter the client group.</td>
</tr>
</tbody>
</table>

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 22 on page 63.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 22: Access Profile Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the access profile.</td>
<td>1. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Name</strong> box, enter the name of the access profile.</td>
</tr>
</tbody>
</table>

Related Topics

- Configuring Access Profiles for L2TP or PPP Parameters (NSM Procedure) on page 49
- Configuring the RADIUS Parameters (NSM Procedure) on page 60
Chapter 8

Configuring Accounting Options

- Configuring Accounting Options (NSM Procedure) on page 65

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 65
- Configuring a Log File (NSM Procedure) on page 66
- Configuring the Filter Profile (NSM Procedure) on page 67
- Configuring the Interface Profile (NSM Procedure) on page 68
- Configuring the Policy Decision Statistics Profile (NSM Procedure) on page 69
- Configuring the MIB Profile (NSM Procedure) on page 70
- Configuring the Routing Engine Profile (NSM Procedure) on page 71

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 23 on page 66.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
Table 23: 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 24 on page 67.
6. Click one:
   ■ **OK**—Saves the changes.
   ■ **Cancel**—Cancels the modifications.
### Table 24: 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 25 on page 68.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.
Table 25: Filter Profile Configuration Details

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

| 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 26 on page 69.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.
Table 26: Interface Profile Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure an interface profile.</td>
<td>1. Click <strong>Add new entry</strong> next to Interface Profile.</td>
</tr>
<tr>
<td></td>
<td>2. Expand <strong>interface-profile</strong></td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the name of the log file.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment for the interface profile.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>File</strong> box, enter the name of the log file.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Interval</strong> list, select the amount of time between each</td>
</tr>
<tr>
<td></td>
<td>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>
</tbody>
</table>

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**.

4. Select **Policy Decision Statistics Profile**.

5. Add or modify the settings as specified in Table 27 on page 70.

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

### Table 27: 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 28 on page 71.

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

**Table 28: MIB Profile Configuration Details**

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

**Configuring the Routing Engine Profile (NSM Procedure)**

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

To configure the Routing Engine profile in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Accounting Options.
4. Select Routing Engine Profile.
5. Add or modify the settings as specified in Table 29 on page 72.
6. Click one:
- OK—Saves the changes.
- Cancel—Cancels the modifications.

### Table 29: Routing Engine Profile Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Routing Engine profile</td>
<td>1. Click <strong>Add new entry</strong> next to Routing Engine Profile.</td>
</tr>
<tr>
<td></td>
<td>2. Expand <strong>routing-engine-profile</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the name of the Routing Engine statistics profile.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment for the routing engine profile.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>File</strong> box, enter the name of the log file.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Interval</strong> 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>
</tbody>
</table>

| 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 yyyyymmdd 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. |
Configuring Applications

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 30 on page 74.
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 30: 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-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. From the Name list, select the identifier of the application.  
7. In the Comment box, enter the comment. |
Chapter 10
Configuring Bridge Domains

- Configuring Bridge Domains Properties (NSM Procedure) on page 75

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 75
- Configuring Layer 2 Learning and Forwarding Properties for a Bridge Domain (NSM Procedure) on page 76
- Configuring Forwarding Options (NSM Procedure) on page 78
- Configuring Logical Interfaces (NSM Procedure) on page 79
- Configuring Multicast Snooping Options (NSM Procedure) on page 80
- Configuring IGMP Snooping (NSM Procedure) on page 82
- Configuring VLAN ID (NSM Procedure) on page 87

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 31 on page 76.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.
Table 31: 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 Add new entry next to Domain.</td>
</tr>
<tr>
<td></td>
<td>2. Click domain.</td>
</tr>
<tr>
<td></td>
<td>3. In the Name box, enter the name of the bridge domain.</td>
</tr>
<tr>
<td></td>
<td>4. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. In the Description box, enter the text to describe the bridge domain.</td>
</tr>
<tr>
<td></td>
<td>6. From the Domain Type list, select the type of domain for a Layer 2 bridge domain.</td>
</tr>
<tr>
<td></td>
<td>7. Select the No Local Switching check box to enable or disable local switching within customer edge(ce)-facing interfaces.</td>
</tr>
<tr>
<td></td>
<td>8. In the Routing Interface 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 32 on page 77.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
### Table 32: Bridge Options Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure bridge domain. | 1. Click **Add new entry** next to Domain.  
2. Click **Bridge Options**.  
3. Expand **Bridge Options**.  
4. In the **Comment** box, enter the comment.  
5. In the **Mac Table Aging Time** list, select the timeout interval for entries in the MAC table.  
6. Select the **No Mac Learning** check box to disable MAC learning.  
7. Select the **Mac Statistics** 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.  
8. In the **Routing Interface** box, enter the interface name. |
| Specify the logical interfaces to include in the bridge domain. | 1. Click **Interface** next to Bridge Options.  
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. From the **Remote Site Id** list, select the remote site ID.  
6. Select the **No Mac Learning** check box to disable MAC learning.  
7. In the **Description** box, enter the description.  
8. Click **Interface Mac Limit** next to interface.  
9. In the **Comment** box, enter the comment.  
10. From the **Limit** list, select the maximum number of MAC addresses learned from an interface. Range: 1 through 131,071 MAC addresses per interface  
11. From the **Packet Action** list, select the packet action for the packets for new source MAC addresses.  
12. Click **Static Mac** next to interface.  
13. Click **Add new entry** next to Static Mac.  
14. In the **Name** box, enter the interface name.  
15. In the **Comment** box, enter the comment.  
16. Click **Vlan Id** next to static-mac.  
17. Click **Add new entry** next to Vlan ID.  
18. From the **Name** list, select the VLAN identifier to associate with the static MAC address.  
   Range: 1 to 4094  
19. In the **Comment** box, enter the comment.  
| Configure a limit to the number of MAC addresses that can be learned from a bridge domain, virtual switch, or set of bridge domains. | 1. Click **Interface Mac Limit** next to Bridge Options.  
2. In the **Comment** box, enter the comment.  
3. From the **Limit** list, select the maximum number of MAC addresses learned from an interface.  
   Range: 1 through 131,071 MAC addresses per interface |
Table 32: Bridge Options Configuration Details (continued)

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

**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 33 on page 78.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 33: Forwarding Options Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the extended DHCP relay agent.</td>
<td>1. Click <strong>Add new entry</strong> next to Domain.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Forwarding Options</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Expand <strong>Dhcp Relay</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. Select <strong>Authentication</strong>.</td>
</tr>
<tr>
<td></td>
<td>5. For Configuring Authentication Support for the DHCP Relay Agent, see</td>
</tr>
<tr>
<td></td>
<td>“Configuring Authentication Support for the DHCP Relay Agent (NSM Procedure)” on page 183.</td>
</tr>
</tbody>
</table>

| Configuring Group.                                                   | 1. Click **Group** next to Dhcp Relay.                                      |
|                                                                      | 2. For configuring group, see “Configuring Group (NSM Procedure)” on page 184. |

| Overriding the default configuration settings for the extended      | 1. Click **Overrides** next to Dhcp Relay.                                  |
| DHCP relay agent.                                                  | 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 185.                   |
Table 33: Forwarding Options Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configuring relay option 60 information for forwarding client traffic to specific DHCP servers. | 1. Click Relay option 60 next to Dhcp Relay.  
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 186. |
| Configuring relay option 82 for a DHCP server. | 1. Click Relay option 82 next to Dhcp Relay.  
2. For configuring relay option 82 for a DHCP server, see “Configuring Relay Option 82 for a DHCP Server (NSM Procedure)” on page 188. |
| Specifying the name of a group of DHCP server addresses for use by the extended DHCP relay agent. | 1. Click Server Group next to Dhcp Relay.  
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 189. |
| Configuring tracing operations for extended DHCP relay agent processes. | 1. Click Traceoptions next to Dhcp Relay.  
2. For configuring tracing operations for extended DHCP relay agent processes see “Configuring Operations for Extended DHCP Relay Agent Processes (NSM Procedure)” on page 190. |
| Apply a forwarding table filter at the ingress of a forwarding table. | 1. Click Filter next to Forwarding Options.  
2. In the Comment box, enter the comment.  
3. From the Input list, select the name of the applied filter. |
| Apply a forwarding table filter to a flood table. | 1. Click Flood next to Forwarding Options.  
2. In the Comment box, enter the comment.  
3. From the Input list, select the name of the forwarding table filter. |

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 34 on page 80.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
Table 34: 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 Add new entry next to Domain.</td>
</tr>
<tr>
<td></td>
<td>2. Click Interface.</td>
</tr>
<tr>
<td></td>
<td>3. Click Add new entry next to Interface.</td>
</tr>
<tr>
<td></td>
<td>4. From the Name list, select the name of a logical interface.</td>
</tr>
<tr>
<td></td>
<td>5. In the Comment 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 35 on page 81.
6. Click one:
   - OK—saves the changes
   - Cancel—cancels the modifications
<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish multicast snooping option values.</td>
<td>1. Click <strong>Add new entry</strong> next to Domain.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Multicastsnooping Options</strong> next to domain.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Establish a list of flood group addresses for multicast snooping.</td>
<td>1. Click <strong>Flood Groups</strong> next to Multicast Snooping Options.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Flood Groups.</td>
</tr>
<tr>
<td></td>
<td>3. In the dialog box, enter the IP addresses.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure multicast forwarding cache properties.</td>
<td>1. Click <strong>Forwarding Cache</strong> next to Multicast Snooping Options.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comments.</td>
</tr>
<tr>
<td></td>
<td>3. Expand <strong>Forwarding Cache</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Threshold</strong> next to Forwarding Cache.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comments.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Suppress</strong> 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 <strong>Reuse</strong> list, select the reuse value for the threshold. The reuse value must be</td>
</tr>
<tr>
<td></td>
<td>less than the suppression threshold value.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 200,000</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Establish the graceful restart duration for multicast snooping.</td>
<td>1. Click <strong>Graceful Restart</strong> next to Multicast Snooping Options.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comments.</td>
</tr>
<tr>
<td></td>
<td>3. From the <strong>Restart Duration</strong> 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>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Establish multicast snooping option values.</td>
<td>1. Click <strong>Option</strong> next to Multicast Snooping Options.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comments.</td>
</tr>
<tr>
<td></td>
<td>3. Expand <strong>Options</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Syslog</strong> next to Options.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comments.</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Upto</strong> list, select the level up to which severity the messages are to be syslogged.</td>
</tr>
<tr>
<td></td>
<td>7. From the <strong>Mark</strong> list, select the time interval in seconds to mark the trace file.</td>
</tr>
<tr>
<td></td>
<td>Range : -2147483647 seconds to 2147483647 Seconds</td>
</tr>
<tr>
<td></td>
<td>Default : 0</td>
</tr>
<tr>
<td></td>
<td>8. Expand <strong>Syslog</strong>.</td>
</tr>
<tr>
<td></td>
<td>9. Click <strong>Level</strong> next to Syslog.</td>
</tr>
<tr>
<td></td>
<td>10. Select the Level of severity to be logged.</td>
</tr>
</tbody>
</table>
Table 35: Multicast Snooping Options Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure tracing options.</td>
<td>1. Click Traceoptions next to Multicast Snooping Options.</td>
</tr>
<tr>
<td></td>
<td>2. In the Comment box, enter the comments.</td>
</tr>
<tr>
<td></td>
<td>3. Expand Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>4. Click File next to Trace Options.</td>
</tr>
<tr>
<td></td>
<td>5. In the Comment box, enter the comments.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>7. In the Size box, enter the maximum size of each trace file in bytes.</td>
</tr>
<tr>
<td></td>
<td>Range: 10240 to 4294967295 bytes</td>
</tr>
<tr>
<td></td>
<td>8. From the Files list, select the maximum number of files.</td>
</tr>
<tr>
<td></td>
<td>9. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>■ world-readable—To enable log file access to all users.</td>
</tr>
<tr>
<td></td>
<td>■ no-world-readable—To prevent all users from reading the log file.</td>
</tr>
<tr>
<td></td>
<td>10. Click Flag next to Trace Options.</td>
</tr>
<tr>
<td></td>
<td>11. Click Add new entry next to flag.</td>
</tr>
<tr>
<td></td>
<td>12. From the Name list, select a tracing operation to perform.</td>
</tr>
<tr>
<td></td>
<td>13. In the Comment box, enter the comments.</td>
</tr>
</tbody>
</table>

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 36 on page 83.
6. Click one:
   ■ OK—Saves the changes.
   ■ Cancel— Cancels the modifications.
Table 36: Igmp Snooping Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure IGMP snooping</td>
<td>1. Click <strong>Add new entry</strong> next to Domain.</td>
</tr>
<tr>
<td></td>
<td>2. Click and expand <strong>Protocol</strong></td>
</tr>
<tr>
<td></td>
<td>3. Select <strong>Igmp Snooping</strong></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>Query Interval</strong> list, select the time interval the querier router sends general host-query messages.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 1024</td>
</tr>
<tr>
<td></td>
<td>Default: 125 seconds</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Query Response Interval</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 1024</td>
</tr>
<tr>
<td></td>
<td>Default: 10 seconds</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Query Last Member Interval</strong> box, enter the time interval the querier router sends group-specific query messages.</td>
</tr>
<tr>
<td></td>
<td>Range: 0.1 through 0.9, then in 1-second intervals 1 through 1024</td>
</tr>
<tr>
<td></td>
<td>Default: 1 second</td>
</tr>
<tr>
<td></td>
<td>8. From the <strong>Robust Count</strong> list, select the robustness variable used to calculate several IGMP message intervals.</td>
</tr>
<tr>
<td></td>
<td>Range: 2 through 10</td>
</tr>
<tr>
<td></td>
<td>Default: 2</td>
</tr>
<tr>
<td></td>
<td>9. Select the <strong>Immediate Leave</strong> check box to enable immediate leave.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.
Enable IGMP on an interface and configure interface-specific properties.

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

Configuring IGMP snooping proxy mode.

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Click <strong>Proxy</strong> next to Igmp Snooping.</td>
<td>1. Click <strong>Proxy</strong> next to Igmp Snooping.</td>
</tr>
<tr>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td>3. In the <strong>Source Address</strong> box, enter the IP address to use as the source for IGMP snooping reports in proxy mode.</td>
<td>3. In the <strong>Source Address</strong> box, enter the IP address to use as the source for IGMP snooping reports in proxy mode.</td>
</tr>
</tbody>
</table>
Table 36: Igmp Snooping Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure IGMP tracing options</td>
<td>1. In the <strong>Comment</strong> box, enter the comment for the 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 filename.</td>
</tr>
<tr>
<td></td>
<td>4. 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>5. In the <strong>Size</strong> box, enter the maximum trace file size in bytes.</td>
</tr>
<tr>
<td></td>
<td>Range: 10240 to 4294967295</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Files</strong> list, select the maximum number of trace files.</td>
</tr>
<tr>
<td></td>
<td>Range: 2 through 1000 files</td>
</tr>
<tr>
<td></td>
<td>Default: 2 files</td>
</tr>
<tr>
<td></td>
<td>7. 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>8. Click <strong>Flag</strong> next to Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>9. Click <strong>Add new entry</strong> next to Flag.</td>
</tr>
<tr>
<td></td>
<td>10. From the <strong>Name</strong> list, select the flag to perform the trace operation.</td>
</tr>
<tr>
<td></td>
<td>11. In the <strong>Comment</strong> box, enter the comment for the flag.</td>
</tr>
<tr>
<td></td>
<td>12. Select the corresponding flag modifier check box.</td>
</tr>
</tbody>
</table>
### Table 36: 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 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 36: 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 37 on page 88.  
6. Click one:  
   ■ **OK**—Saves the changes.  
   ■ **Cancel**—Cancels the modifications.
### Table 37: 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 <strong>Add new entry</strong> next to Domain.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Vlan Id</strong></td>
</tr>
<tr>
<td></td>
<td>3. Select <strong>vlan-id</strong> and enter the VLAN ID.</td>
</tr>
<tr>
<td></td>
<td>4. Select <strong>vlan tag</strong> 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 <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Inner</strong> box, enter the VLAN identifier.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Outer</strong> box, enter the VLAN identifier.</td>
</tr>
</tbody>
</table>
Chapter 11
Configuring Chassis

- Configuring Aggregated Devices (NSM Procedure) on page 89
- Configuring Chassis Alarms (NSM Procedure) on page 90
- Configuring Container Interfaces (NSM Procedure) on page 91
- Configuring Chassis FPC (NSM Procedure) on page 92
- Configuring a T640 Router on a Routing Matrix (NSM Procedure) on page 98
- Configuring Routing Engine Redundancy (NSM Procedure) on page 104
- Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors (NSM Procedure) on page 106

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 38 on page 90.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
Table 38: 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 System Priority box, enter the priority for the aggregated Ethernet system.  
5. Click Link Protection next to Lacp.  
6. Select the Non Reverting 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 Device Count list, select the number of aggregated logical devices available to the router.  
Range: 1 through 16 Devices |

Related Topics
- Configuring Chassis Alarms (NSM Procedure) on page 90
- Configuring a T640 Router on a Routing Matrix (NSM Procedure) on page 98
- Configuring Routing Engine Redundancy (NSM Procedure) on page 104
- Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors (NSM Procedure) on page 106

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 39 on page 91.
5. Click one:  
   - OK—Saves the changes.  
   - Cancel—Cancels the modifications.
Table 39: 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 89
- Configuring Chassis FPC (NSM Procedure) on page 92
- Configuring Routing Engine Redundancy (NSM Procedure) on page 104

Configuring Container Interfaces (NSM Procedure)

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

To configure container interfaces in NSM:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Chassis.
4. Select Container Devices.
5. Add or modify settings as specified in Table 40 on page 91.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 40: 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 Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>2. From the Device list, select the number of container devices.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 128</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring Aggregated Devices (NSM Procedure) on page 89
- Configuring Chassis FPC (NSM Procedure) on page 92
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 41 on page 92.
5. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

<table>
<thead>
<tr>
<th>Table 41: FPC Configuration Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Task</strong></td>
</tr>
</tbody>
</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 41: FPC Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure 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 Dlcis** check box to support a full data-link connection identifier (DLCI) range (1 through 1022).  
11. From the **Mlfr Uni Nni Bundles** list, select the number of multilink frame relay user-to-network interface network-to-network interface (UNI-NNI) (FRF.16) bundles to allocate on a link services PIC.  
  Range: 1 through 255  
12. From the **Max Queues Per Interface** list, select the required egress queues on IQ interfaces.  

Enable a service package on adaptive services interfaces.  
1. Click **Add new entry** next to Fpc.  
2. Click **Pic** next to fpc.  
3. Click **Add new entry** next to Pic.  
4. Click **Adaptive Services** next to pic.  
5. Select **Adaptive Services** to enable a service package on adaptive services interfaces.
### Table 41: FPC 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. |
Table 41: 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 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.  |
| 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 41: 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 41: 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. |

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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 |

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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. |
Table 41: FPC Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Port-Mirroring Instances.</td>
<td>1. Click Add new entry next to Fpc.</td>
</tr>
<tr>
<td></td>
<td>2. Click Port Mirror Instance next to fpc and perform the following:</td>
</tr>
<tr>
<td></td>
<td>■ Add—Adds the selected port-mirroring instances from the Non member list to the Members list.</td>
</tr>
<tr>
<td></td>
<td>■ Remove—Removes the selected port-mirroring instances from the Members list.</td>
</tr>
<tr>
<td></td>
<td>■ Add All—Adds all the port-mirroring instances from the Non-members list to the Members list.</td>
</tr>
<tr>
<td></td>
<td>■ Remove All—Removes all the port-mirroring instances from the Members list.</td>
</tr>
<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 fpc.</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 89
- Configuring Chassis Alarms (NSM Procedure) on page 90
- Configuring a T640 Router on a Routing Matrix (NSM Procedure) on page 98

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 42 on page 99.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
### Table 42: Lcc Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure the T640 routing node. | 1. Click **Add new entry** next to Lcc.  
2. From the **Name** list, select the number that specifies a T640 router on a routing matrix. Range: 0 through 3  
3. In the **Comment** box, enter the comment.  
4. Select one of the following:  
   - **online-expected**—On a TX Matrix router, configures a T640 router so that if it does not come online, an alarm is sent to the TX Matrix router. On a TX Matrix Plus router, configure a T1600 router so that if it does not come online, an alarm is sent to the TX Matrix Plus router.  
   - **offline**—On a TX Matrix router, configures a T640 router so that it is not part of the routing matrix. On a TX Matrix Plus router, configure a T1600 router so that it is not part of the routing matrix. |
| Configure a port-mirroring instance for the DPC and its corresponding Packet Forwarding Engines. | 1. Click **Fpc** next to Lcc.  
2. Click **Add new entry** next to Fpc.  
3. From the **Name** list, select the slot number of the DPC.  
4. From the **Power** list, configure the Flexible PIC Concentrator (FPC) to stay offline or to come online automatically. |
### Table 42: Lcc Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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 Dlcis** check box to support a full data-link connection identifier (DLCI) range (1 through 1022).  
11. From the **Mlfr Uni Nni Bundles** list, select the number of multilink frame relay user-to-network interface network-to-network interface (UNI-NNI) (FRF.16) bundles to allocate on a Link Services PIC.  
  Range: 1 through 255  
12. From the **Max Queues Per Interface** list, select the required egress queues on IQ interfaces. |

Enable a service package on adaptive services interfaces.  

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 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 42: Lcc Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure channelized E1 port and</strong></td>
<td>1. Click <strong>Add new entry</strong> next to Fpc.</td>
</tr>
<tr>
<td><strong>channel specifications.</strong></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>
<tr>
<td><strong>Configure channelized T3 port and</strong></td>
<td>1. Click <strong>Add new entry</strong> next to Fpc.</td>
</tr>
<tr>
<td><strong>channel specifications.</strong></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>
<tr>
<td><strong>Configure data used in a hash key for</strong></td>
<td>1. Click <strong>Add new entry</strong> next to Fpc.</td>
</tr>
<tr>
<td><strong>a protocol family.</strong></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>Hash Key</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>Family</strong> next to Hash Key.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
</tbody>
</table>
### Table 42: 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 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. |
### Table 42: Lcc Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure delay buffers.</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>Q Pic Large Buffer</strong> next to pic.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td>Configure port-mirroring instances for PIC.</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>Port Mirror Instance</strong> next to pic and perform the following:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Add</strong>—Adds the selected port-mirroring instances from the Non member list to the Members list.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Remove</strong>—Removes the selected port-mirroring instances from the Members list.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Add All</strong>—Adds all the port-mirroring instances from the Non-members list to the Members list.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Remove All</strong>—Removes all the port-mirroring instances from the Members list.</td>
</tr>
<tr>
<td>Enable shaping on an L2TP session.</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>Traffic Manager</strong> next to pic.</td>
</tr>
<tr>
<td></td>
<td>5. From the <strong>Ingress Shaping Overhead</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 255</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Egress Shaping Overhead</strong> list, select the number of CoS shaping overhead bytes to add to the packets on the egress interface.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 255</td>
</tr>
<tr>
<td></td>
<td>7. From the <strong>Mode</strong> list, select the mode of shaping.</td>
</tr>
<tr>
<td>Configure the amount of bandwidth for tunnel services.</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>Tunnel Service</strong> next to pic.</td>
</tr>
<tr>
<td></td>
<td>5. From the <strong>Bandwidth</strong> list, select the bandwidth of 1 Gbps or 10Gbps on the Packet Forwarding Engine connected to a Gigabit Ethernet 40-port DPC.</td>
</tr>
</tbody>
</table>
Table 42: Lcc Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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. |

| Associate a sampling instance. | 1. Click **Add new entry** next to Fpc.  
2. Click **Sampling Instances** next to fpc.  
3. Click **Add new entry** next to Sampling Instances.  
4. From the **Name** list, select the sampling instance name.  
5. In the **Comment** box, enter the comment. |

Related Topics
- Configuring Aggregated Devices (NSM Procedure) on page 89
- Configuring Routing Engine Redundancy (NSM Procedure) on page 104
- Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors (NSM Procedure) on page 106

Configuring Routing Engine Redundancy (NSM Procedure)

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

To configure routing engine redundancy in NSM:
1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, select **Chassis > Redundancy**.
4. Add or modify settings as specified in Table 43 on page 105.
5. Click one:  
  ■ **OK**—Saves the changes.
Table 43: 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 <strong>Redundancy</strong>.</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>
<tr>
<td>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.</td>
<td>1. Click <strong>Graceful Switchover</strong> next to <strong>Redundancy</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td>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.</td>
<td>1. Click <strong>Routing Engine</strong> next to <strong>Redundancy</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. From the <strong>Name</strong> list, select the slot number.</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 function of the Routing Engine for the specified slot.</td>
</tr>
<tr>
<td></td>
<td>5. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>■ master—To configure the routing engine to be the master.</td>
</tr>
<tr>
<td></td>
<td>■ backup—To configure the routing engine to be the backup.</td>
</tr>
<tr>
<td></td>
<td>■ disabled—To disable the routing engine.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Configuring Aggregated Devices (NSM Procedure) on page 89
- Configuring a T640 Router on a Routing Matrix (NSM Procedure) on page 98
- Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors (NSM Procedure) on page 106
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 44 on page 106.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 44: 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 89
- Configuring a T640 Router on a Routing Matrix (NSM Procedure) on page 98
- Configuring Routing Engine Redundancy (NSM Procedure) on page 104
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 45 on page 107.
5. Click one:
   - **New**—Adds a new RADIUS server.
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the IP address of the RADIUS server.</td>
<td>Enter the IP address of the RADIUS server.</td>
</tr>
</tbody>
</table>
### Table 45: 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.</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 108
- Configuring Authentication Order (NSM Procedure) on page 109
- Configuring User Access (NSM Procedure) on page 110

### Configuring TACACS+ Authentication (NSM Procedure)

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

To configure TACACS+ authentication:
1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab and then double-click the device for which you want to configure TACACS+ authentication.
3. Click the **Configuration** tab. In the configuration tree, select **System > TACACS+ Server**.
4. Add or modify TACACS+ settings as specified in Table 46 on page 108.
5. Click one:
   - **New**—Adds a new TACACS+ server.
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

### Table 46: 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 46: 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 107
- Configuring Authentication Order (NSM Procedure) on page 109
- Configuring User Access (NSM Procedure) on page 110

Configuring Authentication Order (NSM Procedure)

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

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

Related Topics
- Configuring RADIUS Authentication (NSM Procedure) on page 107
- Configuring TACACS+ Authentication (NSM Procedure) on page 108
- Configuring User Access (NSM Procedure) on page 110
Configuring User Access (NSM Procedure)

This section includes the following topics:

- Configuring Login Classes on page 110
- Configuring User Accounts on page 111

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 47 on page 110.
5. Click one:
   - New—Adds a new login class.
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 47: Login Class Authentication Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a name for the login class.</td>
<td>Enter a name for the login class.</td>
</tr>
<tr>
<td>Allow Commands</td>
<td>Specifies the operational mode commands that members of a login class can use.</td>
<td>Enter the command name enclosed in quotation marks. For example, “request system reboot”.</td>
</tr>
</tbody>
</table>

Login > Class > Permissions

Permissions | Configures the login access privileges to be provided on the device. | Enter a new permission. |
Configuring User Accounts

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

To configure user accounts:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab and then double-click the device for which you want to configure login class.
3. Click the Configuration tab. In the configuration tree, select System > Login > User.
4. Add or modify login class settings as specified in Table 48 on page 111.
5. Click one:
   - New—Adds a new user account.
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

### Table 48: 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>
</tbody>
</table>

**Login > User > Authentication**

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

### Related Topics
- Configuring RADIUS Authentication (NSM Procedure) on page 107
- Configuring TACACS+ Authentication (NSM Procedure) on page 108
- Configuring Authentication Order (NSM Procedure) on page 109

### Configuring Template Accounts (NSM Procedure)

You can create template accounts that are shared by a set of users when you are using RADIUS or TACACS+ authentication. When a user is authenticated by a
template account, the CLI username is the login name, and the privileges, file ownership, and effective user ID are inherited from the template account.

To configure template accounts, follow these procedures:
- Creating a Remote Template Account on page 112
- Creating a Local Template Account on page 113

**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 49 on page 112.
5. Click one:
   - **New**—Creates a new remote template account.
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

**Table 49: Remote Template Account Details**

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a name for the user name. Enter the user name. For example, type remote.</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 operator.</td>
<td></td>
</tr>
</tbody>
</table>
Creating a Local Template Account

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

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

To create a local template account:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab and then double-click the device for which you want to create a local template account.
3. Click the Configuration tab. In the configuration tree, select System > Login > User.
4. Add or modify login class settings as specified in Table 50 on page 113.
5. Click one:
   - New—Creates a new local template account.
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a name for the user name.</td>
<td>Enter the user name. For example, type admin.</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 superuser.</td>
</tr>
</tbody>
</table>

Related Topics

- Configuring RADIUS Authentication (NSM Procedure) on page 107
- Configuring TACACS+ Authentication (NSM Procedure) on page 108
- Configuring Authentication Order (NSM Procedure) on page 109
Chapter 13
 Configuring Class of Service Features

■ Configuring CoS Classifiers (NSM Procedure) on page 116
■ Configuring CoS Code Point Aliases (NSM Procedure) on page 118
■ Configuring CoS Drop Profile (NSM Procedure) on page 119
■ Configuring CoS Forwarding Classes (NSM Procedure) on page 121
■ Configuring CoS Forwarding Policy (NSM Procedure) on page 123
■ Configuring CoS Fragmentation Maps (NSM Procedure) on page 124
■ Configuring CoS Host Outbound Traffic (NSM Procedure) on page 126
■ Configuring CoS Interfaces (NSM Procedure) on page 127
■ Configuring CoS Routing Instances (NSM Procedure) on page 132
■ Configuring CoS Schedulers (NSM Procedure) on page 134
■ Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 135
■ Configuring CoS Restricted Queues (NSM Procedure) on page 137
■ Configuring Tracing Operations (NSM Procedure) on page 138
■ Configuring CoS Traffic Control Profiles (NSM Procedure) on page 139
■ Configuring CoS Translation Table (NSM Procedure) on page 141
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 51 on page 116.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

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

<table>
<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 51: Configuring and Applying Behavior Aggregate Classifiers (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
</table>
| **Configure a best-effort forwarding class classifier.** | 1. Click **Add new entry** next to Forwarding class.  
2. In the Class name box, type the name of the previously configured best-effort forwarding class—for example, **be-class**.  
3. Click **Add new entry** next to Loss priority.  
4. From the Loss val list, select **high**.  
5. Click **Add new entry** next to Code points.  
6. In the Value box, type the value of the high-priority code point for best-effort traffic—for example, **00001**.  
7. Click **OK** three times. |

| Configure an expedited forwarding class classifier. | 1. Click **Add new entry** next to Forwarding class.  
2. In the Class name box, type the name of the previously configured expedited forwarding—for example, **class-ef-class**.  
3. Click **Add new entry** next to Loss priority.  
4. From the Loss val list, select **high**.  
5. Click **Add new entry** next to Code points.  
6. In the Value box, type the value of the high-priority code point for expedited forwarding traffic—for example, **101111**.  
7. Click **OK** three times. |

| Configure an assured forwarding class classifier. | 1. Click **Add new entry** next to Forwarding class.  
2. In the Class name box, type the name of the previously configured assured forwarding—for example, **class-af-class**.  
3. Click **Add new entry** next to Loss priority.  
4. From the Loss val list, select **high**.  
5. Click **Add new entry** next to Code points.  
6. In the Value box, type the value of the high-priority code point for assured forwarding traffic—for example, **001100**.  
7. Click **OK** three times. |

| Apply the behavior aggregate classifier to an interface. | 1. Click **Add new entry** next to Interfaces.  
2. In the Interface name box, type the name of the interface—for example, **ge-0/0/0**.  
3. Click **Add new entry** next to Unit.  
4. In the Unit number box, type the logical interface unit number—for example, **0**.  
5. Click **Configure** next to Classifiers.  
6. In the Classifiers box, under Dscp, type the name of the previously configured behavior aggregate classifier—for example, **ba-classifier**.  
7. Click **OK**. |
Related Topics

- Configuring CoS Code Point Aliases (NSM Procedure) on page 118
- Configuring CoS Drop Profile (NSM Procedure) on page 119
- Configuring CoS Forwarding Classes (NSM Procedure) on page 121
- Configuring CoS Interfaces (NSM Procedure) on page 127
- Configuring CoS Rewrite Rules (NSM Procedure)
- Configuring CoS Schedulers (NSM Procedure) on page 134
- Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 135

Configuring CoS Code Point Aliases (NSM Procedure)

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

To configure code-point aliases:

1. In the navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device for which you want to configure CoS code point aliases.
3. Click the Configuration tab. In the configuration tree, expand Class of Service.
4. Select Code Point Aliases.
5. Add or modify the settings as specified in Table 52 on page 119
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the Network and Security Manager Administration Guide for more information.
## 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 116
- Configuring CoS Drop Profile (NSM Procedure) on page 119
- Configuring CoS Forwarding Classes (NSM Procedure) on page 121
- Configuring CoS Interfaces (NSM Procedure) on page 127
- Configuring CoS Rewrite Rules (NSM Procedure)
- Configuring CoS Schedulers (NSM Procedure) on page 134
- Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 135

---

**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 53 on page 120.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

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

### Table 53: Drop Profile Configuration Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Drop Profile | **Name**                                | 1. Click the **New** button or **Edit** button in the Drop Profile interface.  
                                                          2. Enter the drop profile name in the Name box. |
|              | **Comment**                             | 1. Click the **New** button or **Edit** button in the Drop Profile interface.  
                                                          2. Enter the comment for the drop profile in the Comment box. |
| Fill Level   | **Name**                                | 1. On Drop Profile interface click the **New** button or select a profile and  
                                                          click the **Edit** button.  
                                                          2. Expand the Drop Profile tree and select Fill Level.  
                                                          3. Click the **New** button or select a fill level and click the **Edit** button.  
                                                          4. Select a value from Name list. |
Table 53: Drop Profile 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 the fill level</td>
<td>1. On the Drop Profile interface click the <strong>New</strong> button or select a profile and click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Expand the Drop Profile tree and select Fill Level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click the <strong>New</strong> button or select a fill level and click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Enter a comment in the Comment box.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Configuring CoS Classifiers (NSM Procedure) on page 116
- Configuring CoS Code Point Aliases (NSM Procedure) on page 118
- Configuring CoS Forwarding Classes (NSM Procedure) on page 121
- Configuring CoS Interfaces (NSM Procedure) on page 127
- Configuring CoS Rewrite Rules (NSM Procedure)
- Configuring CoS Schedulers (NSM Procedure) on page 134
- Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 135

### 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 54 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 54: Assigning Forwarding Classes to Output Queues

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign best-effort traffic to queue 0.</td>
<td>1. Select <strong>Queue</strong> and click <strong>Add new entry</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the Queue num box, type <strong>0</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. In the Class name box, type the previously configured name of the best-effort class—for example, <strong>be-class</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong></td>
</tr>
<tr>
<td>Assign expedited forwarding traffic to queue 1.</td>
<td>1. Select <strong>Queue</strong> and click <strong>Add new entry</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the Queue num box, type <strong>1</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. In the Class name box, type the previously configured name of the expedited forwarding class—for example, <strong>ef-class</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong></td>
</tr>
<tr>
<td>Configure an assured forwarding class classifier.</td>
<td>1. Select <strong>Queue</strong> and click <strong>Add new entry</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the Queue num box, type <strong>3</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. In the Class name box, type the previously configured name of the assured forwarding class—for example, <strong>af-class</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong></td>
</tr>
</tbody>
</table>

**Related Topics**

- Configuring CoS Classifiers (NSM Procedure) on page 116
- Configuring CoS Code Point Aliases (NSM Procedure) on page 118
- Configuring CoS Drop Profile (NSM Procedure) on page 119
- Configuring CoS Interfaces (NSM Procedure) on page 127
- Configuring CoS Rewrite Rules (NSM Procedure)
- Configuring CoS Schedulers (NSM Procedure) on page 134
- Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 135
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 55 on page 123.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

### Table 55: 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 55: Forwarding Policy Configuration Details (continued)

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

Related Topics
- Configuring CoS Classifiers (NSM Procedure) on page 116
- Configuring CoS Routing Instances (NSM Procedure) on page 132
- Configuring Tracing Operations (NSM Procedure) on page 138

**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 56 on page 125.

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

### Table 56: Fragmentation Maps Configuration Details

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

| Set the fragmentation threshold for an individual forwarding class for only AS PIC link services | IQ interfaces (lsq). | 1. Click **Add new entry** next to Fragmentation Maps.<br>2. Click **Forwarding Class** next to fragmentation-maps.<br>3. Click **Add new entry** next to Forwarding Class.<br>4. Click **Fragment Threshold** next to forwarding-class.<br>5. Set the fragmentation threshold for an individual forwarding class.<br>   Range: 64 through 9192 bytes |

**Related Topics**

- Configuring CoS Forwarding Policy (NSM Procedure) on page 123
- Configuring CoS Schedulers (NSM Procedure) on page 134
Configuring CoS Traffic Control Profiles (NSM Procedure) on page 139

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 57 on page 126.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 57: 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 121
- Configuring CoS Fragmentation Maps (NSM Procedure) on page 124
- Configuring CoS Traffic Control Profiles (NSM Procedure) on page 139
- Configuring CoS Interfaces (NSM Procedure) on page 127
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 58 on page 127.
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>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td></td>
<td></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>Comment</td>
<td>Specifies the comment for the interface.</td>
<td>2. Click the New button or select an interface and click the Edit button in Interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the interface name in the Name box</td>
</tr>
</tbody>
</table>

Table 58: Interfaces Configuration Fields
### Table 58: Interfaces Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Scheduler Map           | Specifies the scheduler configuration mapped to the forwarding class.     | 1. Expand the **Interfaces** tree and select **Interface**.  
2. Click the **New** button or select an interface and click the **Edit** button in **Interface**.  
3. Select the scheduler map from the list. |
| Scheduler Map Chassis   | Specifies the scheduler configuration mapped to the forwarding class for the particular chassis in the chassis queue. | 1. Expand the **Interfaces** tree and select **Interface**.  
2. Click the **New** button or select an interface and click the **Edit** button in **Interface**.  
3. Select the scheduler map chassis from the list. |
| Input Traffic Control Profile | Applies an input traffic scheduling and shaping profile to the logical interface. | 1. Click the **New** button or select an interface and click the **Edit** button in **Interface**.  
2. Expand the **Interface** tree and select **Input Traffic Control Profile**.  
3. Specify a comment and the profile name.  
4. Click **Ok**. |
| Input Traffic Control Profile Remaining | Applies an input traffic scheduling and shaping profile for remaining traffic to the logical interface. | 1. Click the **New** button or select an interface and click the **Edit** button in **Interface**.  
2. Expand the **Interface** tree and select **Input Traffic Control Profile Remaining**.  
3. Specify a comment and a profile name.  
4. Click **Ok**. |
| Output Traffic Control Profile | Applies an output traffic scheduling and shaping profile to the logical interface. | 1. Click the **New** button or select an interface and click the **Edit** button in **Interface**.  
2. Expand the **Interface** tree and select **Output Traffic Control Profile**.  
3. Specify a comment and a profile name.  
4. Click **Ok**. |
### Table 58: Interfaces Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output Traffic Control Profile Remaining</td>
<td>Applies an output traffic scheduling and shaping profile for remaining traffic to the logical interface.</td>
<td>1. 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 <strong>Interface</strong> 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>
<tr>
<td>Shaping Rate</td>
<td>Shapes the output of the physical interface, so that the interface transmits less traffic than it is physically capable of carrying.</td>
<td>1. Click the <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 <strong>Interface</strong> tree and select <strong>Shaping Rate</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the comment and the rate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click <strong>Ok</strong>.</td>
</tr>
<tr>
<td>Unit</td>
<td>Sets the units that need to be allocated to the specific forwarding class and scheduling map.</td>
<td>1. Click the <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in Interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Expand <strong>Interface</strong> tree and select <strong>Unit</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the Unit, Classifiers, Output Traffic Control Profile and Shaping Rate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click <strong>Ok</strong>.</td>
</tr>
<tr>
<td>Interface Set</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the interface set name.</td>
<td>1. Expand the <strong>Interfaces</strong> tree and select <strong>Interface Set</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the <strong>New</strong> button or select an interface set and click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Select the name from the list.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for the interface.</td>
<td>1. Expand the <strong>Interfaces</strong> tree and select <strong>Interface Set</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the <strong>New</strong> button or select an interface set and click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the comment.</td>
</tr>
<tr>
<td>Option</td>
<td>Function</td>
<td>Your Action</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</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 58: Interfaces Configuration Fields (continued)

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

**Related Topics**
- Configuring CoS Classifiers (NSM Procedure) on page 116
- Configuring CoS Code Point Aliases (NSM Procedure) on page 118
- Configuring CoS Drop Profile (NSM Procedure) on page 119
- Configuring CoS Forwarding Classes (NSM Procedure) on page 121
- Configuring CoS Rewrite Rules (NSM Procedure)
Configuring CoS Routing Instances (NSM Procedure)

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

To configure Class-of-Service routing instances in NSM:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Class of Service.
4. Select Routing Instances.
5. Add or modify settings as specified in Table 59 on page 132.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

Table 59: Routing Instances Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply a custom MPLS EXP classifier to the routing instance for routing instances with VRF table labels enabled.</td>
<td>1. Click Add new entry next to Routing Instances.</td>
</tr>
<tr>
<td></td>
<td>2. In the Name box, enter the name of the routing instance.</td>
</tr>
</tbody>
</table>
Table 59: Routing Instances Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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. |

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 116
- Configuring CoS Forwarding Policy (NSM Procedure) on page 123
- Configuring CoS Restricted Queues (NSM Procedure) on page 137
- Configuring Tracing Operations (NSM Procedure) on page 138
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 60 on page 134.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

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

Table 60: Configuring Schedulers

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the buffer size.</td>
<td>1. Click the Add New icon.</td>
</tr>
<tr>
<td></td>
<td>2. Expand Buffer Size.</td>
</tr>
<tr>
<td></td>
<td>3. Select Percent.</td>
</tr>
<tr>
<td></td>
<td>4. Under Percent, select the appropriate option:</td>
</tr>
<tr>
<td></td>
<td>■ To specify no buffer size, select None.</td>
</tr>
<tr>
<td></td>
<td>■ To specify buffer size as a percentage of the total buffer, select percent and type an integer from 1 through 100.</td>
</tr>
<tr>
<td></td>
<td>■ To specify buffer size as the remaining available buffer, select remainder.</td>
</tr>
<tr>
<td></td>
<td>5. Click OK</td>
</tr>
</tbody>
</table>
Table 60: Configuring Schedulers (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure drop profile map</td>
<td>1. Click the Add New icon.</td>
</tr>
<tr>
<td></td>
<td>2. Select drop-profile-map.</td>
</tr>
<tr>
<td></td>
<td>3. In the Loss Priority box, select the required loss priority—for example, high.</td>
</tr>
<tr>
<td></td>
<td>4. In the Protocol box, select the type of protocol—for example, any.</td>
</tr>
<tr>
<td></td>
<td>5. In the Drop Profile box, select the previously configured drop profile.</td>
</tr>
<tr>
<td></td>
<td>6. Click OK.</td>
</tr>
</tbody>
</table>

Specify the transmit rate. 1. Click the Add New icon. 2. Expand Transmit Rate. 3. Select Rate. 4. Under Rate, select the appropriate option:

- To not specify transmit rate, select None.
- To enforce a specific transmission rate, select rate and type the transmission rate that you want to enforce.
- To specify a percentage of transmission capacity, select percent and type an integer from 1 through 100.
- To specify the remaining transmission capacity, select remainder. 5. Click OK.

Related Topics
- Configuring CoS Classifiers (NSM Procedure) on page 116
- Configuring CoS Code Point Aliases (NSM Procedure) on page 118
- Configuring CoS Drop Profile (NSM Procedure) on page 119
- Configuring CoS Forwarding Classes (NSM Procedure) on page 121
- Configuring CoS Interfaces (NSM Procedure) on page 127
- Configuring CoS Rewrite Rules (NSM Procedure)
- Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 135

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 61 on page 136.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

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

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a scheduler map for DiffServ CoS</td>
<td>1. Click <strong>Add new entry</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the Name box, type the name of the scheduler map—for example, diffserv-cos-map</td>
</tr>
<tr>
<td>Configure a best-effort forwarding class and scheduler</td>
<td>1. Select <strong>Forwarding Class</strong> and click <strong>Add new entry</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the Name box, type the name of the previously configured best-effort forwarding class—for example, be-class.</td>
</tr>
<tr>
<td></td>
<td>3. Select the previously configured best-effort scheduler—for example, be-scheduler.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong></td>
</tr>
<tr>
<td>Configure an expedited forwarding class and scheduler</td>
<td>1. Select <strong>Forwarding Class</strong> and click <strong>Add new entry</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the Name box, type the name of the previously configured expedited forwarding class—for example, ef-class.</td>
</tr>
<tr>
<td></td>
<td>3. Select the previously configured expedited forwarding scheduler—for example, ef-scheduler.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong></td>
</tr>
<tr>
<td>Configure an assured forwarding class and scheduler</td>
<td>1. Select <strong>Forwarding Class</strong> and click <strong>Add new entry</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the Name box, type the name of the previously configured assured forwarding class—for example, af-class.</td>
</tr>
<tr>
<td></td>
<td>3. Select the previously configured assured forwarding scheduler—for example, af-scheduler.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong></td>
</tr>
</tbody>
</table>
Table 61: Assigning Forwarding Classes to Output Queues (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply the scheduler map to an interface.</td>
<td>1. Select Interfaces &gt; Interface and click Add new entry.  &lt;br&gt;2. In the Interface name box, type the name of the interface—for example, ge-0/0/0.  &lt;br&gt;3. Select Unit and click Add new entry.  &lt;br&gt;4. In the Unit name box, select the logical interface unit number—for example, 0.  &lt;br&gt;5. In the Scheduler map box, type the name of the previously configured scheduler map—for example, diffserv-cos-map.  &lt;br&gt;6. Click OK.</td>
</tr>
</tbody>
</table>

Related Topics

- Configuring CoS Classifiers (NSM Procedure) on page 116
- Configuring CoS Code Point Aliases (NSM Procedure) on page 118
- Configuring CoS Drop Profile (NSM Procedure) on page 119
- Configuring CoS Forwarding Classes (NSM Procedure) on page 121
- Configuring CoS Interfaces (NSM Procedure) on page 127
- Configuring CoS Rewrite Rules (NSM Procedure)
- Configuring CoS Schedulers (NSM Procedure) on page 134

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 62 on page 137.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 62: 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>
Table 62: Restricted Queue Configuration Details (continued)

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

Related Topics
- Configuring CoS Classifiers (NSM Procedure) on page 116
- Configuring CoS Forwarding Policy (NSM Procedure) on page 123
- Configuring CoS Translation Table (NSM Procedure) on page 141
- Configuring Tracing Operations (NSM Procedure) on page 138

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 63 on page 138.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 63: Traceoptions Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure tracing operations.</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>
</tbody>
</table>
Table 63: Traceoptions Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task Description</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the name of the file to receive the output of the tracing operation</td>
<td>1. Click <strong>File</strong> next to Traceoptions.</td>
</tr>
<tr>
<td>and specifies the maximum number of trace files.</td>
<td>2. In the <strong>Comment</strong> box, enter the comment for the file.</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>of the tracing operation.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Size</strong> box, enter the maximum size of each trace file, in</td>
</tr>
<tr>
<td></td>
<td>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 <strong>world-readable</strong> to enable unrestricted file access.</td>
</tr>
<tr>
<td></td>
<td>7. Select <strong>no-world-readable</strong> to restrict file access to owner. This is</td>
</tr>
<tr>
<td></td>
<td>the default setting</td>
</tr>
<tr>
<td></td>
<td>8. In the <strong>Match</strong> box, enter the regular expression.</td>
</tr>
<tr>
<td>Specifies the tracing operation to perform. To specify more than one tracing</td>
<td>1. Click <strong>Flag</strong> next to Traceoptions.</td>
</tr>
<tr>
<td>operation, include multiple flag statements.</td>
<td>2. Click <strong>Add new entry</strong> next to Flag.</td>
</tr>
<tr>
<td></td>
<td>3. From the <strong>Name</strong> list, select the flag.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Comment</strong> box, enter the comment for the flag.</td>
</tr>
</tbody>
</table>

Related Topics

- Configuring CoS Rewrite Rules (NSM Procedure)
- Configuring CoS Routing Instances (NSM Procedure) on page 132
- Configuring CoS Restricted Queues (NSM Procedure) on page 137
- Configuring CoS Traffic Control Profiles (NSM Procedure) on page 139

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

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

To configure CoS Traffic Control Profiles in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure CoS Restricted Queues.
3. Click the **Configuration** tab. In the configuration tree, expand **Class of Service**.
4. Select **Traffic Control Profiles**.
5. Add or modify settings as specified in Table 64 on page 140.

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

### Table 64: 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 119
- Configuring CoS Host Outbound Traffic (NSM Procedure) on page 126
- Configuring CoS Routing Instances (NSM Procedure) on page 132
- Configuring CoS Translation Table (NSM Procedure) on page 141
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 65 on page 142.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
### Table 65: 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 65: 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 65: 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 65: 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 132  
- Configuring Tracing Operations (NSM Procedure) on page 138  
- Configuring CoS Traffic Control Profiles (NSM Procedure) on page 139
Chapter 14
Configuring Event Options

- Configuring Destinations for File Archiving (NSM Procedure) on page 147
- Configuring Event Script (NSM Procedure) on page 148
- Generating Internal Events (NSM Procedure) on page 150
- Configuring Event Policy (NSM Procedure) on page 151
- Configuring Event Policy Tracing Operations (NSM Procedure) on page 154

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 66 on page 147.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 66: 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 148
- Generating Internal Events (NSM Procedure) on page 150
- Configuring Event Policy (NSM Procedure) on page 151
- Configuring Event Policy Tracing Operations (NSM Procedure) on page 154

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 67 on page 149.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
### Table 67: Event Script Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Specify the name of an Extensible Stylesheet Language Transformations (XSLT) or Stylesheet Language Alternative Syntax (SLAX) file containing an event script. | 1. Click **File** next to Event Script.  
2. Click **Add new entry** next to File.  
3. In the **Name** box, enter the filename.  
4. In the **Comment** box, enter the comment. |
| Calculate the checksum.                                              | 1. Click **Checksum** next to file.  
2. In the **Comment** box, enter the comment.  
3. In the **Md5** box, enter the MD5 checksum.  
4. In the **Sha1** box, enter the SHA-1 checksum.  
5. In the **Sha 256** box, enter the SHA-256 checksum. |
| Configure the username and passphrase for a remote machine.          | 1. Click **Remote Execution** next to file.  
2. Click **Add new entry** next to Remote Execution.  
3. In the **Name** box, enter the filename.  
4. In the **Comment** box, enter the comment.  
5. In the **Username** box, enter the username for the remote machine.  
6. In the **Passphrase** box, enter the passphrase for the remote machine. |
| Define tracing operations for event scripts.                        | 1. Click **Traceoptions** next to Event Script.  
2. In the **Comment** box, enter the comment.  
3. Expand traceoptions.  
4. Click **File** next to Traceoptions.  
5. In the **Comment** box, enter the comment.  
6. In the **Filename** box, enter the name of the file to receive the output of the tracing operation.  
7. In the **Size** box, enter the maximum trace file size.  
8. From the **Files** list, select the maximum number of trace files.  
9. Select one of the following:  
   - **no-world-readable**—To restrict the file access to owner.  
   - **world-readable**—To enable unrestricted access.  
10. Click **Flag** next to traceoptions.  
11. Click **Add new entry** next to Flag.  
12. From the **Name** list, select the flag to perform the trace operation.  
13. In the **Comment** box, enter the comment for the flag. |
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 68 on page 150.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Generate an internal event, based on a time interval or the time of day. | 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. |
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 68 on page 150.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 69: Generate Event Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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. |
| 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. |
| 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. |
### Table 69: Generate Event Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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. |
| Specify operational mode commands to be issued, the format of the command output, and a name and destination for the output file. | 1. Expand **Then** and select **Event Script**.  
2. Click **Add new entry** next to **Event Script**.  
3. In the **Name** box, enter the filename.  
4. In the **comment** box, enter the comment for the event script.  
5. From the **Username** list, select the user associated with an action in an event policy.  
6. In the **Output Filename** box, enter the filename to which to write command or script output for the specified commands or script.  
7. From the **Output Format** list, select the format for the output of the specified commands. |
Table 69: Generate Event Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include command-line arguments to the script for JUNOS op scripts</td>
<td>1. Expand <code>event-script</code>.</td>
</tr>
<tr>
<td>and assign a location to which to upload command or script output</td>
<td>2. Click <code>Arguments</code> next to <code>event-script</code>.</td>
</tr>
<tr>
<td>for the specified policy.</td>
<td>3. Click <code>Add new entry</code> next to <code>Arguments</code>.</td>
</tr>
<tr>
<td></td>
<td>4. In the <code>Name</code> box, enter the arguments to the script as name.</td>
</tr>
<tr>
<td></td>
<td>5. In the <code>comment</code> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. In the <code>Value</code> box, enter the variables in the argument values to</td>
</tr>
<tr>
<td></td>
<td>allow data from the triggering event to be automatically included in</td>
</tr>
<tr>
<td></td>
<td>the argument.</td>
</tr>
<tr>
<td></td>
<td>7. Click <code>Destination</code> next to <code>event-script</code>.</td>
</tr>
<tr>
<td></td>
<td>8. From the <code>Name</code> list, select the location to which to upload command</td>
</tr>
<tr>
<td></td>
<td>or script output for the specified policy.</td>
</tr>
<tr>
<td></td>
<td>9. In the <code>Comment</code> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>10. From the <code>Transfer Delay</code> list, select the delay in seconds before</td>
</tr>
<tr>
<td></td>
<td>transferring files.</td>
</tr>
<tr>
<td></td>
<td>11. Expand <code>Destinations</code> and select <code>Retry Count</code> next to it.</td>
</tr>
<tr>
<td></td>
<td>12. In the <code>Comment</code> box, enter the comment for the retry count.</td>
</tr>
<tr>
<td></td>
<td>13. From the <code>Retry</code> list, select the number of retries.</td>
</tr>
<tr>
<td></td>
<td>14. From the <code>Retry Interval</code> list, select the length of time to wait</td>
</tr>
<tr>
<td></td>
<td>between retries.</td>
</tr>
</tbody>
</table>

Specify operational mode commands to be issued, the format of the command output, and a name and destination for the output file on receipt of an event.

1. Expand `Execute Commands`.                                        
2. Click `Commands`.                                                   
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 event.

1. Click `Upload` next to `Event Script`.                              
2. In the `Filename` box, enter the name of the file to be uploaded.   
3. From the `Destination` list, select the name of a destination.      
4. From the `User Name` list, select the username.                     
5. From the `transfer relay` list, select the delay before transferring files.
Table 69: Generate Event Details (continued)

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

Related Topics
- Configuring Destinations for File Archiving (NSM Procedure) on page 147
- Configuring Event Script (NSM Procedure) on page 148
- Generating Internal Events (NSM Procedure) on page 150
- Configuring Event Policy Tracing Operations (NSM Procedure) on page 154

Configuring Event Policy Tracing Operations (NSM Procedure)

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

To configure event policy tracing operations in NSM:
1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Event Options**.
4. Select **Traceoptions**.
5. Add or modify settings as specified in Table 70 on page 155.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

### Table 70: Event Options Traceoptions Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Define tracing operations for event policy. | 1. In the **Comment** box, enter the comment for the traceoptions.  
2. Select the **No Remote Trace** check box to disable remote tracing globally or for a specific tracing operation. |
| Specify the name of the file to receive the output of the tracing operation and the maximum number of trace files. | 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.  
7. In the **Match** box, enter the regular expression. |
| 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. |
Related Topics

- Configuring Destinations for File Archiving (NSM Procedure) on page 147
- Configuring Event Script (NSM Procedure) on page 148
- Generating Internal Events (NSM Procedure) on page 150
- Configuring Event Policy (NSM Procedure) on page 151
Chapter 15
Configuring Firewall

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

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

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

To configure firewall filter in NSM:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Firewall > Family > Any.
4. Add or modify settings as specified in Table 71 on page 158.
5. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.
### Table 71: Firewall Filter Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure firewall filters for protocol-independent match conditions. | 1. Expand Any.  
2. In the Comment box, enter the comment for Any.  
3. Click Filter next to Any.  
4. Click Add new entry next to Filter.  
5. In the name box, enter the name that identifies the filter.  
6. In the Comment box, enter the comment for the filter.  
7. Expand Filter.  
8. Click Term next to Filter.  
9. Click Add new entry next to Term.  
10. Expand Term.  
11. In the Name box, enter the name that identifies the term.  
12. In the Comment box, enter the comment for the term.  
13. Expand From.  
14. From the listed protocol-independent match conditions, select the filters defined for the any family type.  
The protocol-independent match conditions are Forwarding Class, Interface, Interface Set, Loss Priority, and Packet Length.  
15. Expand Then.  
16. In the Comment box, enter the comment for then.  
17. In the Count box, enter the number of packets.  
18. From the Loss Priority list, set the packet loss priority (PLP) to low, medium-low, medium-high, or high.  
19. In the Forwarding Class box, enter the packet forwarding class name.  
20. Click Accept next to Then.  
21. Select one of the following:  
   - Accept—To accept a packet.  
   - Discard—To discard a packet silently, without sending an ICMP message.  
   - Next—To evaluate the next term in the firewall filter.  
22. Click Policer next to Then.  
23. Select one of the following:  
   - 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.  
     a. Select single-rate if the named tricolor policer is a single-rate policer.  
     b. Select 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 159  
- Configuring the Firewall Filter for Ccc Family Type (NSM Procedure) on page 161  
- Configuring Filters for inet Family Type (NSM Procedure) on page 163
Configuring the Firewall Filter for Bridge Family Type (NSM Procedure)

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

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Firewall > Family > Bridge.
4. Add or modify settings as specified in Table 72 on page 159.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 72: Bridge Filter Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure firewall filters for Layer 2 packets that are part of bridging domain for MX series routers.</td>
<td>1. Click Filter next to Bridge. &lt;br&gt;2. Click Add new entry next to Filter. &lt;br&gt;3. Expand Filter. &lt;br&gt;4. In the name box, enter the name that identifies the filter. &lt;br&gt;5. In the Comment box, enter the comment. &lt;br&gt;6. Select Interface Specific to configure interface-specific names for firewall counters.</td>
</tr>
<tr>
<td>Configure accounting for firewall filter.</td>
<td>1. Click Accounting Profile next to filter. &lt;br&gt;2. In the New accounting-profile window, enter the name to be assigned to the accounting profile.</td>
</tr>
</tbody>
</table>
Table 72: 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.  
   ■ Select **Policer** to configure a new policer for each filter and select the policer name.  
   ■ Select **three-color-policer** to configure a tricolor marking policer,  
   ▪ Expand **Three Color Policer**.  
   ▪ Click **Single Rate** next to Three Color Policer.  
     ■ Select **single-rate** if the named tricolor policer is a single-rate policer.  
     ■ Select **two-rate** if the named tricolor policer is a two-rate policer.   

Related Topics  
■ Configuring the Firewall Filter for Any Family Type (NSM Procedure) on page 157  
■ Configuring the Firewall Filter for Ccc Family Type (NSM Procedure) on page 161  
■ Configuring Filters for inet Family Type (NSM Procedure) on page 163  
■ Configuring Filters for inet6 Family Type (NSM Procedure) on page 168  
■ Configuring the Firewall Filter for MPLS Family Type (NSM Procedure) on page 172
Configuring the Firewall Filter for Ccc Family Type (NSM Procedure)

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

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Firewall > Family > Ccc.
4. Add or modify settings as specified in Table 73 on page 161.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 73: 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 73: 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 Policier**.  
     b. Click **Single Rate** next to Three Color Policier.  
     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 159  
- Configuring the Firewall Filter for MPLS Family Type (NSM Procedure) on page 172  
- Configuring the Firewall Filter for VPLS Family Type (NSM Procedure) on page 175
Configuring Filters for inet Family Type (NSM Procedure)

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

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

Configuring Firewall Filter for inet Family Type (NSM Procedure)

You can configure a firewall filter for inet family type.

To configure the firewall filter in NSM:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Firewall > Family > Inet.
4. Select Filter.
5. Add or modify settings as specified in Table 74 on page 163.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

Table 74: 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 74: 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 Is Fragment check box if the packet is a trailing fragment.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>10. Select the First Fragment check box if it matches the first fragment of a fragmented packet.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>11. In the Fragment Flags box, enter the IP fragmentation flags.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>12. 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>13. 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>14. In the Tcp Flags box, enter the TCP flags.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>15. 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, 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>Define firewall filter term.</td>
<td>16. Expand Then.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>17. In the Comment box, enter the comment for then.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>18. In the Count box, enter the number of packets.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>19. 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>20. Select Syslog to log an alert for the packet.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>21. Select the Sample check box to sample the packet traffic.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>22. Select the Port Mirror check box to port-mirror the packets.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>23. 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>24. In the Forwarding Class box, enter the packet forwarding class name.</td>
</tr>
<tr>
<td>Define firewall filter term.</td>
<td>25. From the Prefix Action list, select the prefix specific action.</td>
</tr>
</tbody>
</table>
### Table 74: Firewall Filter Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 26. | 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.  
   - Select **Routing instance** to specify a routing table to which packets are forwarded.  
   - Select **IPsec Sa** to specify an IP Security (IPsec) security association (SA) for the packet.  
   - Select **Reject** to discard a packet, and send an ICMP destination unreachable message. |
| 27. | Click **Policer** next to Then.  
  28. Select one of the following:  
   - Select **Policer** to configure a new policer for each filter and select the policer name.  
   - Select **three-color-policer** to configure a tricolor marking policer,  
     a. Expand **Three Color Policier**.  
     b. Click **Single Rate** next to Three Color Policier.  
     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. |

---

**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 75 on page 166.
6. Click one:  
   - **OK**—Saves the changes.  
   - **Cancel**— Cancels the modifications.
Table 75: Prefix Actions Details

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

Configuring Service Filters (NSM Procedure)

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

To configure the service filters for inet in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Firewall > Family > Inet.
4. Click Prefix Action.
5. Add or modify settings as specified in Table 76 on page 166.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 76: Service Filter Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure service filter. | 1. Click Service Filter next to Inet.  
2. Click Add new entry next to Service Filter.  
3. Expand service-filter.  
4. In the Name box, enter the name that identifies the service filter. |
Table 76: 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 77 on page 168.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

### Table 77: 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 Simple Filter next to Inet.</td>
</tr>
<tr>
<td></td>
<td>2. Click Add new entry next to Simple Filter.</td>
</tr>
<tr>
<td></td>
<td>3. In the Name box, enter the name that identifies the simple filter.</td>
</tr>
</tbody>
</table>

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

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

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

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

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

To configure the firewall filter in NSM:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Firewall > Family > Inet6.
4. Add or modify settings as specified in Table 78 on page 169.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 78: Inet6 Firewall Filter Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure firewall filter to filter IPv6 packets. | 1. Click Filter next to Inet6.  
2. Click Add new entry next to Filter.  
3. Expand Filter.  
4. In the Name box, enter the name that identifies the filter.  
5. In the Comment box, enter the comment.  
6. Select the Interface Specific check box to configure interface-specific names for firewall counters. |
| Configure accounting for firewall filters. | 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>
<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.&lt;br&gt;2. Click Add new entry next to Term.&lt;br&gt;3. Expand Term.&lt;br&gt;4. In the Name box, enter the name that identifies the term.&lt;br&gt;5. In the Comment box, enter the comment for the term.&lt;br&gt;6. From the Filter list, select the name that identifies the filter.&lt;br&gt;7. Expand From.&lt;br&gt;8. In the Comment box, enter the comment.&lt;br&gt;9. Select the Tcp Initial check box if it matches the first TCP packet of a connection.&lt;br&gt;10. Select the Tcp established check box if it matches the TCP packets other than the first packet of a connection.&lt;br&gt;11. In the Tcp Flags box, enter the TCP flags.&lt;br&gt;12. From the listed protocol-independent match conditions, select the filters defined for the inet family type. The protocol-independent match conditions are Address, Destination Address, Destination Class, Destination port, Destination prefix List, Dscp, Forwarding Class, Fragment offset, Icmp Code, Icmp Type, Interface, Interface Group, Interface Set, Ip Options, Loss Priority, Packet Length, Port, prefix List, Protocol, Source Address, Source Port, Source Prefix List, and traffic list.&lt;br&gt;13. Expand Then.&lt;br&gt;14. In the Comment box, enter the comment for then.&lt;br&gt;15. In the Count box, enter the number of packets.&lt;br&gt;16. Select the Log check box to store the header information of a packet on the Routing Engine.&lt;br&gt;17. Select the Syslog check box to log an alert for the packet.&lt;br&gt;18. Select the Sample check box to sample the packet traffic.&lt;br&gt;19. Select the Port Mirror check box to port-mirror the packets.&lt;br&gt;20. From the Loss Priority list, set the packet loss priority (PLP) to low, medium-low, medium-high, or high.&lt;br&gt;21. In the Forwarding Class box, enter the packet forwarding class name.&lt;br&gt;22. From the Prefix Action list, select the prefix specific action.</td>
</tr>
</tbody>
</table>
Table 78: Inet6 Firewall Filter Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>23. Click Accept next to Then.</td>
<td></td>
</tr>
<tr>
<td>24. Select one of the following:</td>
<td></td>
</tr>
<tr>
<td>■ Accept—To accept a packet.</td>
<td></td>
</tr>
<tr>
<td>■ Discard—To discard a packet silently, without sending an ICMP message.</td>
<td></td>
</tr>
<tr>
<td>■ Next—To evaluate the next term in the firewall filter.</td>
<td></td>
</tr>
<tr>
<td>25. Click Policer next to Then.</td>
<td></td>
</tr>
<tr>
<td>26. Select one of the following:</td>
<td></td>
</tr>
<tr>
<td>■ policer—To configure a new policer for each filter and select the policer name.</td>
<td></td>
</tr>
<tr>
<td>■ three-color-policer—To configure a tricolor marking policer,</td>
<td></td>
</tr>
<tr>
<td>a. Expand Three Color Policier.</td>
<td></td>
</tr>
<tr>
<td>b. Click Single Rate next to Three Color Policier.</td>
<td></td>
</tr>
<tr>
<td>c. Select one of the following:</td>
<td></td>
</tr>
<tr>
<td>■ Select single-rate if the named tricolor policer is a single-rate policer.</td>
<td></td>
</tr>
<tr>
<td>■ Select two-rate if the named tricolor policer is a two-rate policer.</td>
<td></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 79 on page 171.
5. Click one:
   ■ OK—Saves the changes.
   ■ Cancel—Cancels the modifications.

Table 79: 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 Service Filter next to inet.</td>
</tr>
<tr>
<td></td>
<td>2. Click Add new entry next to Service Filter.</td>
</tr>
<tr>
<td></td>
<td>3. Expand service-filter.</td>
</tr>
<tr>
<td></td>
<td>4. In the Name box, enter the name that identifies the service filter.</td>
</tr>
</tbody>
</table>
Table 79: 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</td>
</tr>
<tr>
<td></td>
<td>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 80 on page 173.
5. Click one:
   ■ OK—Saves the changes.
   ■ Cancel—Cancels the modifications.
### Table 80: 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 80: MPLS Firewall Filter Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define a 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. 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.</td>
</tr>
<tr>
<td></td>
<td>10. Expand <strong>Then</strong>.</td>
</tr>
<tr>
<td></td>
<td>11. In the <strong>Comment</strong> box, enter the comment for then.</td>
</tr>
<tr>
<td></td>
<td>12. In the <strong>Count</strong> box, enter the number of packets.</td>
</tr>
<tr>
<td></td>
<td>13. Select the <strong>Sample</strong> check box to sample the packet traffic.</td>
</tr>
<tr>
<td></td>
<td>14. 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>15. In the <strong>Forwarding Class</strong> box, enter the packet forwarding class name.</td>
</tr>
<tr>
<td></td>
<td>16. Click <strong>Accept</strong> next to Then.</td>
</tr>
<tr>
<td></td>
<td>17. Select one of the following:</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>18. Click <strong>Policer</strong> next to Then.</td>
</tr>
<tr>
<td></td>
<td>19. 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>■ 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>

**Related Topics**
- Configuring the Firewall Filter for Any Family Type (NSM Procedure) on page 157
- Configuring Filters for inet Family Type (NSM Procedure) on page 163
Configuring 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 81 on page 176.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.
### Table 81: 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 81: 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 Ip 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 Loss Priority list, set the packet loss priority (PLP) to low, medium-low, medium-high, or high.  
15. In the Forwarding Class box, enter the packet forwarding class name.  
16. Select the Port Mirror check box to configure port mirroring for VPLS traffic.  
17. Click Accept next to Then.  
18. Select one of the following:  
   ■ 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. |
Configuring a Policer for a Firewall Filter

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

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

The following policer limits apply on the switch:

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

1. In the navigation tree, select Device Manager > Devices. In Device Manager, select the device for which you want to configure a policer.
2. In the configuration tree, expand Firewall.
3. Perform the configuration tasks as described in Table 82 on page 178.

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

Table 82: 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 Policer and click Add new entry. In the Policer 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.</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>3. Select Bandwidth Limit, select bandwidth-limit. 4. In the box, type 10. 5. Click OK.</td>
</tr>
</tbody>
</table>
Table 82: 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.
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 83 on page 181.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure an accounting group. | 1. Click Add new entry next to Accounting.
| | 2. In the Name box, type the name of the accounting group. |
### Table 83: Accounting Options Configuration Details (continued)

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

**Related Topics**  ■ Configuring the Extended DHCP Agent (NSM Procedure) on page 183
See the following sections for details on configuring the extended Dynamic Host Configuration Protocol agent.

- Configuring Authentication Support for the DHCP Relay Agent (NSM Procedure) on page 183
- Configuring Group (NSM Procedure) on page 184
- Overriding the Default Configuration Settings for the Extended DHCP Relay Agent (NSM Procedure) on page 185
- Configuring Relay Option 60 Information for Forwarding Client Traffic to Specific DHCP Servers (NSM Procedure) on page 186
- Configuring Relay Option 82 for a DHCP Server (NSM Procedure) on page 188
- Specifying the Name of a Group of DHCP Server Addresses for Use by the Extended DHCP Relay Agent (NSM Procedure) on page 189
- Configuring Operations for Extended DHCP Relay Agent Processes (NSM Procedure) on page 190

**Configuring the Extended DHCP 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 84 on page 184.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.
Table 84: 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. In the Comment box, enter the comment for authentication.</td>
</tr>
<tr>
<td></td>
<td>2. In the Password box, enter the password to be sent to the external AAA authentication server for subscriber authentication.</td>
</tr>
</tbody>
</table>

Configure the username.

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></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 85 on page 185.
6. Click one:
■ OK—Saves the changes.
■ Cancel— Cancels the modifications.

Table 85: 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 183</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></td>
<td>3. Click Interface next to group.</td>
</tr>
<tr>
<td></td>
<td>4. Click Add new entry next to Interface.</td>
</tr>
<tr>
<td></td>
<td>5. From the Name list, select the name of the interface.</td>
</tr>
<tr>
<td></td>
<td>6. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>7. From the Upto list, select the upper end of the range of interfaces.</td>
</tr>
<tr>
<td></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.

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 86 on page 186.         |
6. Click one:
- OK—Saves the changes.
- Cancel—Cancels the modifications.

### Table 86: 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 87 on page 187.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

**Table 87: Relay Option 60 Configuration Details**

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the match criteria when you use the DHCP vendor class</td>
<td>1. In the <strong>Comment</strong> box, enter the comment for the relay option 60.</td>
</tr>
<tr>
<td>identifier option (option 60) in DHCP client packets to forward client</td>
<td>2. Click <strong>Vendor Option</strong> next to Relay Option 60.</td>
</tr>
<tr>
<td>traffic to specific DHCP servers.</td>
<td>3. In the <strong>Comment</strong> box, enter the comment for Vendor Option.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Default Relay Server Group</strong> next to Vendor Option and select</td>
</tr>
<tr>
<td></td>
<td>the name of the default DHCP relay server group.</td>
</tr>
<tr>
<td></td>
<td>■ Select <strong>Drop</strong> to drop DHCP client packets that contain an option 60</td>
</tr>
<tr>
<td></td>
<td>string that matches the ASCII or hexadecimal match string and match criteria.</td>
</tr>
</tbody>
</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.
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 88 on page 189.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

---

Table 87: 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. |
Table 88: 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 89 on page 190.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
Table 89: Server 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 90 on page 190.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 90: 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 90: 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 91 on page 192.
5. Click one:
   ■ OK—Saves the changes.
   ■ Cancel—Cancels the modifications.
Table 91: 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. |
| Apply a forwarding table filter for VPLS. | 1. Click Vpls next to Family.  
2. Expand Vpls.  
3. Click Filter next to Vpls.  
4. In the Comment box, enter the comment.  
5. From the Input list, select the name of the applied filter.  
6. Click Flood next to Vpls.  
7. In the Comment box, enter the comment.  
8. From the Input list, select the name of the applied filter. |

Related Topics

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

Configuring Load Balancing Using Hash Key (NSM Procedure)

When there are multiple equal-cost paths to the same destination for the active route, the JUNOS 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 92 on page 193.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
### Table 92: 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.</td>
<td>1. Click <strong>Inet</strong> next to Family.</td>
</tr>
<tr>
<td>Only the IPv4 protocol is supported.</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></td>
<td>Configure layer information for the load-balancing specification. Only the IPv4 protocol is supported.</td>
</tr>
</tbody>
</table>

| Configure load balancing based on MPLS labels. Only the IPv4 protocol is supported. | 1. Click **Mpls** next to Family.                                                               |
|                                                                                     | 2. Expand **Mpls**.                                                                                |
|                                                                                     | 3. Click **Payload** next to Mpls.                                                                |
|                                                                                     | 4. In the **Comment** box, enter the comment.                                                     |
|                                                                                     | 5. Click **Ip** next to Payload.                                                                 |
|                                                                                     | 6. In the **Comment** box, enter the comment.                                                     |
|                                                                                     | 7. Expand **Ip**.                                                                                 |
|                                                                                     | 8. Click **Layer 3 Only** next to **Ip**.                                                         |
|                                                                                     | 9. Select **layer-3-only** to include only Layer 3 IP information.                               |
|                                                                                     | 10. Select **port-data** to include the source and destination port field information.           |
|                                                                                     | a. In the **Comment** box, enter the comment.                                                     |
|                                                                                     | b. Select **Source Msb** to include the most significant byte of the source port.                 |
|                                                                                     | c. Select **Source Lsb** to include the least significant byte of the source port.                |
|                                                                                     | d. Select **Destination Msb** to include the most significant byte of the destination port.       |
|                                                                                     | e. Select **Destination Lsb** to include the least significant byte of the destination port.      |

| Configure load balancing based on Layer 2 media access control information. | 1. Click **Multiservice** next to Mpls.                                                          |
|                                                                             | 2. In the **Comment** box, enter the comment.                                                     |
|                                                                             | 3. Select **Source Mac** to include the source-address MAC information in the hash key.         |
|                                                                             | 4. Select **Destination Mac** to include the destination-address MAC information in the hash key.|

**Related Topics**
- Configuring Accounting Options (NSM Procedure) on page 181
- Configuring Helpers (NSM Procedure) on page 194
- Configuring Per-Flow and Per-Prefix Load Balancing (NSM Procedure) on page 202
Configuring Helpers (NSM Procedure)

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

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

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

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

To configure a BOOTP relay agent in NSM:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Forwarding Options > Helpers > BOOTP.
4. Add or modify settings as specified in Table 93 on page 194.
5. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

<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 IIP time-to-live (TTL) value in DHCP response packets sent to a DHCP client. |
<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure DHCP option 82.</td>
<td>1. Click <strong>Dhcp Option82</strong> next to Bootp.</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 disable DHCP option 82 on this VLAN.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Circuit Id</strong> next to Dhcp Option82.</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>Prefix</strong> list, select the prefix</td>
</tr>
<tr>
<td></td>
<td>■ <strong>hostname</strong>—Set hostname as the prefix.</td>
</tr>
<tr>
<td></td>
<td>7. Select the <strong>Use Interface Description</strong> check box to use interface description instead of name.</td>
</tr>
<tr>
<td></td>
<td>8. Select the <strong>Use Vlan Id</strong> check box to use vlan id.</td>
</tr>
<tr>
<td></td>
<td>9. Click <strong>Remote Id</strong> next to Dhcp Option82.</td>
</tr>
<tr>
<td></td>
<td>10. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>11. From the <strong>Prefix</strong> list, select the prefix</td>
</tr>
<tr>
<td></td>
<td>■ <strong>none</strong>—Set no prefix.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>hostname</strong>—Set hostname as the prefix.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>mac</strong>—Set chassis MAC as the prefix.</td>
</tr>
<tr>
<td></td>
<td>12. Select the <strong>Use Interface Description</strong> check box to use interface description instead of name.</td>
</tr>
<tr>
<td></td>
<td>13. In the <strong>Use String</strong> check box, enter the raw string instead of the default remote ID.</td>
</tr>
<tr>
<td></td>
<td>14. Click <strong>Vendor Id</strong> next to Dhcp Option82.</td>
</tr>
<tr>
<td></td>
<td>15. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>16. In the <strong>Use String</strong> check box, enter the raw string instead of the default remote ID.</td>
</tr>
</tbody>
</table>
Table 93: BOOTP Configuration Details (continued)

<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 IIP time-to-live (TTL) value in DHCP response packets sent to a DHCP client. |
Table 93: 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 94 on page 199.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.
### Table 94: 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.  
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 95 on page 200.

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

**Table 95: 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 Name System (DNS), or Trivial File Transfer Protocol (TFTP) service, or 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 or stop packets from being forwarded on a logical interface, a group of 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 a broadcast message.</td>
</tr>
<tr>
<td></td>
<td>12. In the Descriptions box, enter the description of BOOTP, DHCP, Domain Name System (DNS), or Trivial File Transfer Protocol (TFTP) service, or of an interface that is configured for the service.</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 96 on page 201.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 96: Traceoptions Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Define tracing operations for event policy. | 1. In the Comment box, enter the comment for the traceoptions.  
2. Select the No Remote Trace check box to disable remote tracing globally or for a specific tracing operation.  
3. From the Level list, select the level. |
**Table 96: Traceoptions Configuration Details (continued)**

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the name of the file to receive the output of the tracing</td>
<td>1. In the <strong>Comment</strong> box, enter the comment for the file.</td>
</tr>
<tr>
<td>operation and the maximum number of trace files.</td>
<td>2. In the <strong>Filename</strong> box, enter the name of the file to receive the output of the tracing</td>
</tr>
<tr>
<td></td>
<td>operation.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Size</strong> box, enter the maximum size of each trace file, in kilobytes (KB),</td>
</tr>
<tr>
<td></td>
<td>megabytes (MB), or gigabytes (GB).</td>
</tr>
<tr>
<td></td>
<td>4. 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>Default: 3.</td>
</tr>
<tr>
<td></td>
<td>5. 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. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Match</strong> box, enter the regular expression.</td>
</tr>
<tr>
<td>Specify the tracing operation to perform</td>
<td>1. Click <strong>Add new entry</strong> next to Flag</td>
</tr>
<tr>
<td></td>
<td>2. From the <strong>Name</strong> list, select the flag.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Comment</strong> box, enter the comment for the flag.</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 97 on page 203.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.
Table 97: 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 203
- Configuring Helpers (NSM Procedure) on page 194
- Configuring Load Balancing Using Hash Key (NSM Procedure) on page 192

**Configuring Port Mirroring (NSM Procedure)**

On all M Series, T Series, and MX Series routers, you can send a copy of an IPv4 or IPv6 packet from the routers to an external host address or a packet analyzer for analysis. This is known as port mirroring. In addition, on the M7i, M10i, M120, M320 and MX Series routers only, you can configure port mirroring for VPLS traffic. VPLS port mirroring is supported only on M7i and M10i routers with Enhanced CFEB (CFEB-E). In addition, on M320 routers, VPLS port mirroring is supported only on Enhanced III Flexible PIC Concentrators (FPCs).

To configure port mirroring in NSM:
1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Forwarding Options > Port Mirroring**.
4. Add or modify settings as specified in Table 98 on page 204.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
### Table 98: 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 98: Port Mirroring Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure a port-mirroring instance. | 1. Click **Instance** next to Port Mirroring.  
2. Click **Add new entry** next to Instance.  
3. In the **Name** box, enter the name of the port-mirroring instance.  
4. To configure the address type family to sample for port mirroring, refer Table 98 on page 204.  
5. To configure input packet properties for port mirroring, refer Table 98 on page 204. |

| Configure traffic sampling tracing operations. | 1. In the **Comment** box, enter the comment for traceoptions.  
2. Click **File** next to Traceoptions.  
3. In the **Comment** box, enter the comment for the file.  
4. In the **Filename** box, enter the name of the file containing the trace information.  
   Default: /var/log/sampled  
5. In the **Size** box, enter the maximum size of each traffic sampling file or trace log file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).  
   Syntax: xk to specify KB, xm to specify MB, or xg to specify GB  
   Range: 10 KB through the maximum file size supported on your router  
   Default: 1 MB for sampling data; 128 KB for log information  
6. From the **Files** list, select the maximum number of traffic sampling or trace log files.  
   Range: 1 through 100 files  
   Default: 5 files for sampling output; 10 files for trace log information  
7. Select one of the following:  
   - **world-readable**—To enable unrestricted file access.  
   - **no-world-readable**—To restrict file access to owner. |

**Related Topics**  
- Configuring Per-Flow and Per-Prefix Load Balancing (NSM Procedure) on page 202  
- Configuring Load Balancing Using Hash Key (NSM Procedure) on page 192  
- Specifying Address Family for Filters (NSM Procedure) on page 191
Configuring Port Mirroring (NSM Procedure)
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 209
- Configuring Receive Bucket Properties on Interfaces (NSM Procedure) on page 210
- Configuring Tracing Operations of an Individual Router Interface (NSM Procedure) on page 210
- Configuring Transmit Leaky Bucket Properties (NSM Procedure) on page 211
- Configuring Logical Interface Properties (NSM Procedure) on page 212
- Configuring Protocol Family Information for the Logical Interface (NSM Procedure) on page 215
- Configuring the Traffic Shaping Profile (NSM Procedure) on page 233

Configuring Interface Properties (NSM Procedure)

You can configure interfaces on the router using this option. The management and internal Ethernet interfaces are automatically configured. You must configure all other interfaces.

To configure interfaces in NSM:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Interfaces.
4. Select Interface.
NOTE: You can also configure interfaces through the Quick Configuration tab. Also, you can configure interfaces in a Config group and apply them to the interface node.

5. Add or modify settings as specified in Table 99 on page 208.

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

### Table 99: 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. 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>- <strong>traps</strong>—To enable the sending of Simple Network Management Protocol (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 (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 100 on page 209.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

<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 |

Table 100: Hold Time Configuration Details
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 101 on page 210.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure receive bucket properties.</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 Receive Bucket next to interface.</td>
</tr>
<tr>
<td></td>
<td>4. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. From the Overflow list, select how to handle packets that exceed the threshold for the receive leaky bucket.</td>
</tr>
<tr>
<td></td>
<td>■ Select tag to tag, count, and process received packets that exceed the threshold.</td>
</tr>
<tr>
<td></td>
<td>■ Select discard to discard received packets that exceed the threshold.</td>
</tr>
<tr>
<td></td>
<td>6. From the Rate 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 Threshold 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 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 102 on page 211.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

**Table 102: Trace Options Configuration Details**

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Define tracing operations for individual interfaces. | 1. Click **Add Interface** next to Interface.  
2. In the **Add Interface Dialog** box, enter the interface name.  
3. Click **Traceoptions** next to interface.  
4. In the **Comment** box, enter the comment.  
5. Expand **Traceoptions**.  
6. Click **Flag** next to Traceoptions.  
7. Click **Add new entry** next to Flag.  
8. From the **Name** list, select the tracing operation to perform.  
9. In the **Comment** box, enter the comment. |

**Configuring Transmit Leaky Bucket Properties (NSM Procedure)**

For all interface types except ATM, channelized E1, E1, Fast Ethernet, Gigabit Ethernet, and channelized IQ, you can configure leaky bucket properties, which allow you to limit the amount of traffic transmitted by a particular interface. You effectively specify what percentage of the interface’s total capacity can be used to transmit packets. You might want to set leaky bucket properties to limit the traffic flow from a link that is known to transmit a high volume of traffic.

To configure transmit leaky bucket properties in NSM:
1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in Table 103 on page 212.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.
Table 103: 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 104 on page 213.
6. Click one:
   ■ **OK**—Saves the changes.
   ■ **Cancel**—Cancels the modifications.
Table 104: Logical Unit Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure logical unit</td>
<td>1. Click Add Interface next to Interface.</td>
</tr>
<tr>
<td>unit properties.</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. From the Name list, select the interface name.</td>
</tr>
<tr>
<td></td>
<td>6. In the Comment check box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>7. Select the Disable check box to disable a physical or a logical interface,</td>
</tr>
<tr>
<td></td>
<td>effectively unconfiguring it.</td>
</tr>
<tr>
<td></td>
<td>8. Select the Reassemble Packets check box to enable reassembly of fragmented</td>
</tr>
<tr>
<td></td>
<td>tunnel packets on generic routing encapsulation (GRE) tunnel interfaces.</td>
</tr>
<tr>
<td></td>
<td>9. In the Description box, enter the text to describe the interface.</td>
</tr>
<tr>
<td></td>
<td>10. From the Encapsulation list, select the encapsulation type.</td>
</tr>
<tr>
<td></td>
<td>11. In the Bandwidth box, enter the peak rate.</td>
</tr>
<tr>
<td></td>
<td>12. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>■ traps—to enable the sending of Simple Network Management Protocol (SNMP)</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>(SNMP) notifications when the state of the connection changes.</td>
</tr>
<tr>
<td></td>
<td>13. From the Accounting Profile 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 105 on page 214.
6. Click one:
   ■ OK—Saves the changes.
   ■ Cancel— Cancels the modifications.
Table 105: IP Demux Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure the logical demultiplexing (demux) destination family type. | 1. Click **Add Interface** next to Interface.  
2. In the **Add Interface Dialog** box, enter the interface name.  
3. Click **Unit** next to interface.  
4. Click **Add new entry** next to Unit.  
5. Click **Demux Destination** next to Unit.  
6. Click **Add new entry** next to Demux Destination.  
7. From the **New demux-destination** window, select the family type. |

Configuring the Logical Demux Source Family Type on the IP Demux Underlying Interface (NSM Procedure)

You can configure the logical demultiplexing (demux) source family type on the IP demux underlying interface using this option.

To configure logical demux source family type in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Interfaces**.
4. Select **Interface**.
5. Add or modify settings as specified in Table 106 on page 214.
6. Click one:  
   - **OK**—Saves the changes.  
   - **Cancel**—Cancels the modifications.

Table 106: 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 107 on page 215.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.

---

**Table 107: 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 plp0** box, enter the early packet discard threshold value.  
8. In the **Plp1** box, enter the maximum number of cells.  
   - Range: For 1-port and 2-port OC12 interfaces, 1 through 425,984 cells |

---

**Configuring Protocol Family Information for the Logical Interface (NSM Procedure)**

You can configure the family information for the logical interface for different protocols using the following options:

1. Configuring Protocol Family (Ccc) Information for the Logical Interface (NSM Procedure) on page 216
2. Configuring Protocol Family (Inet) Information for the Logical Interface (NSM Procedure) on page 217
3. Configuring Protocol Family (Inet6) Information for the Logical Interface (NSM Procedure) on page 223
4. Configuring Protocol Family (ISO) Information for the Logical Interface (NSM Procedure) on page 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 108 on page 216.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 108: Ccc Family Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Apply a filter to an 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 Family next to Unit.  
6. Expand Family  
7. Click Ccc next to Family.  
8. In the Comment box, enter the comment.  
9. Click Filter next to Ccc.  
10. In the Comment box, enter the comment.  
11. From the Group list, select the filter group number. (Range: 0 through 255) |
| Configure input filter. | 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.  
     a. 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 108: Ccc Family Configuration Details *(continued)*

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure output filter</td>
<td>1. Click <strong>Output</strong> next to Filter.</td>
</tr>
<tr>
<td></td>
<td>2. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>output</strong>—To configure name of one filter to evaluate when packets are transmitted on the interface.</td>
</tr>
<tr>
<td></td>
<td>a. Enter the output filter name.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>output-list</strong>—To apply a group of filters to evaluate when packets are transmitted on an interface.</td>
</tr>
<tr>
<td></td>
<td>a. Click <strong>Add new entry</strong> next to output-list.</td>
</tr>
<tr>
<td></td>
<td>b. In the <strong>New output-list</strong> window, enter the filter names. Up to 16 filters can be included in a filter input list.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Apply a policer to an interface</th>
<th>1. Click <strong>Policer</strong> next to Filter.</th>
</tr>
</thead>
<tbody>
<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 109 on page 218.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.
Table 109: Inet Family Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure Inet information. | 1. Click **Add Interface** next to Interface.  
2. In the **Add Interface Dialog** box, enter the interface name.  
3. Click **Unit** next to interface.  
4. Click **Add new entry** next to Unit.  
5. Click **Family** next to Unit.  
6. Expand **Family**.  
7. Click **Inet** next to Family.  
8. In the **Comment** box, enter the comment.  
9. From the **Mac Validate** list, select one of the following:  
   - **strict**—Forwards incoming packets when both the IP source address and the MAC source address match one of the trusted address tuples. Drops packets when the MAC address does not match the tuple’s MAC source address, or when IP source address of the incoming packet does not match any of the trusted IP addresses.  
   - **loose**—Forwards incoming packets when both the IP source address and the MAC source address match one of the trusted address tuples. Drops packets when the IP source address matches one of the trusted tuples, but the MAC address does not match the MAC address of the tuple. Continues to forward incoming packets when the source address of the incoming packet does not match any of the trusted IP addresses.  
10. From the **Mtu** list, select the MTU size.  
   Range: 0 through 4294967295  
11. Select the **No Redirects** check box to disable the sending of protocol redirect messages for the entire routing platform.  
12. Select the **No Arp Learn** check box to disable ARP mappings.  
13. Select the **Primary** check box to configure the address to be the primary address of the protocol on the interface.  
Enable IP packet counters on an interface. | 1. Click **Accounting** next to Inet.  
2. In the **Comment** box, enter the comment.  
3. Select the **Destination Class Usage** check box to enable packet counters on an interface that count packets that arrive from specific customers and are destined for specific prefixes on the provider core router.  
4. Click **Source Class Usage** next to Accounting.  
5. In the **Comment** box, enter the comment.  
6. Select the **Input** check box to configure at least one expected ingress point.  
7. Select the **Output** check box to configure at least one expected egress point.  

---

218  
 Configuring Protocol Family (Inet) Information for the Logical Interface (NSM Procedure)
Table 109: Inet 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 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 109: Inet Family Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a backup router to preempt the master router.</td>
<td>1. Click <strong>Preempt</strong> next to vrrp-group.</td>
</tr>
<tr>
<td></td>
<td>2. Select <strong>preempt</strong> to allow the master router to be preempted.</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>Hold Time</strong> list, select the hold time before a higher-priority backup router preempts the master router.</td>
</tr>
<tr>
<td></td>
<td>3. Select <strong>no-preempt</strong> to prohibit the preemption of the master router.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Track</strong> next to vrrp-group.</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>Priority Hold Time</strong> list, select the minimum length of time that must elapse between dynamic priority changes.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 3600 seconds</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>Interface</strong> next to Track.</td>
</tr>
<tr>
<td></td>
<td>8. Click <strong>Add new entry</strong> next to Interface.</td>
</tr>
<tr>
<td></td>
<td>9. In the <strong>Name</strong> box, enter the interface name.</td>
</tr>
<tr>
<td></td>
<td>10. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>11. From the <strong>Priority Cost</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 254</td>
</tr>
</tbody>
</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. |
## Table 109: Inet Family Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.</td>
<td>Click <strong>Virtual Address</strong> next to vrrp-group.</td>
</tr>
<tr>
<td>11.</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>virtual-address</strong>—To configure the addresses of the virtual routers in a Virtual Router Redundancy Protocol (VRRP) IPv4 group. You can configure up to eight addresses.</td>
</tr>
<tr>
<td></td>
<td>a. Click <strong>Add new entry</strong> and in the New virtual-address window, enter the addresses of one or more virtual routers.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>virtual-inet6-address</strong>—To configure the addresses of the virtual routers in a Virtual Router Redundancy Protocol (VRRP) IPv6 group. You can configure up to eight addresses.</td>
</tr>
<tr>
<td></td>
<td>a. Click <strong>Add new entry</strong> and in the New virtual-inet6-address window, enter the addresses of one or more virtual routers.</td>
</tr>
<tr>
<td>1.</td>
<td>Click <strong>Input</strong> next to Filter.</td>
</tr>
<tr>
<td>2.</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>input</strong>—To configure name of one filter to evaluate when packets are received on the interface.</td>
</tr>
<tr>
<td></td>
<td>a. Enter the input filter name.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>input-list</strong>—To apply a group of filters to evaluate when packets are received on an interface.</td>
</tr>
<tr>
<td></td>
<td>a. Click <strong>Add new entry</strong> next to input-list.</td>
</tr>
<tr>
<td></td>
<td>b. In the <strong>New input-list</strong> window, enter the filter names. Up to 16 filters can be included in a filter input list.</td>
</tr>
<tr>
<td>1.</td>
<td>Click <strong>Output</strong> next to Filter.</td>
</tr>
<tr>
<td>2.</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>output</strong>—To configure name of one filter to evaluate when packets are transmitted on the interface.</td>
</tr>
<tr>
<td></td>
<td>a. Enter the output filter name.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>output-list</strong>—To apply a group of filters to evaluate when packets are transmitted on an interface.</td>
</tr>
<tr>
<td></td>
<td>a. Click <strong>Add new entry</strong> next to output-list.</td>
</tr>
<tr>
<td></td>
<td>b. In the <strong>New output-list</strong> window, enter the filter names. Up to 16 filters can be included in a filter input list.</td>
</tr>
<tr>
<td>1.</td>
<td>Click <strong>Policer</strong> next to Filter.</td>
</tr>
<tr>
<td>2.</td>
<td>In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td>3.</td>
<td>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>4.</td>
<td>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>
### Table 109: Inet Family Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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. |
| 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.  
6. Expand **Input**.  
7. Click **Service Set** next to Input.  
8. Click **Add new entry** next to Service Set.  
9. From the **Name** list, select the service set name.  
10. In the **Comment** box, enter the comment.  
11. In the **Service Filter** box, enter the filter name.  
12. Click **Output** next to Service.  
13. In the **Comment** box, enter the comment.  
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 110 on page 224.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.
Table 110: Inet6 Family Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure Inet6 information. | 1. Click **Add Interface** next to Interface.  
2. In the **Add Interface Dialog** box, enter the interface name.  
3. Click **Unit** next to interface.  
4. Click **Add new entry** next to Unit.  
5. Click **Family** next to Unit.  
6. Expand **Family**.  
7. Click **Inet** next to Family.  
8. In the **Comment** box, enter the comment.  
9. From the **Mac Validate** list, select one of the following:  
   - **strict**—Forwards incoming packets when both the IP source address and the MAC source address match one of the trusted address tuples. Drops packets when the MAC address does not match the tuple’s MAC source address, or when IP source address of the incoming packet does not match any of the trusted IP addresses.  
   - **loose**—Forwards incoming packets when both the IP source address and the MAC source address match one of the trusted address tuples. Drops packets when the IP source address matches one of the trusted tuples, but the MAC address does not match the MAC address of the tuple. Continues to forward incoming packets when the source address of the incoming packet does not match any of the trusted IP addresses.  
10. From the **Mtu** list, select the MTU size.  
   Range: 0 through 4294967295  
11. Select the **No Redirects** check box to disable the sending of protocol redirect messages for the entire routing platform.  
12. Select the **No Arp Learn** check box to disable arp.  
13. Select the **Primary** check box to configure the address to be the primary address of the protocol on the interface. |
| Enable IP packet counters on an interface. | 1. Click **Accounting** next to Inet.  
2. In the **Comment** box, enter the comment.  
3. Select **Destination Class Usage** check box to enable packet counters on an interface that count packets that arrive from specific customers and are destined for specific prefixes on the provider core router.  
4. Click **Source Class Usage** next to Accounting.  
5. In the **Comment** box, enter the comment.  
6. Select the **Input** check box to configure at least one expected ingress point.  
7. Select the **Output** check box to configure at least one expected egress point. |
Table 110: Inet6 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>
<tr>
<td></td>
<td>8. Click <strong>Vrrp Group</strong> next to address.</td>
</tr>
<tr>
<td></td>
<td>9. Click <strong>Add new entry</strong> next to Vrrp Group.</td>
</tr>
<tr>
<td></td>
<td>10. In the <strong>Name</strong> box, enter the interface name.</td>
</tr>
<tr>
<td></td>
<td>11. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>12. In the <strong>Virtual Link Local Address</strong> box, enter the virtual link local address.</td>
</tr>
<tr>
<td></td>
<td>13. From the <strong>priority</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 255</td>
</tr>
<tr>
<td></td>
<td>Default: 100 (for backup routers)</td>
</tr>
<tr>
<td></td>
<td>14. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>accept-data</strong>—To enable the interface to accept packets destined for the virtual IP address.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>no-accept-data</strong>—To prevent the interface from accepting packets destined for the virtual IP address.</td>
</tr>
<tr>
<td></td>
<td>15. From the <strong>Authentication Type</strong> list, select the authentication type.</td>
</tr>
<tr>
<td></td>
<td>16. In the <strong>Authentication Key</strong> box, enter the authentication password.</td>
</tr>
<tr>
<td></td>
<td>17. Select <strong>Advertise-Interval</strong> next to vrrp-group.</td>
</tr>
<tr>
<td></td>
<td>18. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>advertise-interval</strong>—To configure the interval between Virtual Router Redundancy Protocol (VRRP) IPv4 advertisement packets.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 255 seconds</td>
</tr>
<tr>
<td></td>
<td>■ <strong>fast-interval</strong>—To configure the interval, in milliseconds, between Virtual Router Redundancy Protocol (VRRP) advertisement packets.</td>
</tr>
<tr>
<td></td>
<td>Range: 100 through 999 milliseconds</td>
</tr>
<tr>
<td></td>
<td>■ <strong>inet6-advertise-interval</strong>—To configure the interval between Virtual Router Redundancy Protocol (VRRP) IPv6 advertisement packets.</td>
</tr>
<tr>
<td></td>
<td>Range: 100 to 40,950 milliseconds (ms)</td>
</tr>
</tbody>
</table>
Table 110: Inet6 Family Configuration Details *(continued)*

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.</td>
<td>Click <strong>Preempt</strong> next to vrrp-group.</td>
</tr>
<tr>
<td>20.</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td>■ preempt—To allow the master router to be preempted.</td>
<td>a. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td>■ preempt—To allow the master router to be preempted.</td>
<td>b. From the <strong>Hold Time list</strong>, select the hold time before a higher-priority backup router preempts the master router. Range: 0 through 3600</td>
</tr>
<tr>
<td>■ no-preempt—To prohibit the preemption of the master router.</td>
<td>21. Click <strong>Track</strong> next to vrrp-group.</td>
</tr>
<tr>
<td>22.</td>
<td>In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td>23.</td>
<td>From the <strong>Priority Hold Time list</strong>, select the minimum length of time that must elapse between dynamic priority changes. Range: 1 through 3600 seconds</td>
</tr>
<tr>
<td>24.</td>
<td>Click <strong>Interface</strong> next to Track.</td>
</tr>
<tr>
<td>25.</td>
<td>Click <strong>Add new entry</strong> next to Interface.</td>
</tr>
<tr>
<td>26.</td>
<td>In the <strong>Name</strong> box, enter the interface name.</td>
</tr>
<tr>
<td>27.</td>
<td>In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td>28.</td>
<td>From the <strong>Priority Cost list</strong>, 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</td>
</tr>
<tr>
<td>Task</td>
<td>Your Action</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>29.</td>
<td>Click <strong>Bandwidth Threshold</strong> next to interface.</td>
</tr>
<tr>
<td>30.</td>
<td>Click <strong>Add new entry</strong> next to Bandwidth Threshold.</td>
</tr>
<tr>
<td>31.</td>
<td>In the <strong>Name</strong> box, enter the interface name.</td>
</tr>
<tr>
<td>32.</td>
<td>In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td>33.</td>
<td>From the <strong>Priority Cost</strong> 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</td>
</tr>
<tr>
<td>34.</td>
<td>Click <strong>Route</strong> next to Track.</td>
</tr>
<tr>
<td>35.</td>
<td>In the <strong>Route_address</strong> box, enter the address.</td>
</tr>
<tr>
<td>36.</td>
<td>In the <strong>Routing Instances</strong> box, enter the routing instance in which the route is to be tracked.</td>
</tr>
<tr>
<td>37.</td>
<td>From the <strong>Priority Cost</strong> 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.</td>
</tr>
<tr>
<td>38.</td>
<td>Click <strong>Virtual Address</strong> next to vrrp-group.</td>
</tr>
<tr>
<td>39.</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>virtual-address</strong>—To configure the addresses of the virtual routers in a Virtual Router Redundancy Protocol (VRRP) IPv4 group. You can configure up to eight addresses.</td>
</tr>
<tr>
<td></td>
<td>a. Click <strong>Add new entry</strong> and in the <strong>New virtual-address</strong> window, enter the addresses of one or more virtual routers.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>virtual-inet6-address</strong>—To configure the addresses of the virtual routers in a Virtual Router Redundancy Protocol (VRRP) IPv6 group. You can configure up to eight addresses.</td>
</tr>
<tr>
<td></td>
<td>a. Click <strong>Add new entry</strong> and in the <strong>New virtual-inet6-address</strong> window, enter the addresses of one or more virtual routers.</td>
</tr>
<tr>
<td>1.</td>
<td>Click <strong>Input</strong> next to Filter.</td>
</tr>
<tr>
<td>2.</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>■ Select <strong>input</strong> to configure name of one filter to evaluate when packets are received on the interface.</td>
</tr>
<tr>
<td></td>
<td>a. Enter the input filter name.</td>
</tr>
<tr>
<td></td>
<td>■ Select <strong>input-list</strong> to apply a group of filters to evaluate when packets are received on an interface.</td>
</tr>
<tr>
<td></td>
<td>a. Click <strong>Add new entry</strong> next to input-list.</td>
</tr>
<tr>
<td></td>
<td>b. In the <strong>New input-list</strong> window, enter the filter names. Up to 16 filters can be included in a filter input list.</td>
</tr>
</tbody>
</table>
### Table 110: Inet6 Family Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure output filter.</strong></td>
<td>1. Click <strong>Output</strong> next to Filter.</td>
</tr>
<tr>
<td></td>
<td>2. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>output</strong> to configure name of one filter to evaluate when</td>
</tr>
<tr>
<td></td>
<td>packets are transmitted on the interface.</td>
</tr>
<tr>
<td></td>
<td>a. Enter the output filter name.</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>output-list</strong> to apply a group of filters to evaluate when</td>
</tr>
<tr>
<td></td>
<td>packets are transmitted on an interface.</td>
</tr>
<tr>
<td></td>
<td>a. Click <strong>Add new entry</strong> next to output-list.</td>
</tr>
<tr>
<td></td>
<td>b. In the <strong>New output-list</strong> window, enter the filter names.</td>
</tr>
<tr>
<td></td>
<td>Up to 16 filters can be included in a filter input list.</td>
</tr>
<tr>
<td><strong>Apply a policer to an interface.</strong></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</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>packets are transmitted on the interface.</td>
</tr>
<tr>
<td><strong>Check whether traffic is arriving on an expected path.</strong></td>
<td>1. Click <strong>Rpf Check</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. In the <strong>Fail Filter</strong> box, enter the filter name to evaluate when</td>
</tr>
<tr>
<td></td>
<td>packets are received on the interface.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Mode</strong> next to Rpf Check.</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>loose</strong> check box to check whether the packet has a</td>
</tr>
<tr>
<td></td>
<td>source address with a corresponding prefix in the routing table.</td>
</tr>
<tr>
<td><strong>Configure the direction of traffic to be sampled.</strong></td>
<td>1. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>2. Select the <strong>Input</strong> check box to configure at least one expected</td>
</tr>
<tr>
<td></td>
<td>ingress point.</td>
</tr>
<tr>
<td></td>
<td>3. Select the <strong>Output</strong> check box to configure at least one expected</td>
</tr>
<tr>
<td></td>
<td>egress point.</td>
</tr>
</tbody>
</table>
### Table 110: Inet6 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. |

---

#### 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 111 on page 230.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
### Table 111: 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 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 Iso 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>
</tbody>
</table>

Configure the interface address.

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Click Address next to Inet.</td>
</tr>
<tr>
<td></td>
<td>2. Click Add new entry next to Address.</td>
</tr>
<tr>
<td></td>
<td>3. Expand address.</td>
</tr>
<tr>
<td></td>
<td>4. In the Name box, enter the interface name.</td>
</tr>
<tr>
<td></td>
<td>5. In the Comment 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 112 on page 231.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.
<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure MPLS information. | 1. Click **Add Interface** next to Interface.  
2. In the **Add Interface Dialog** box, enter the interface name.  
3. Click **Unit** next to interface.  
4. Click **Add new entry** next to Unit.  
5. Click **Family** next to Unit.  
6. Expand **Family**.  
7. Click **MPLS** next to Family.  
8. In the **Comment** box, enter the comment.  
9. From the **Mtu** list, select the MTU size. Range: 0 through 4294967295 |

| 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.  
     a. 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.  
     a. 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. |
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 113 on page 232.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

### Table 113: 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>
<tr>
<td>Apply a policer to an interface.</td>
<td>1. Click Policier next to Tcc.</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>
<tr>
<td>Configure Ethernet TCC encapsulation.</td>
<td>1. Click proxy next to TCC.</td>
</tr>
<tr>
<td></td>
<td>2. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. Click Remote next to TCC.</td>
</tr>
<tr>
<td></td>
<td>4. In the Comment box, enter the comment.</td>
</tr>
</tbody>
</table>
**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 114 on page 234.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.
Table 114: 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:  
    - **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).  
    - **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.  
    - **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 115 on page 235.  
6. Click one:  
   - **OK**—Saves the changes.
Table 115: Interface Set Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Define the interface set. | 1. Click **Add new entry** next to Interface Set.  
2. Click **interface-set**.  
3. In the **Name** box, enter the name for the interface set.  
4. In the **Comment** box, enter the comment. |
| Apply the interface set to interfaces. | 1. Click **interface** next to interface-set.  
2. Click **Add new entry** next to Interface.  
3. In the **Name** box, enter the interface name.  
4. In the **Comment** box, enter the comment.  
5. Click **Unit** next to interface.  
6. Click **Add new entry** next to Unit.  
7. From the **Name** list, select the number of the logical unit.  
   Range: 0 through 16,385  
8. In the **Comment** box, enter the comment.  
9. Click **Vlan Tags Outer** next to Interface.  
10. Click **Add new entry** next to Vlan tags Outer.  
11. From the **Name** list, select the outer VLAN ID.  
12. In the **Comment** box, enter the comment. |

Related 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 **Traceoptions**.
5. Add or modify settings as specified in Table 116 on page 236.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.
### Table 116: 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.  
   - **Select world-readable**—To enable unrestricted access.  
9. In the **Match** box, 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
Chapter 18

Configuring Multicast Snooping Options

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 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 35 on page 81.
5. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
### Table 117: 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 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 117: 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.  
   Range: 10240 to 4294967295 bytes  
7. In the **Size** box, enter the maximum size of each trace file in 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. |
M-series and MX-series Devices
Chapter 19
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 246
- 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 118 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 118: 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 119 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 119: 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 120 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 120: 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 121 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 121: 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 122 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 122: 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.</td>
<td>Select the check-box to disable damping Clear the check-box to enable damping</td>
</tr>
<tr>
<td></td>
<td>Any damping state that is present in the routing table for a prefix is deleted if damping is disabled.</td>
<td></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>
<tr>
<td>Max Suppress</td>
<td>Indicates the maximum time in minutes that a route can be suppressed no matter how unstable it has been.</td>
<td>1. Enter the time limit or select it from the list. 2. Click OK.</td>
</tr>
</tbody>
</table>

### 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 123 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 123: Configuring Policy Statement Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of the policy statement.</td>
<td>1. Click the New button or select a policy statement and click Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select <strong>policy-statement</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the name.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for the policy statement.</td>
<td>1. Click the New button or select a policy statement and click Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select <strong>policy-statement</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the comment.</td>
</tr>
<tr>
<td>From</td>
<td>Enables you to define the criteria that an incoming route must match.</td>
<td>1. Click the New button or select a policy statement and click Edit button.</td>
</tr>
<tr>
<td></td>
<td>You can specify one or more match conditions. If you specify more than</td>
<td>2. Expand <strong>policy-statement</strong> tree and select <strong>From</strong>.</td>
</tr>
<tr>
<td></td>
<td>one, all conditions must match the route for a match to occur.</td>
<td>3. Enter the From criteria.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Expand <strong>From</strong> tree and specify the match conditions.</td>
</tr>
</tbody>
</table>
### Table 123: Configuring Policy Statement Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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 124 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 124: 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 prefix-list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the name.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for the prefix list.</td>
<td>1. Click the New button or select a prefix list and click Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select prefix-list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the comment.</td>
</tr>
<tr>
<td>Apply Path</td>
<td>Indicates that the prefix list should include all IP prefixes pointed to 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 prefix-list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the path.</td>
</tr>
<tr>
<td>Prefix List Item</td>
<td>Specifies the prefix list item.</td>
<td>1. Click the New button or select a prefix list and click Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Expand prefix-list tree and select Prefix List Item.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the name and comment.</td>
</tr>
</tbody>
</table>
Chapter 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 257
- Configuring Layer 2 Circuit (NSM Procedure) on page 258
- Configuring Layer 2 Protocol Tunneling and BPDU Protection (NSM Procedure) on page 264
- Configuring Label Distribution Protocol (NSM Procedure) on page 266
- Configuring Link Management Protocol (NSM Procedure) on page 277
- Configuring MSTP (NSM Procedure) on page 280
- Configuring OSPF (NSM Procedure) on page 281
- Configuring RIP (NSM Procedure) on page 285
- Configuring RSVP (NSM Procedure) on page 287
- Configuring VRRP (NSM Procedure) on page 294
- Configuring VSTP (NSM Procedure) on page 295

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 125 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 125: 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>
</tbody>
</table>
| Traceoptions | Enables you to define tracing operations that track all routing protocol functionality in the device. You can configure the tracing flag, filter, and the tracing policy. | 1. Expand the Bfd tree and select Traceoptions.  
2. Expand the Traceoptions tree and set up the file and flag parameters. |

### Configuring BGP (NSM Procedure)

Border Gateway Protocol (BGP) is used for exchanging routing information between gateway hosts/internet service providers. The routing information refers to the routing tables containing information about the list of known devices, the addresses they can reach, and a cost metric associated with the path to each device so that the best available route is chosen. The primary function of a BGP speaking system is to exchange network reachability information with other BGP systems. This feature enables you to configure BGP peering sessions.

To configure BGP in NSM:
1. In the navigation tree select **Device Manager > Devices** and select the device from the list.
2. In the configuration tree, expand **Protocols**.
3. Select **BGP**.
4. Add/Modify the parameters under the respective tabs as specified in Table 126 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>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| General   | The general parameters to be set up for applying BGP.                    | 1. Expand the Protocol tree.  
2. Select BGP and select General tab.  
3. Specify the general parameters like comment, description, local address, hold time, etc. |
| Path Selection | Enables you to specify the path selection criteria.                         | 1. Expand the Protocol tree.  
2. Select BGP and select Path Selection tab.  
3. Set up the path selection parameters and med plus IGP. |
| Traceoptions | Defines trace options for IGMP snooping.                                   | 1. Expand the Protocol tree.  
2. Select BGP and select Traceoptions tab.  
3. Set up the file and flag parameters. |
| Metric Out | Enables you to specify the metric value to add to the routes transmitted to the neighbor. | 1. Expand the Protocol tree.  
2. Select BGP and select Metric Out tab.  
3. Set up the metric value and minimum IGP. |
| 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. |
Table 126: BGP Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advertise</td>
<td>Enables you to specify whether BGP should advertise the best route even if</td>
<td>1. Expand the Protocol tree.</td>
</tr>
<tr>
<td></td>
<td>the routing table did not select it to be an active route.</td>
<td>2. Select BGP and select Advertise tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify whether Advertise has to be inactivated and set up the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Advertise Peer As.</td>
</tr>
<tr>
<td>Import</td>
<td>Enables you to apply one or more routing policies to routes being imported</td>
<td>1. Expand the Protocol tree.</td>
</tr>
<tr>
<td></td>
<td>into the JUNOS routing table from BGP.</td>
<td>2. Select BGP and select Import tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the export policies configured on the peer.</td>
</tr>
<tr>
<td>Family</td>
<td>Enables you to configure protocol family information for the logical</td>
<td>1. Expand the Protocol tree.</td>
</tr>
<tr>
<td></td>
<td>interface.</td>
<td>2. Select BGP and select Family tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the Family and Inet parameters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Expand the Inet tree and set up the parameters.</td>
</tr>
<tr>
<td>Authentication Settings</td>
<td>Enables you to specify the authentication settings for BGP.</td>
<td>1. Expand the Protocol tree.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select BGP and select Authentication Settings tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the authentication key, algorithm and key chain.</td>
</tr>
<tr>
<td>Export</td>
<td>Enables you to apply one or more routing policies to routes being exported</td>
<td>1. Expand the Protocol tree.</td>
</tr>
<tr>
<td></td>
<td>from the JUNOS routing table from BGP.</td>
<td>2. Select BGP and select Export tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the export policies configured on the peer.</td>
</tr>
<tr>
<td>Local As</td>
<td>Enables you to configure BGP with a different local autonomous session</td>
<td>1. Expand the Protocol tree.</td>
</tr>
<tr>
<td></td>
<td>(AS) number for each BGP session</td>
<td>2. Select BGP and select Local As tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the comment, as number, loop and specify whether it is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>private.</td>
</tr>
<tr>
<td>Graceful Restart</td>
<td>Enables you to specify the graceful restart parameters.</td>
<td>1. Expand the Protocol tree.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select BGP and select Graceful Restart tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the graceful restart parameters.</td>
</tr>
</tbody>
</table>
Table 126: BGP Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Bfd Liveness Detection | Enables you to configure bidirectional forwarding detection (BFD) timers. | 1. Expand the Protocol tree.  
2. Select BGP and select Bfd Liveness Detection tab.  
3. Specify the Bfd Liveness Detection parameters, Detection Time and Transmit Interval. |
| Group               | Enables you to configure BGP group.                                        | 1. Expand the Protocol tree.  
2. Select BGP and select Group tab.  
3. Click the New button or select a group and click Edit button.  
4. Enter all the group parameters. |

Configuring 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 127 on page 255.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

Table 127: Trace Options Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define tracing options.</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>
</tbody>
</table>
Table 127: Trace Options Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<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 <strong>File</strong> next to <strong>Traceoptions</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Comment</strong> box, enter the comment for the file.</td>
</tr>
<tr>
<td></td>
<td>3. 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>4. In the <strong>Size</strong> box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). Range: 10240 through 1073741824</td>
</tr>
<tr>
<td></td>
<td>5. From the <strong>Files</strong> 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>■ <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. This is the default setting.</td>
</tr>
</tbody>
</table>

Specify the tracing operation to perform. 1. Click **Add new entry** next to **Flag**. 2. From the **Name** list, select the flag:  ■ **database**—Trace database events.  ■ **routing-socket**—Trace Routing socket events.  ■ **state**—Trace state change events.  ■ **debug**—Trace debug messages.  ■ **event**—Trace event handler events.  ■ **packet**—Trace packet events.  ■ **all**—Trace all areas of code. 3. In the **Comment** box, enter the comment for the flag.

**Related Topics**  ■ Configuring Link Management Protocol (NSM Procedure) on page 277  ■ Configuring Layer 2 Address Learning and Forwarding Properties (NSM Procedure) on page 257
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 128 on page 257.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

### Table 128: L2 Learning Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Layer 2 address learning and forwarding properties globally.</td>
<td>1. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>2. From the <strong>Global Mac Table Aging Time</strong> list, select the time elapsed before MAC table entries are timed out and entries are deleted.</td>
</tr>
<tr>
<td></td>
<td>Range: 10 through 1000000</td>
</tr>
<tr>
<td></td>
<td>3. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Global No Mac Learning</strong>—To disable MAC learning for the entire router</td>
</tr>
<tr>
<td></td>
<td>- <strong>Global Mac Statistics</strong>—To enable MAC accounting for the entire router</td>
</tr>
<tr>
<td>Limit the number of media access control (MAC) addresses learned from the logical interfaces on the router.</td>
<td>1. Click <strong>Global Mac Limit</strong> next to L2 Learning.</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>Mac Limit</strong> list, select the <strong>Number of MAC addresses that can be learned systemwide</strong>.</td>
</tr>
<tr>
<td></td>
<td>Range: 20 through 1,048,575</td>
</tr>
<tr>
<td></td>
<td>4. From the <strong>Packet Action</strong> list, select <strong>drop</strong> to specify that packets for new source MAC addresses be dropped after the MAC address limit is reached.</td>
</tr>
</tbody>
</table>
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 258
- Configuring the Neighbor Interface for the Layer 2 Circuit (NSM Procedure) on page 259
- Tracing Layer 2 Circuit Creation and Changes (NSM Procedure) on page 263

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 129 on page 258.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 129: 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 Comment box, enter the comment.</td>
</tr>
</tbody>
</table>
### 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 130 on page 260.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

---

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</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. |
### Table 130: Neighbor Interface Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a neighbor.</td>
<td>1. In the Name box, enter the IP address of a neighboring router.</td>
</tr>
<tr>
<td></td>
<td>2. In the Comment box, enter the comment.</td>
</tr>
</tbody>
</table>
Table 130: Neighbor Interface Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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 130: 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. |
Table 130: Neighbor Interface Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure static Layer 2 circuit pseudowires.</td>
<td>1. Click <strong>Interface</strong> next to neighbor.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Interface.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Static</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>Incoming Label</strong> list, select the incoming label for the static pseudowire. Range: 1000000 through 1048575</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Outgoing Label</strong> list, select the outgoing label for the static pseudowire. Range: 299776 through 1048575</td>
</tr>
<tr>
<td></td>
<td>7. Select the <strong>Send Oam</strong> check box to send oam.</td>
</tr>
</tbody>
</table>

**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 131 on page 263.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.

Table 131: 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>
Table 131: Layer2 Circuit Traceoption 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. This is the default setting. |

Specify the tracing operation to perform.

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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 of 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 BDUs 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 132 on page 265.

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

### Table 132: Layer2 Circuit Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Enable BPDU blocking on an interface | 1. Click **Bpdu Block** next to Layer2 Control.  
2. In the **Comment** box, enter the comment.  
3. From the **Disable Timeout** list, select the disable timeout value.  
   Range: 10 through 3600  
   Default: If this option is not configured, the interface is not periodically checked and remains disabled  
4. Click **Interface** next to Bpdu Block.  
5. Click **Add new entry** next to Interface.  
6. In the **Name** box, enter the interface name.  
7. In the **Comment** box, enter the comment. |

| 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. |
Table 132: Layer2 Circuit Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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 277  
■ Configuring Layer 2 Address Learning and Forwarding Properties (NSM Procedure) on page 257

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 133 on page 268.

5. Click one:
   - OK – To save the changes
   - Cancel – To cancel the modifications
### Table 133: LDP Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure LDP.</td>
<td>1. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>2. From the <strong>Preference</strong> list, select the route preference level for LDP routes.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 4294967295</td>
</tr>
<tr>
<td></td>
<td>3. Select the <strong>No Forwarding</strong> check box to omit the Ingress routes from the inet.0 routing table.</td>
</tr>
<tr>
<td></td>
<td>4. Select the <strong>L2 Smart Policy</strong> check box to prevent LDP from exporting IPv6 FECs over sessions with layer 2 neighbors.</td>
</tr>
<tr>
<td></td>
<td>5. Select the <strong>Track IGP Metric</strong> check box to cause the IGP route metric to be used for the LDP routes instead of the default LDP route metric.</td>
</tr>
<tr>
<td></td>
<td>6. Select the <strong>Strict Targeted Hellos</strong> check box to prevent LDP sessions from being established with remote neighbors that have not been specifically configured.</td>
</tr>
<tr>
<td></td>
<td>7. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>deaggregate</strong>—To control forwarding equivalence class (FEC) deaggregation on the router.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>no-deaggregate</strong>—To control forwarding equivalence class (FEC) aggregation on the router.</td>
</tr>
<tr>
<td></td>
<td>8. Select the <strong>Explicit Null</strong> check box to advertise label 0 to the egress router of a label-switched path (LSP).</td>
</tr>
<tr>
<td></td>
<td>9. From the <strong>Label Withdrawal Delay</strong> list, select the number of seconds to wait before withdrawing labels for the LDP LSPs.</td>
</tr>
<tr>
<td></td>
<td>■ Default: 60 seconds</td>
</tr>
<tr>
<td></td>
<td>■ Range: 0 through 120 seconds</td>
</tr>
<tr>
<td></td>
<td>10. From the <strong>Keep Alive Interval</strong> list, select a Keep Alive value.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 65,535 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 10 seconds</td>
</tr>
<tr>
<td></td>
<td>11. From the <strong>Keep Alive Timeout</strong> list, select a Keep Alive Timeout value.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 65,535 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 30 seconds</td>
</tr>
<tr>
<td>Configure the prefixes advertised into LDP from the routing table.</td>
<td>1. Expand LDP.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Egress Policy</strong> next to LDP.</td>
</tr>
<tr>
<td></td>
<td>3. 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>4. 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>5. Click <strong>Add All</strong> to add all the Non members to the Members list.</td>
</tr>
<tr>
<td></td>
<td>6. Click <strong>Remove All</strong> to remove all the members from the Members list.</td>
</tr>
</tbody>
</table>
### Table 133: 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 133: 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:  
   a. **router-id**—The router identifier is used as the transport address  
   b. **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 133: 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 133: 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 133: 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:  
   - **bfd-liveness-detection**—To enable BFD for all MPLS LSPs or for just a specific LSP.  
   - **no-bfd-liveness-detection**—To disable BFD for all MPLS LSPs or for just a specific LSP.  
6. Click **Periodic Traceroute** next to fec.  
7. In the **Comment** box, enter the comment.  
8. From the **Frequency** list, select the interval between traceroute attempts.  
   Range: 15 through 120 minutes  
9. From the **Ttl** list, select the maximum time-to-live value.  
   Range: 1 through 255  
10. From the **Retries** list, select the number of attempts to send a probe to a specific node before giving up.  
   Range: 1 through 9  
11. From the **Wait** list, select the wait interval before resending a probe packet.  
   Range: 5 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 |

| 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. |
<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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 through 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 |
| Enable policing of forwarding equivalence classes (FECs) for LDP.    | 1. Click Policing next to Ldp.  
2. In the Comment box, enter the comment.  
3. Click Fec next to Policing.  
4. Click Add new entry next to Fec.  
5. In the Name box, enter the address for the FEC.  
6. In the Comment box, enter the comment.  
7. From the Ingress Traffic list, select the name of the filter for policing ingress FEC traffic.  
8. From the Transit Traffic list, select the name of the filter for policing transit FEC traffic. |
| Specify the LDP session to which you want to attach the Transmission Control Protocol (TCP) MD5 signature. | 1. Click Session next to Ldp.  
2. Click Add new entry next to Session.  
3. In the Name box, enter the address for the remote end of the LDP session.  
4. In the Comment box, enter the comment.  
5. In the Authentication Key box, enter the authentication key.  
6. From the Authentication Algorithm list, select the algorithm.  
7. In the Authentication Key Chain box, enter the MD5 authentication signature. The maximum length of the authentication signature is 69 characters. |
### Table 133: LDP Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure session protection. | 1. Click **Session Protection** next to Ldp.  
2. From the **Timeout** list, select the session protection timeout.  
   Range: 1 through 65535 |
| Specify parameters for targeted hellos. | 1. Click **Targeted Hello** next to Ldp.  
2. In the **Comment** box, enter the comment.  
3. From the **Hello Interval** list, select the hello interval in seconds.  
   Range: 1 through 65535  
4. From the **Hold Time** list, select the hold time interval in seconds.  
   Range: 1 through 65535 |
| 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. |
Table 133: LDP Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure LDP traffic statistics.</td>
<td>1. Click <strong>Traffic Statistics</strong> next to Ldp.&lt;br&gt;2. In the <strong>Comment</strong> box, enter the comment.&lt;br&gt;3. From the <strong>Interval</strong> list, select the interval at which the statistics are polled and written to the file.&lt;br&gt;   Range: 60 through 65535&lt;br&gt;4. Select <strong>No Penultimate Hop</strong> check box to disable penultimate hop statistics collection.&lt;br&gt;5. Click <strong>File</strong> next to Traffic Statistics.&lt;br&gt;6. In the <strong>Comment</strong> box, enter the comment for the file.&lt;br&gt;7. In the <strong>Filename</strong> box, enter the name of the file to receive the output of the tracing operation.&lt;br&gt;8. In the <strong>Size</strong> box, enter the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).&lt;br&gt;9. From the <strong>Files</strong> list, select the maximum number of trace files.&lt;br&gt;   Range: 2 through 1000.&lt;br&gt;10. Select one of the following:&lt;br&gt;   ■ <strong>world-readable</strong>—To enable unrestricted file access.&lt;br&gt;   ■ <strong>no-world-readable</strong>—To restrict file access to owner. This is the default setting.</td>
</tr>
<tr>
<td>Allow control of the transport address used by LDP.</td>
<td>1. Click <strong>Transport Address</strong> next to Ldp.&lt;br&gt;2. In the <strong>Comment</strong> box, enter the comment.&lt;br&gt;3. Click <strong>Router Id</strong> next to Transport Address.&lt;br&gt;4. Select one of the following:&lt;br&gt;   ■ <strong>router-id</strong>—The router identifier is used as the transport address.&lt;br&gt;   ■ <strong>interface</strong>—The first IP address on the interface is used as the transport address.&lt;br&gt;   ■ <strong>address</strong>—IP address to be advertised as the transport address.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Configuring the ILMI Protocol (NSM Procedure) on page 255
- Configuring RSVP (NSM Procedure) on page 287
- Configuring Link Management Protocol (NSM Procedure) on page 277
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 134 on page 278.
5. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.
Table 134: 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 Peer next to Link Management.</td>
</tr>
<tr>
<td></td>
<td>2. Click Add new entry next to Peer.</td>
</tr>
<tr>
<td></td>
<td>3. In the Name box, enter the name of the peer.</td>
</tr>
<tr>
<td></td>
<td>4. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>5. In the Address box, enter the ID of the peer.</td>
</tr>
<tr>
<td></td>
<td>7. Click Control Channel next to Peer.</td>
</tr>
<tr>
<td></td>
<td>8. Click Add new entry 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>
<tr>
<td></td>
<td>10. Click Lmp Control Channel next to peer.</td>
</tr>
<tr>
<td></td>
<td>11. Click Add new entry next to Lmp Control Channel.</td>
</tr>
<tr>
<td></td>
<td>12. In the Name box, enter the peer name.</td>
</tr>
<tr>
<td></td>
<td>13. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>14. 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>15. Click Lmp Protocol next to peer.</td>
</tr>
<tr>
<td></td>
<td>16. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>17. From the Hello Interval list, select how often the router sends Link Management Protocol (LMP) hello packets. Range: 150 through 21845 Default: 150 milliseconds</td>
</tr>
<tr>
<td></td>
<td>18. From the Hello Dead Interval list, select how long the Link Management Protocol (LMP) waits before declaring the control channel to be dead. Range: 500 through 300,000 Default: 500 milliseconds (three times the hello interval)</td>
</tr>
<tr>
<td></td>
<td>19. From the Retransmission Interval list, select how often Link Management Protocol (LMP) sends Config and LinkSummary messages on the LMP control channel. Range: 500 through 300,000 Default: 500 milliseconds</td>
</tr>
<tr>
<td></td>
<td>20. From the Retry Limit list, select the maximum number of times messages are sent without receiving an acknowledgment. Range: 3 through 1000 Default: 3</td>
</tr>
<tr>
<td></td>
<td>21. 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>22. Click Te-Link next to peer.</td>
</tr>
<tr>
<td></td>
<td>23. Click Add new entry next to Te-Link.</td>
</tr>
<tr>
<td></td>
<td>24. In the dialog box, enter the name of the te-link to be associated with this peer.</td>
</tr>
</tbody>
</table>
**Table 134: 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 287  
■ Configuring Layer 2 Circuit (NSM Procedure) on page 258
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 135 on page 280.

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>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>
</tbody>
</table>
### Table 135: MSTP Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bpdu Block on Edge</td>
<td>Specifies whether Bpdu blocks must be processed.</td>
<td>Select to enable the feature.</td>
</tr>
<tr>
<td>Interface</td>
<td>Specifies MSTP settings for the interface.</td>
<td>1. Click the expand icon.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Specify the interface name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the port priority.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Specify the path cost. MSTP uses the path cost when selecting an</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interface to place into the forwarding state. A lower path cost</td>
</tr>
<tr>
<td></td>
<td></td>
<td>represents higher-speed transmission.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Specify the mode. The link type can be shared or point-to-point.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. Select Edge to enable the feature.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7. Select No root port if it is not specified.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8. Click OK.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9. Specify the Bpdu timeout action:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Block</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Alarm</td>
</tr>
<tr>
<td>Msti</td>
<td>Specifies MST instances settings for an interface or VLAN.</td>
<td>1. Specify the Msti ID.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter a comment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the bridge priority.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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 136 on page 282.

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>
<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 136: OSPF Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Specifies the comment for OSPF.</td>
<td>1. Enter the comment.</td>
</tr>
<tr>
<td>Disable</td>
<td>Specifies whether to disable the OSPF configuration.</td>
<td>1. Specify whether to enable or disable OSPF.</td>
</tr>
<tr>
<td></td>
<td>- To enable OSPF, clear the check box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- To disable OSPF, select the check box.</td>
<td></td>
</tr>
<tr>
<td>Prefix Export Limit</td>
<td>Configure a limit to the number of prefixes to be exported.</td>
<td>1. Enter the prefix export limit or select from the list.</td>
</tr>
<tr>
<td>Rib Group</td>
<td>Specifies the routing table group.</td>
<td>1. Select rib group from the list.</td>
</tr>
<tr>
<td>Route Type Community</td>
<td>Specifies an extended community value to encode the OSPF route type.</td>
<td>1. Select route type community from the list.</td>
</tr>
<tr>
<td>Domain VPN Tag</td>
<td>Virtual private network (VPN) tag for OSPFv2 external routes generated by the provider edge (PE) router.</td>
<td>1. Enter the domain VPN tag or select from the list.</td>
</tr>
<tr>
<td>Preference</td>
<td>Specifies the route preference for OSPF internal routes.</td>
<td>1. Enter the preference or select from the list.</td>
</tr>
<tr>
<td>External Preference</td>
<td>Specifies the external route preference.</td>
<td>1. Enter the external route preference or select from the list.</td>
</tr>
<tr>
<td>Reference Bandwidth</td>
<td>Specifies the reference bandwidth used in calculating the default interface cost.</td>
<td>1. Enter the reference bandwidth.</td>
</tr>
<tr>
<td>No RFC 1583</td>
<td>Disable compatibility with RFC 1583. Disabling compatibility with RFC 1583 can prevent routing loops.</td>
<td>1. Specify whether to configure RFC 1583.</td>
</tr>
<tr>
<td></td>
<td>- To enable compatibility with RFC 1583, clear the check box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- To disable compatibility with RFC 1583, select the check box.</td>
<td></td>
</tr>
<tr>
<td>No NSSA ABR</td>
<td>Disable compatibility with NSSA ABR.</td>
<td>1. Specify whether NSSA ABR has to be configured.</td>
</tr>
<tr>
<td></td>
<td>- To enable NSSA ABR, clear the check box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- To disable NSSA ABR, select the check box.</td>
<td></td>
</tr>
<tr>
<td>Area</td>
<td>Enables you to set up the area details for OSPF.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 136: OSPF Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain ID</td>
<td>Enables you to configure domain ID for the OSPF.</td>
<td>1. Expand the <strong>OSPF</strong> tree and select <strong>Domain ID</strong>. 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>. 2. Specify the export policies.</td>
</tr>
<tr>
<td>Graceful Restart</td>
<td>Enables you to specify the graceful restart parameters for OSPF.</td>
<td>1. Expand the <strong>OSPF</strong> tree and select <strong>Graceful Restart</strong>. 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>. 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>. 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>. 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>. 2. Specify the comment, delay, holddown and rapid runs.</td>
</tr>
</tbody>
</table>
Table 136: OSPF Configuration Fields (continued)

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

Configuring RIP (NSM Procedure)

Routing Information Protocol (RIP) is an interior gateway protocol (IGP) typically used in small, homogeneous networks. RIP uses distance-vector routing to route information through IP networks. Distance-vector routing requires that each device simply informs its neighbors of its routing table. For each network path, the receiving device picks the neighbor advertising the lowest metric, then adds this entry into its routing table for readvertisement. Any host that uses RIP is assumed to have interfaces to one or more networks. These networks are considered to be directly connected networks. RIP relies on access to certain information about each of these networks. The most important information is the network's metric. RIP uses the hop count as the metric (also known as cost) to compare the value of different routes. The hop count is the number of devices that data packets must traverse between RIP networks.

To configure RIP in NSM:

1. In the navigation tree select Device Manager > Devices.
2. In the Devices list, double click the device to select it.
3. Click the Configuration tab.
4. In the configuration tree, expand Protocols and select Rip.
5. Add/Modify the parameters under the respective tabs as specified in Table 137 on page 286.
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 137: RIP Configuration Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP</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>
</tbody>
</table>
| Group        | RIP neighbors that share an export policy and metric. The export policy and metric govern what routes to advertise to neighbors in a given group. | 1. Expand the RIP tree and select Group.  
2. Click the New button or select a group and click Edit button.  
3. Set up the Bfd Liveness Detection , Export, Import and Neighbor for RIP. |
| Import       | Enables you to specify the import policies to be configured on the peer. | 1. Expand the RIP tree and select Import.  
2. Specify the import policies.                                     |
| Receive      | Enables you to configure RIP receive options.                            | 1. Expand the RIP tree and select Receive.  
2. Specify the receive options.                                        |
Table 137: RIP Configuration Fields (continued)

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

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 138 on page 288.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.
Table 138: 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 Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. Select the Disable check box to explicitly disable RSVP or RSVP graceful</td>
</tr>
<tr>
<td></td>
<td>restart.</td>
</tr>
<tr>
<td></td>
<td>4. Select the No-P2mp-Sublsp check box to reject Resv messages which</td>
</tr>
<tr>
<td></td>
<td>include the S2L_SUB_LSP object.</td>
</tr>
<tr>
<td></td>
<td>5. From the Refresh Time 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 Keep Multiplier 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 Graceful Deletion-Timeout list, select the time before completing</td>
</tr>
<tr>
<td></td>
<td>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 seconds                                             |
|                                                          | Default: 0 (disabled)                                                      |

| 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)                                                      |
Table 138: RSVP Configuration Details *(continued)*

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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 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.  
11. From the **Update Threshold** list, select the percentage change in bandwidth to trigger an Interior Gateway Protocol (IGP) update.  
   Range: 1 through 60 seconds  
   Default: 9 seconds |
Table 138: RSVP Configuration Details (continued)

<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  
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 Csdp** 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.  |
|  | Range: 0 through 7, where 0 is the highest and 7 is the lowest priority  
Default: 7 (The session cannot preempt any existing sessions.)  
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: 0 (Once the session is set up, no other session can preempt it.)  
11. From the **Reservation Priority** list, select the reservation priority.  |


### Table 138: RSVP Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure administrative groups for bypass LSPs. | 1. Click Admin Group next to Link Protection.  
2. Click Exclude next to Admin Group.  
3. Click Add new entry next to Exclude.  
4. In the New exclude window, enter the administrative groups to exclude for a bypass LSP.  
5. Click Include All next to Admin Group.  
6. Click Add new entry next to Include All.  
7. In the New include-all window, enter the administrative groups whose links the bypass LSP must traverse.  
8. Click Include Any next to Admin Group.  
9. Click Add new entry next to Include Any.  
10. In the New include-any window, enter the administrative groups whose links the bypass LSP can traverse. |
| Configuring the bandwidth for bypass LSPs. | 1. Click Bandwidth next to Link Protection.  
2. In the Per Traffic Class Bandwidth box, enter the bandwidth.  
3. In the class-type number box, enter the class-type bandwidth. |
| Configure a bypass LSP | 1. Click Bypass next to Link Protection.  
2. Click Add new entry next to Bypass.  
3. Click Admin Group next to Bypass.  
4. Click Exclude next to Admin Group.  
5. Click Add new entry next to Exclude.  
6. In the New exclude window, enter the administrative groups to exclude for a bypass LSP.  
7. Click Include All next to Admin Group.  
8. Click Add new entry next to Include All.  
9. In the New include-all window, enter the administrative groups whose links the bypass LSP must traverse.  
10. Click Include Any next to Admin Group.  
11. Click Add new entry next to Include Any.  
12. In the New include-any window, enter the administrative groups whose links the bypass LSP can traverse.  
13. Click Bandwidth next to Link Protection.  
14. In the Per Traffic Class Bandwidth box, enter the bandwidth.  
15. In the class-type number box, enter the class-type bandwidth.  
16. Click Path next to Bypass.  
17. Click Add new entry next to Path.  
18. In the Name box, enter the IP address of each transit router in the LSP.  
19. Select one of the following:  
   - loose—If the LSP can traverse other routers before reaching this router.  
   - strict—If the LSP must go to the next address specified in the path statement without traversing other nodes. |
### Configuring an explicit path for bypass LSPs

1. Click **Path** next to Link Protection.
2. Click **Add new entry** next to Path.
3. In the **Name** box, enter the IP address of each transit router in the LSP.
4. In the **Comment** box, enter the comment.
5. Select one of the following:
   - **loose**—If the LSP can traverse other routers before reaching this router.
   - **strict**—If the LSP must go to the next address specified in the path statement without traversing other nodes.

### Configuring the bandwidth subscription percentage for LSPs

1. Click **Subscription** next to interface.
2. In the **Link Subscription** box, enter the class-type bandwidth that RSVP allows to be used for reservations.
3. In the class-type number percentage box, enter the percent of class-type bandwidth. You can specify bandwidth subscriptions for class types 0 through 3.

### Configuring load balancing across RSVP LSPs

1. Click **Load Balance** next to Rsvp.
2. In the **Comment** box, enter the comment.
3. Select the **Bandwidth** check box to load-balance traffic between RSVP LSPs based on the bandwidth configured for each LSP.

### Configuring RSVP for LMP peer interfaces

1. Click **Peer Interface** next to Rsvp.
2. Click **Add new entry** next to Peer Interface.
3. In the **Name** box, enter the peer interface name.
4. In the **Comment** box, enter the comment.
5. Select **Disable** check box Explicitly disable RSVP or RSVP graceful restart.
6. In the **Authentication Key** box, enter the authentication key (password).
7. Select one of the following:
   - **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

---

**Table 138: RSVP Configuration Details (continued)**

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configuring an explicit path for bypass LSPs. | 1. Click **Path** next to Link Protection.  
2. Click **Add new entry** next to Path.  
3. In the **Name** box, enter the IP address of each transit router in the LSP.  
4. In the **Comment** box, enter the comment.  
5. Select one of the following:  
   - **loose**—If the LSP can traverse other routers before reaching this router.  
   - **strict**—If the LSP must go to the next address specified in the path statement without traversing other nodes. |
| Configuring the bandwidth subscription percentage for LSPs. | 1. Click **Subscription** next to interface.  
2. In the **Link Subscription** box, enter the class-type bandwidth that RSVP allows to be used for reservations.  
3. In the class-type number percentage box, enter the percent of class-type bandwidth. You can specify bandwidth subscriptions for class types 0 through 3. |
| Configuring load balancing across RSVP LSPs. | 1. Click **Load Balance** next to Rsvp.  
2. In the **Comment** box, enter the comment.  
3. Select the **Bandwidth** check box to load-balance traffic between RSVP LSPs based on the bandwidth configured for each LSP. |
| Configuring RSVP for LMP peer interfaces. | 1. Click **Peer Interface** next to Rsvp.  
2. Click **Add new entry** next to Peer Interface.  
3. In the **Name** box, enter the peer interface name.  
4. In the **Comment** box, enter the comment.  
5. Select **Disable** check box Explicitly disable RSVP or RSVP graceful restart.  
6. In the **Authentication Key** box, enter the authentication key (password).  
7. Select one of the following:  
   - **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 |
### Table 138: 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.  
  - Select **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  
   - Select **no-world-readable**—To restrict the file access to owner.  
   - Select **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 277
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 139 on page 294.
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 139: VRRP Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Startup Silent Period | Enables the system to ignore the Master Down Event when an interface transitions from the disabled state to the enabled state. It avoids an incorrect error alarm caused by delay or interruption of incoming VRRP advertisement packets during the interface startup phase. | 1. Expand the Protocol tree and select VRRP.  
2. Enter the startup silent period or select from the list. |

Traceoptions | Enables you to configure VRRP level tracing options. | 1. Expand the Protocol tree.  
2. Select VRRP and expand the tree.  
3. Select Traceoptions.  
4. Set up the file and flag parameters. | 

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 140 on page 296.
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 140: 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 <strong>Protocol</strong> tree and select <strong>VSTP</strong>.</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 <strong>Protocol</strong> tree and select <strong>VSTP</strong>.</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 <strong>Protocol</strong> tree and select <strong>VSTP</strong>.</td>
</tr>
<tr>
<td></td>
<td>If two bridges have the same path cost to the root bridge, the bridge priority determines which bridge becomes the designated bridge for a LAN segment.</td>
<td>2. Enter the bridge priority.</td>
</tr>
<tr>
<td>Max Age</td>
<td>Specifies the maximum age of received protocol BPDUs.</td>
<td>1. Expand the <strong>Protocol</strong> tree and select <strong>VSTP</strong>.</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 <strong>Protocol</strong> tree and select <strong>VSTP</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the hello time or select from the list.</td>
</tr>
<tr>
<td>Forward Delay</td>
<td>Specifies how long a bridge interface remains in the listening and learning states before transitioning to the forwarding state.</td>
<td>1. Expand the <strong>Protocol</strong> tree and select <strong>VSTP</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the forward delay time or select from the list.</td>
</tr>
<tr>
<td>Interface</td>
<td>Specifies the interface to be associated with VSTP.</td>
<td>1. Expand the <strong>Protocol</strong> tree.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select <strong>VSTP</strong> and expand the tree.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Select <strong>Interfaces</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Set up the priority, cost, mode, edge and specify whether the interface has to be disabled.</td>
</tr>
<tr>
<td>Traceoptions</td>
<td>Enables you to configure VSTP level tracing options.</td>
<td>1. Expand the <strong>Protocol</strong> tree.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select <strong>VSTP</strong> and expand the tree.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Select <strong>Traceoptions</strong>.</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 297
- Configuring Dynamic Tunnels (NSM Procedure) on page 298
- Configuring Fate Sharing (NSM Procedure) on page 300
- Configuring Flow Route (NSM Procedure) on page 302
- Configuring Forwarding Table (NSM Procedure) on page 304
- Configuring Generated Routes (NSM Procedure) on page 305
- Configuring Instance Export (NSM Procedure) on page 306
- Configuring Instance Import (NSM Procedure) on page 307
- Configuring Interface Routes (NSM Procedure) on page 308
- Configuring Martian Addresses (NSM Procedure) on page 309
- Configuring Maximum Paths (NSM Procedure) on page 310
- Configuring Maximum Prefixes (NSM Procedure) on page 311
- Configuring Multicast (NSM Procedure) on page 313
- Configuring Options (NSM Procedure) on page 316
- Configuring Routing Tables (NSM Procedure) on page 317
- Configuring Routing Table Groups (NSM Procedure) on page 319
- Configuring Source Routing (NSM Procedure) on page 320
- Configuring Static Routes (NSM Procedure) on page 321
- Configuring Traceoptions (NSM Procedure) on page 323

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 141 on page 298.
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 141: 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 confederation.</td>
<td>Enter a comment.</td>
</tr>
<tr>
<td>Confederation As</td>
<td>Specifies the confederation AS number.</td>
<td>Enter a number from 1 through 65535.</td>
</tr>
<tr>
<td>Members</td>
<td>Specifies the AS number of the confederation member, allowing you to add</td>
<td>1. Expand the Confederation tree and select Members.</td>
</tr>
<tr>
<td></td>
<td>members to the confederation.</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 142 on page 299.
6. Click one:
   - OK— Saves the changes.
   - Cancel— Cancels the modifications.

Table 142: 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</td>
</tr>
<tr>
<td></td>
<td>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>
Table 142: Dynamic Tunnels Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</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 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 143 on page 301.

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 143: 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>
</tbody>
</table>

**Group**

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Name | Specifies the name of the fate sharing group. | 1. Expand the **Fate Sharing** tree and select **Group**.  
2. Click the New button or select a group and click the Edit button.  
3. Enter the group name. |
| Comment | Specifies the comment for the fate sharing group. | 1. Expand the **Fate Sharing** tree and select **Group**.  
2. Click the New button or select a group and click the Edit button.  
3. Enter the comment. |
| Cost | Specifies the configurable cost attributed to each group, which represents the level of impact this group has on CSPF computations. The higher the cost, the less likely a backup path will share any objects in the group with the primary path. | 1. Expand the **Fate Sharing** tree and select **Group**.  
2. Click the New button or select a group and click the Edit button.  
3. Enter the cost or select a value from the list. |
### 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 144 on page 303.
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 144: 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><strong>Route</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the name of the flow route.</td>
<td>1. Expand the <strong>Flow</strong> tree and select <strong>Route</strong>.</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 <strong>Flow</strong> tree and select <strong>Route</strong>.</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><strong>Match</strong></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 <strong>Route</strong> tree and select <strong>Match</strong>.</td>
</tr>
<tr>
<td></td>
<td>■ Destination Port</td>
<td>2. Enter a comment for <strong>Comment</strong>, a destination address for <strong>Destination</strong>, and a source address for <strong>Source</strong>.</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>■ Source Port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Tcp Flag</td>
<td></td>
</tr>
<tr>
<td><strong>Then</strong></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 <strong>Route</strong> tree and select <strong>Then</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Configure the then conditions for the packet.</td>
</tr>
<tr>
<td><strong>Validation</strong></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 <strong>Flow</strong> tree and select <strong>Validation</strong>.</td>
</tr>
<tr>
<td>Comment</td>
<td></td>
<td>2. Enter the comment for the validation procedure.</td>
</tr>
</tbody>
</table>


### Table 144: Flow Route 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 define tracing operations that track all routing protocol</td>
<td>1. Expand the Validation tree and select Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>functionality in the device and specify that tracing results be saved in</td>
<td>2. Expand the Traceoptions tree and configure the file and flag parameters,</td>
</tr>
<tr>
<td></td>
<td>a log file. You can configure the tracing flag, filter, and the tracing</td>
<td>and the tracing policy.</td>
</tr>
<tr>
<td></td>
<td>policy.</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Forwarding Table (NSM Procedure)

A forwarding table contains the routes actually used to forward packets through the device to their next-hop destination. This feature enables you to configure forwarding table in NSM.

To configure forwarding table in NSM:

1. In the navigation tree, select Device Manager > Devices.
2. In the Devices list, double click the device to select it.
3. Click the Configuration tab.
4. In the configuration tree, expand Routing Options.
5. Select Forwarding Table.
6. Add or modify the parameters as specified in Table 145 on page 304.
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 145: 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>
Table 145: Forwarding Table Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>indirect-next-hop</td>
<td>Specifies that the forwarding table supports indirectly connected next hops.</td>
<td>Select the option button to enable indirect-next-hop.</td>
</tr>
<tr>
<td>no-indirect-next-hop</td>
<td>Specifies that the forwarding table does not support indirectly connected next hops.</td>
<td>Select the option button to enable no-indirect-next-hop.</td>
</tr>
<tr>
<td>Unicast Reverse Path</td>
<td>Enables you to check path validity to protect the network from IP spoofing. A unicast reverse-path-forwarding (RPF) check performs a routing table lookup on an IP packet’s source address and checks the incoming interface. The device determines whether the packet is arriving from a path that the sender would use to reach the destination. If the packet is from a valid path, the device forwards the packet to the destination address. If it is not from a valid path, the device discards the packet.</td>
<td>Select the path from the drop-down list.</td>
</tr>
</tbody>
</table>
| Export             | Enables you to apply one or more policies to routes being exported from the routing table into the forwarding table. | 1. Expand the Forwarding Table tree and select Export.  
2. Enter the export policies. |

**Configuring 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 146 on page 306.
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 generated route.</td>
<td>Enter a comment.</td>
</tr>
<tr>
<td>Defaults</td>
<td>Enables you to specify globally generated route options. These are treated as global defaults and apply to all the generated routes you configure.</td>
<td>1. Expand the Generate tree and select Defaults. 2. Configure the default route options.</td>
</tr>
<tr>
<td>Route</td>
<td>Enables you to configure individually generated routes. You can also configure globally generated route options. These options apply to the individual destination only and override any options you configured in Defaults.</td>
<td>1. Expand the Generate tree and select Route. 2. Configure the individual route options.</td>
</tr>
</tbody>
</table>

**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 147 on page 308.
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 147: 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>
| Family | Specifies the address family as IPv4 or IPv6. | 1. Expand the Interface Routes tree and select Family.  
2. Use the New button or select a family name and click the Edit button.  
3. Enter the family name and comment.  
4. Set up the export policy and import policy. |
### Table 147: Interface Routes Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rib Group</td>
<td>Specifies the routing table groups to which interface routes are imported.</td>
<td>1. Expand the Interface Routes tree and select Rib Group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the comment and Inet.</td>
</tr>
</tbody>
</table>

### 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 148 on page 309.
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 148: Configuring Martian Address Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Specifies the martian address or the destination prefix of a series of martian addresses that are to be allowed or disallowed.</td>
<td>1. Click the New button or select a martian address and click the Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the address.</td>
</tr>
</tbody>
</table>
Table 148: Configuring Martian Address 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 martian address.</td>
<td>1. Click the New button or select a martian address and click the Edit button. 2. Enter the comment for the martian address.</td>
</tr>
<tr>
<td>Allow</td>
<td>Enables you to explicitly allow a subset of a range of addresses that are to be disallowed.</td>
<td>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.</td>
</tr>
<tr>
<td>Exact</td>
<td>Specifies match criteria for the route’s mask length with the martian address. The criteria are: - Exact - Longer - Orlonger - Upto - Through - Prefix Length Range</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 149 on page 311.
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 149: Configuring Maximum Paths 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 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: | 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 150 on page 312.
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 150: Configuring Maximum Prefixes 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 maximum prefix limit.</td>
<td>Enter the comment.</td>
</tr>
<tr>
<td>Limit</td>
<td>Indicates the maximum number of route prefixes. If this limit is reached, a warning is triggered and additional routes are rejected.</td>
<td>Enter limit value or select from the list.</td>
</tr>
<tr>
<td>Log Interval</td>
<td>Indicates the minimum time interval (in seconds) between log messages.</td>
<td>Enter the log interval value or select from the list.</td>
</tr>
</tbody>
</table>
| Threshold    | Specifies what is to be done when the routing table reaches the maximum prefix value. The options are: | 1. Expand the Maximum Prefixes tree and select **Threshold**.  
   - None—No action is to be taken.  
   - threshold—You can configure a percentage for the maximum number of prefixes, which when installed, triggers the warning.  
   - log-only—Sets the prefix limit as an advisory limit. An advisory limit triggers only a warning, and additional routes are not rejected. |

---

**M-series and MX-series Devices**
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 151 on page 313.
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 151: 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 151: Configuring Multicast Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Map</td>
<td>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.</td>
<td>1. Expand the Multicast tree and select Flow Map.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the New button or select a flow map and click the Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Configure the following to create and define a flow map:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Enter the flow map name and comment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Bandwidth—Specify the bandwidth property of the multicast flow map.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Policy—Specify the flow map policies.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Redundant Sources—Specify the addresses for use as backup sources for multicast flows defined by a flow map.</td>
</tr>
<tr>
<td>Forwarding Cache</td>
<td>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.</td>
<td>1. Expand the Multicast tree and select Forwarding Cache.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Configure the timeout and threshold values.</td>
</tr>
</tbody>
</table>
Table 151: Configuring Multicast Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Enables you to configure the interfaces for multicast properties on which you plan to manage the maximum bandwidth.</td>
<td>1. Expand the Multicast tree and select Interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Configure the interface and the bandwidth.</td>
</tr>
<tr>
<td>Rpf Check Policy</td>
<td>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.</td>
<td>1. Expand the Multicast tree and select Rpf Check Policy.</td>
</tr>
<tr>
<td>Scope</td>
<td>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.</td>
<td>1. Expand the Multicast tree and select Scope.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Configure the scope and the interface for the multicast.</td>
</tr>
<tr>
<td>Scope Policy</td>
<td>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.</td>
<td>1. Expand the Multicast tree and select Scope Policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Specify the scope policy for the multicast group.</td>
</tr>
<tr>
<td>Ssm Groups</td>
<td>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).</td>
<td>1. Expand the Multicast tree and select Ssm Groups.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the New button or select a group and click the Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the address range of the SSM group.</td>
</tr>
<tr>
<td>Ssm Map</td>
<td>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.</td>
<td>1. Expand the Multicast tree and select Ssm Map.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the New button or select an SSM map and click the Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the SSM policy for the SSM map and the source address.</td>
</tr>
</tbody>
</table>
Table 151: Configuring Multicast Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traceoptions</td>
<td>Defines tracing options for the multicast group. You can also set up the file management and access control parameters.</td>
<td>1. Expand the Multicast tree and select the Traceoptions tab.  2. Set up the file and flag parameters.</td>
</tr>
</tbody>
</table>

Configuring Options (NSM Procedure)

You can configure the types of system logging messages sent about the routing protocols process to the system log message file. These messages are also displayed on the system console. You can log messages at a particular level or up to and including a particular level.

To configure options in NSM:
1. In the navigation tree, select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. Click the Configuration tab.
4. In the configuration tree, expand Routing Options.
5. Select Options.
6. Enter the parameters as specified in Table 152 on page 316.
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 152: 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>
Table 152: Configuring Options Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</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 153 on page 318.
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 153: Rib 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.</td>
<td>1. Expand the Routing Options tree and select Rib.</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 Routing Options tree and select Rib.</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 Rib and select Aggregate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select the global aggregate route options in Defaults and individual aggregate route options in Route.</td>
</tr>
<tr>
<td>Generate</td>
<td>Enables you to configure generated routes, which are used as routes of last resort in the routing table.</td>
<td>1. Expand the Rib tree and select Generate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select the default route to the destination address in Defaults and individually generated route options in Route.</td>
</tr>
<tr>
<td>Martians</td>
<td>Enables you to configure martian addresses in the routing table.</td>
<td>1. Expand the Rib tree and select Martian.</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 routing table.</td>
<td>1. Expand the Rib tree and select Maximum Paths.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the Maximum Paths and the Threshold.</td>
</tr>
<tr>
<td>Maximum Prefixes</td>
<td>Enables you to configure a limit for the number of routes installed in a routing table.</td>
<td>1. Expand the Rib tree and select Maximum Prefixes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Set up the Maximum Prefixes and the Threshold.</td>
</tr>
</tbody>
</table>
### Table 153: 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 154 on page 320.
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.
## 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.

---

### Table 154: Rib Group Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Name            | Specifies the unique name for the routing table group.                    | 1. Expand the Routing Options tree and select Rib Group.  
|                 |                                                                          | 2. Click the New button or select a routing table group and click the Edit button.                                                            |
|                 |                                                                          | 3. Enter the name for the routing table group.                                                                                                 |
| Comment         | Specifies the comment for the routing table group.                       | 1. Expand the Routing Options tree and select Rib Group.  
|                 |                                                                          | 2. Click the New button or select a routing table group and click the Edit button.                                                            |
|                 |                                                                          | 3. Enter the comment for the routing table group.                                                                                              |
| Export Rib      | Specifies the routing table from which the JUNOS software exports routing information. | 1. Expand the Routing Options tree and select Rib Group.  
|                 |                                                                          | 2. Click the New button or select a routing table group and click the Edit button.                                                            |
|                 |                                                                          | 3. Enter the name of the routing table.                                                                                                       |
| Import Policy   | Enables you to apply one or more policies to routes imported into the routing table group. | 1. Expand the rib-group tree and select Import Policy.  
|                 |                                                                          | 2. Set up the import policies for the routing table group.                                                                                     |
| Import Rib      | Specifies the name of the routing table into which the JUNOS 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. | 1. Expand the rib-group tree and select Import Policy.  
|                 |                                                                          | 2. Enter the name of the routing table.                                                                                                       |
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 155 on page 321.

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 155: 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 addressing family for source routing.</td>
<td>Select the check box.</td>
</tr>
<tr>
<td>Ipv6</td>
<td>Specifies the IPv6 addressing family for source routing.</td>
<td>Select the check box.</td>
</tr>
</tbody>
</table>

---

**Configuring Static Routes (NSM Procedure)**

You can configure static routes for a routing table group. A router uses static routes in the following scenarios:

- When it does not have a route to a destination that has a better (lower) preference value.
- When it cannot determine the route to a destination.
- When it is forwarding unroutable packets.

A static route is installed in the routing table only when the route is active; that is, the list of next-hop routers configured for that route contains at least one next hop on an operational interface.

To configure static routes for a routing table group in NSM:
1. In the navigation tree, select Device Manager > Devices.
2. In the Devices list, double-click the device to select it.
3. Click the Configuration tab.
4. In the configuration tree, expand Routing Options.
5. Select Static.
6. Add or modify the parameters as specified in Table 156 on page 322.
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 156: Static Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Specifies the comment for the static route.</td>
<td>Enter the comment.</td>
</tr>
<tr>
<td>Rib Group</td>
<td>Specifies the routing table group name for which the static route is configured.</td>
<td>Enter the name.</td>
</tr>
</tbody>
</table>
| Defaults | Enables you to configure the global static route options. These options only set the global defaults and apply to all the configured static routes. | 1. Expand the Static tree and select Defaults.  
2. Enter the default route to the destination address. |
| Route | Enables you to configure the individual static routes options. These options apply to the individual destination only and override any options configured in the Defaults section. | 1. Expand the Static tree and select Route.  
2. Enter the individual route. |
**Configuring Traceoptions (NSM Procedure)**

You can configure tracing operations for routing protocols to track all general routing operations and record them in a log file. Any global tracing operations that you configure are inherited by the individual routing protocols. To modify the global tracing operations for an individual protocol, configure the tracing option when configuring that protocol.

To configure tracing options for routing protocols in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the Devices list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Traceoptions**.
6. Add or modify the parameters as specified in Table 157 on page 323.
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><strong>Comment</strong></td>
<td>Specifies the comment for the tracing options.</td>
<td>Enter the comment.</td>
</tr>
<tr>
<td><strong>File</strong></td>
<td>Specifies the file to receive the output of the tracing operation.</td>
<td>1. Expand the <strong>Traceoptions</strong> tree and select <strong>File</strong>. 2. Enter the file parameters.</td>
</tr>
<tr>
<td><strong>Flag</strong></td>
<td>Specifies the global routing protocol tracing options to be performed. You can specify more than one option.</td>
<td>1. Expand the <strong>Traceoptions</strong> tree and select <strong>File</strong>. 2. Enter the flag parameters.</td>
</tr>
</tbody>
</table>
Chapter 22
Configuring Security

Configuring Authentication Key Updates (NSM Procedure) on page 325

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 158 on page 326.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.
### Table 158: Security Authentication Key Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure authentication key updates for BGP and LDP routing protocols. | 1. Expand **Authentication Key Chains**.  
2. Click **Key Chain** next to Authentication Key Chains.  
3. Click **Add new entry** next to Key Chains.  
4. Expand **key-chain**.  
5. In the **Name** box, enter the keychain name.  
6. In the **Comment** box, enter the comment.  
7. In the **Description** box, enter the text description of the authentication keychain in quotes.  
8. From the **Tolerance** list, select the clock skew tolerance.  
   Range: 0 through 999999999  
9. Click **Key** next to key-chain.  
10. Click **Add new entry** next to Key.  
11. From the **Name** list, select the key value.  
12. In the **Comment** box, enter the comment.  
13. In the **Secret** box, enter the secret for the key in encrypted text.  
14. In the **Start Time** box, enter the start time in UTC (Coordinated Universal Time). |
Chapter 23
Configuring Services

- Configuring Adaptive Services PICs (NSM Procedure) on page 327
- Configuring Border Signaling Gateways (NSM Procedure) on page 328
- Configuring Class of Service (NSM Procedure) on page 350
- Configuring Intrusion Detection Service (NSM Procedure) on page 354
- Tracing Services PIC Operations (NSM Procedure) on page 358
- Configuring Network Address Translation (NSM Procedure) on page 359
- Configuring PGCP (NSM Procedure) on page 363
- Configuring Service Interface Pools (NSM Procedure) on page 393
- Configuring a Service Set (NSM Procedure) on page 394
- Configuring Stateful Firewall (NSM Procedure) on page 398

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 159 on page 328.
6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
Table 159: Adaptive Services Pics Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure adaptive services or multiservices PIC tracing operations.</td>
<td>1. Click Traceoptions next to Adaptive Services Pics.</td>
</tr>
<tr>
<td></td>
<td>2. Select the No Remote Trace check box to disable remote tracing.</td>
</tr>
<tr>
<td></td>
<td>3. Expand Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>4. Click File next to Trace Options.</td>
</tr>
<tr>
<td></td>
<td>5. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. In the Filename box, enter the name of the file to receive the output of the tracing operation.</td>
</tr>
<tr>
<td></td>
<td>7. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>9. From the Files list, select the maximum number of trace files.</td>
</tr>
<tr>
<td></td>
<td>10. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>■ no-world-readable—To allow any user to read the log file.</td>
</tr>
<tr>
<td></td>
<td>■ world-readable—To prevent any user from reading the log file.</td>
</tr>
<tr>
<td></td>
<td>11. Click Flag next to Trace Options.</td>
</tr>
<tr>
<td></td>
<td>12. Click Add new entry next to flag.</td>
</tr>
<tr>
<td></td>
<td>13. From the Name list, select a tracing operation to perform.</td>
</tr>
<tr>
<td></td>
<td>14. In the Comment box, enter the comment.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring Service Interface Pools (NSM Procedure) on page 393
- Configuring a Service Set (NSM Procedure) on page 394
- Tracing Services PIC Operations (NSM Procedure) on page 358

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 328

Configuring Gateway Properties (NSM Procedure)
- Configuring Gateway (NSM Procedure) on page 329
- Configuring an Admission Controller (NSM Procedure) on page 329
- Configuring Session Policy Decision Function (NSM Procedure) on page 331
- Configuring Service Point (NSM Procedure) on page 332
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 160 on page 329.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 161 on page 330.
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 161: 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 162 on page 331.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

### Table 162: Session Policy Decision Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the SPDF.</td>
<td>1. Click <strong>Add new entry</strong> next to Gateway.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Embedded Spdf</strong> next to gateway.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td>Configure service classes for the embedded SPDF.</td>
<td>1. Click <strong>Service Class</strong> next to Embedded Spdf.</td>
</tr>
<tr>
<td></td>
<td>2. From the <strong>Service Interface</strong> list, select the name and logical unit number of the Multiservices PIC or DPC.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add new entry</strong> next to Service Class.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Name</strong> box, enter the identifier for the service class.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
</tbody>
</table>
### Table 162: 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 163 on page 333.
6. Click one:  
   - **OK**—Saves the changes.  
   - **Cancel**—Cancels the modifications.
### Table 163: 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 334
- Configuring New Call Usage Policy (NSM Procedure) on page 336
- Configuring New Call Usage Policy Set (NSM Procedure) on page 339
- Configuring New Transaction Policy (NSM Procedure) on page 340
- Configuring a New Transaction Policy Set (NSM Procedure) on page 344
- Configuring Timers (NSM Procedure) on page 345

Configuring Message Manipulation Rules (NSM Procedure)

To configure message manipulation rules in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Services > Border Signaling Gateway**.
4. Select **Gateway**.
5. Add or modify settings as specified in Table 164 on page 334.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 164: 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 <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>Message Manipulation Rules</strong> next to Sip.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
</tbody>
</table>
Table 164: Message Manipulate Rules Configuration Details *(continued)*

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure a manipulation rule. | 1. Click **Manipulation Rule** next to Message Manipulation Rules.  
2. Click **Add new entry** next to Manipulation Rule.  
3. In the **Name** box, enter the name of the manipulation rule.  
4. In the **Comment** box, enter the comment.  
5. Click **Actions** next to manipulation-rule.  
6. In the **Comment** box, enter the comment.  
7. Click **Request Uri** next to Actions.  
8. In the **Comment** box, enter the comment.  
9. Click **Field Value** next to Request Uri.  
10. In the **Comment** box, enter the comment.  
11. Click **Modify Regular Expression** next to Field Value.  
12. Click **Add new entry** next to Modify Regular Expression.  
13. In the **Name** box, enter the regular expression that you want to modify.  
14. In the **Comment** box, enter the comment.  
15. In the **With** box, enter the regular expression that you want to modify followed by the value with which you want to replace the regular expression. |
Table 164: Message Manipulate Rules Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure Session Initiation Protocol (SIP) header. | 1. Click Sip Header next to manipulation-rule.  
2. Click Add new entry next to Sip Header.  
3. In the Name box, enter the name of the header field in SIP headers for which you want to define field values.  
4. In the Comment box, enter the comment.  
5. Click Field Value next to sip-header.  
6. In the Comment box, enter the comment.  
7. Select the Remove All check box to remove all instances of the header field.  
8. Click Add next to Field Value.  
9. Select from the following field values:  
   - **Add**—Adds an instance of the header field with the field value that you define. If the header field already exists, the software creates a new instance of the header field and inserts it before any existing instance of the header field. Having more than one field value is not allowed for some header fields.  
   - **Add Missing**—Adds a new header field with the field value that you define if the header field is missing from the SIP header.  
   - **Add Overwrite**—Adds a new header field with the field value that you define if the header field is missing from the SIP header. If the header field already exists, its field value is overwritten with the new field value. The software overwrites the field value in all instances of the header field.  
   - **Modify Regular Expression**—Changes the value of a regular expression.  
   - **Reject Regular Expression**—Rejects SIP messages and terminates the usage that the message is part of if the header field contains the regular expression.  
   - **Remove Regular Expression**—Removes all of the header fields that have field values that match this regular expression.  
10. Enter the Name and Comment.  

**Configuring New Call Usage Policy (NSM Procedure)**

To configure new call usage policy in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Services > Border Signaling Gateway**.
4. Select **Gateway**.
5. Add or modify settings as specified in Table 165 on page 337.

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

**Table 165: 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>
</tbody>
</table>

| Define the new call usage policy term properties.| 1. Click **Term** next to new-call-usage-policy.                          |
|                                                 | 2. Click **Add new entry** next to Term.                                  |
|                                                 | 3. In the **Name** box, enter the identifier for the term.               |
|                                                 | 4. In the **Comment** box, enter the comment.                            |
Table 165: 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 Regular Expression next to contact.  
9. Click Add new entry next to Regular Expression.  
10. In the New regular-expression window, enter the regular expression used to match the contents of the contact field.  
   Syntax: To specify more than one regular expression, enclose the regular expressions in brackets.  
11. Click Method next to From.  
12. Click Add new entry next to Method.  
13. From the Name list, select method-invite to match the policy to SIP INVITE methods.  
14. In the Comment box, enter the comment.  
15. Click Request Uri next to From.  
16. Click Add new entry next to Request Uri.  
17. In the Comment box, enter the comment.  
18. Click Regular Expression next to request-uri.  
19. In the New regular-expression window, enter the regular expression used to match the contents of the request URI field.  
   Syntax: To specify more than one regular expression, enclose the regular expressions in brackets.  
20. Click Source Address next to From.  
21. Click Add new entry next to Source Address.  
22. In the New source-address window, enter the IP addresses that you want to match.  
   Syntax: To specify more than one IP address, enclose the IP addresses in brackets. |
### Table 165: New Call Usage Policy Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task Description</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define the actions performed on incoming requests that match the new call usage</td>
<td>1. Click <strong>Then</strong> next to From.</td>
</tr>
<tr>
<td>policy.</td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. Select one of the following check boxes:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>accept</strong>—To accept the traffic and send it to its destination.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>reject</strong>—To reject the traffic and return a rejection message. Rejected</td>
</tr>
<tr>
<td></td>
<td>traffic can be logged or sampled.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>trace</strong>—To trace messages accepted by this policy.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Media Policy</strong> next to <strong>Then</strong>.</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 Anchoring</strong> check box to disable or enable media anchoring</td>
</tr>
<tr>
<td></td>
<td>for the policy.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Service Class</strong> box, enter the name of the service class to be</td>
</tr>
<tr>
<td></td>
<td>applied to traffic that matches the new call usage policy.</td>
</tr>
<tr>
<td></td>
<td>8. Click <strong>Data Inactivity Detection</strong> next to <strong>Media Policy</strong>.</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>Inactivity Duration</strong> list, select the time interval that</td>
</tr>
<tr>
<td></td>
<td>determines inactivity. Range: 30 through 3600.</td>
</tr>
</tbody>
</table>

### 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 166 on page 340.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.
Table 166: New Call Usage Policy Set Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure a new call usage policy set. | 1. Click Add new entry next to Gateway.  
2. Click Sip next to gateway.  
3. In the Comment box, enter the comment.  
4. Click New Call Usage Policy Set next to Sip.  
5. Click Add new entry next to New Call Usage Policy Set.  
6. In the Name box, enter the identifier for the new call usage policy set.  
7. In the Comment box, enter the comment. |
| Define the new call usage policies. | 1. Click Policy Name next to new-call-usage-policy-set.  
2. Click Add new entry next to Policy Name.  
3. In the New policy-name window, enter the names of one or more new call usage policies that you want to add to the set.  
Syntax: To specify a list of policies, enclose the policy names in brackets. |

**Configuring New Transaction Policy (NSM Procedure)**

To configure new transaction policy in NSM:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to select it.
3. Click the Configuration tab. In the configuration tree, expand Services > Border Signaling Gateway.
4. Select Gateway.
5. Add or modify settings as specified in Table 167 on page 341.
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 167: 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>
</tbody>
</table>

Define the new transaction policy term properties.  

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define the new transaction policy term</td>
<td>1. Click <strong>Term</strong> next to new-transaction-policy.</td>
</tr>
<tr>
<td>properties.</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 167: Transaction Policy Configuration Details *(continued)*

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure match conditions for a new transaction policy.</td>
<td>1. Click From next to term.</td>
</tr>
<tr>
<td></td>
<td>2. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. Click Add new entry next to Term.</td>
</tr>
<tr>
<td></td>
<td>4. In the Name box, enter the identifier for the term.</td>
</tr>
<tr>
<td></td>
<td>5. Click Contact next to From.</td>
</tr>
<tr>
<td></td>
<td>6. Click Add new entry next to Contact.</td>
</tr>
<tr>
<td></td>
<td>7. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>8. Click Regular Expression next to Contact.</td>
</tr>
<tr>
<td></td>
<td>9. Click Add new entry next to Regular Expression.</td>
</tr>
<tr>
<td></td>
<td>10. In the New regular-expression 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 Method next to From.</td>
</tr>
<tr>
<td></td>
<td>12. Click Add new entry next to Method.</td>
</tr>
<tr>
<td></td>
<td>13. From the Name list, select the type of SIP method.</td>
</tr>
<tr>
<td></td>
<td>14. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>15. Click Request Uri next to From.</td>
</tr>
<tr>
<td></td>
<td>16. Click Add new entry next to Request Uri.</td>
</tr>
<tr>
<td></td>
<td>17. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>18. Click Regular Expression next to request-uri.</td>
</tr>
<tr>
<td></td>
<td>19. In the New regular-expression 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 Source Address next to From.</td>
</tr>
<tr>
<td></td>
<td>21. Click Add new entry next to Source Address.</td>
</tr>
<tr>
<td></td>
<td>22. In the New source-address 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 167: 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 168 on page 344.
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 168: Transaction Policy Set Configuration Details**

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure a new transaction policy set. | 1. Click **Add new entry** next to Gateway.  
2. Click **Sip** next to gateway.  
3. In the **Comment** box, enter the comment.  
4. Click **New Transaction Policy Set** next to Sip.  
5. Click **Add new entry** next to New Transaction Policy Set.  
6. In the **Name** box, enter the identifier for the new transaction policy set.  
7. In the **Comment** box, enter the comment. |

| Define the new transaction policies. | 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 169 on page 345.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

**Table 169: 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 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 Timers next to Sip.</td>
</tr>
<tr>
<td></td>
<td>5. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. From the Inactive Call list, select the maximum time for signaling inactivity. Range: 300 through 86400</td>
</tr>
<tr>
<td></td>
<td>7. From the Timer C 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 170 on page 346.
6. Click one:
   ■ OK—Saves the changes.
   ■ Cancel—Cancels the modifications.

### Table 170: Traceoption BSG Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure border signaling gateway (BSG) tracing operations.         | 1. Click **Add new entry** next to Gateway.
|                                                                     | 2. Click **Traceoptions** next to gateway.
|                                                                     | 3. Click **Flag** next to Traceoptions.
|                                                                     | 4. In the **Comment** box, enter the comment.
|                                                                     | 5. From the **Minimum** list, select the severity of the event being traced:
|                                                                     |   ■ **debug**—Logging of all code flow of control.
|                                                                     |   ■ **trace**—Logging of program trace for START, and EXIT macros.
|                                                                     |   ■ **info**—Summary logs for normal operations e.g. the policy decisions made for a call.
|                                                                     |   ■ **warning**—Failure-recovery or failure of an external entity.
|                                                                     |   ■ **error**—Failure with short-term effect, such as failed processing of a single call.
|                                                                     | 6. From the **Session Trace** list, select the minimum trace level for all session-trace messages. |
| Configure trace level options for the datastore component of the BSG. | 1. Click **Add new entry** next to Gateway.
|                                                                     | 2. Click **Traceoptions** next to gateway.
|                                                                     | 3. Click **Flag** next to Traceoptions.
|                                                                     | 4. Click **Datastore** next to Flag.
|                                                                     | 5. In the **Comment** box, enter the comment.
|                                                                     | 6. From the **Minimum** list, select the minimum trace level for all datastore messages.
|                                                                     | 7. From the **Data** list, select the trace level for the data subcomponent.
|                                                                     | 8. From the **Handle** list, select the trace level for the access API for the database.
|                                                                     | 9. From the **Db** list, select the trace level for the wrapper layer around the database. |
Table 170: Traceoption BSG Configuration Details *(continued)*

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure trace options for the BSG component that provides an infrastructure that enables incremental functionality implementation. | 1. Click **Add new entry** next to Gateway.  
2. Click **Traceoptions** next to gateway.  
3. Click **Flag** next to Traceoptions.  
4. Click **Framework** next to Flag.  
5. In the **Comment** box, enter the comment.  
6. From the **Minimum** list, select the minimum trace level for all framework messages.  
7. From the **Executor** list, select the trace level for the framework subcomponent that executes configured actions for an event, handles any error states, delays processing, and so on.  
8. From the **Action** list, select the trace level for the framework subcomponent that creates, initiates, and manipulates event actions.  
9. From the **Event** list, select the trace level for the framework subcomponent that creates, modifies, and terminates event members.  
10. From the **Freezer** list, select the trace level for the framework subcomponent that delays the execution of an event until certain conditions are met.  
11. From the **Memory Pool** list, select the trace level for the framework subcomponent that creates, deletes, and manipulates memory pools and pool managers, and controls the check-in to and check-out from memory pools of memory objects. |
Table 170: Traceoption BSG Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure trace options for the Signaling Border Controller (SBC) utilities component of the BSG. | 1. Click **Add new entry** next to Gateway.  
2. Click **Traceoptions** next to gateway.  
3. Click **Flag** next to Traceoptions.  
4. Click **Sbc Utils** next to Flag.  
5. In the **Comment** box, enter the comment.  
6. From the **Minimum** list, select the minimum trace level for all sbc-util messages.  
7. From the **Configuration** list, select the trace level for the configuration component of SBC utilities.  
8. From the **Ipc** list, select the trace level for the IPC component of SBC utilities.  
9. From the **Device Monitor** list, select the trace level for the device monitor component of SBC utilities.  
10. From the **Memory Management** list, select the trace level for the memory management component of SBC utilities.  
11. From the **Message** list, select the trace level for the message component of SBC utilities.  
12. From the **Common** list, select the trace level for the common component of SBC utilities.  
13. From the **User Interface** list, select the trace level for the user interface component of SBC utilities.  
14. From the **Memory Pool** list, select the trace level for the message component of SBC utilities.  
15. From the **Memory Pool** list, select the trace level for the memory pool component of SBC utilities. |
Table 170: 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 Add new entry next to Gateway.</td>
</tr>
<tr>
<td></td>
<td>2. Click Traceoptions next to gateway.</td>
</tr>
<tr>
<td></td>
<td>3. Click Flag next to Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>4. Click Signaling next to Flag.</td>
</tr>
<tr>
<td></td>
<td>5. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>6. From the Minimum list, select the minimum trace level for all signaling messages.</td>
</tr>
<tr>
<td></td>
<td>7. From the Sip Stack Wrapper list, select the trace options for the glue layer that receives events from the SIP stack and forwards them to the application and, conversely, receives events from the application and forwards them to the SIP stack.</td>
</tr>
<tr>
<td></td>
<td>8. From the b2b Wrapper list, select the trace options for entry and exit to the BSG signaling application.</td>
</tr>
<tr>
<td></td>
<td>9. From the Ua list, select the trace options for the signaling subcomponent that handles RECEIVE messages.</td>
</tr>
<tr>
<td></td>
<td>10. From the B2b list, select the trace options for the signaling component that implements the b2b logic (translating between dialogs, associating dialogs, creating new downstream dialogs, and so on).</td>
</tr>
<tr>
<td></td>
<td>11. From the Topology Hiding list, select the trace options for the signaling component that hides the network topology of a network by CONTACT replacement and removal or modification of certain headers.</td>
</tr>
<tr>
<td></td>
<td>12. From the Policy list, select the trace options for the signaling component that applies policies for call admission, routing decisions, security settings, and so on.</td>
</tr>
</tbody>
</table>
### Table 170: Traceoption BSG Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Set trace options for the SIP stack component of the BSG. | 1. Click **Add new entry** next to Gateway.  
2. Click **Traceoptions** next to gateway.  
3. Click **Flag** next to Traceoptions.  
4. Click **Sip Stack** next to Flag.  
5. In the **Comment** box, enter the comment.  
6. Select the **Event Tracing** check box to activate or deactivate the stack’s event tracing.  
7. Select the **Event Tracing** check box to activate or deactivate the stack’s event tracing.  
8. Select the **Ips Tracing** check box to activate or deactivate the stack’s IPS tracing.  
9. Select the **Per Tracing** check box to activate or deactivate the stack’s performance tracing.  
10. Select the **Dev Logging** check box to configure development tracing for the stack.  
11. Select the **Verbose Logging** check box to configure verbose tracing for the stack.  
12. From the **Pd Log Level** list, select which types of PD logs are to be printed to the log file. Select one of the following:  
   - **problem**—Problem log messages are sent to the log file.  
   - **exception**—Exception and problem log messages are sent to the log file.  
   - **audit**—All log messages are sent to the log file.  
13. From the **Pd Log Detail** list, select the amount of detail to be sent to the log file. Select one of the following:  
   - **full**—All available information is sent to the log file.  
   - **summary**—The type of logging, the identifier and the first line of the log message are sent to the log file. |

---

### Configuring Class of Service (NSM Procedure)

The Class of Service (CoS) configuration available for the AS PIC enables you to configure Differentiated Services (DiffServ) code point (DSCP) marking and forwarding-class assignment for packets transiting the AS PIC.

To configure CoS in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > CoS**.
4. Add or modify the settings as specified in table Table 171 on page 352.
5. Click one:
- OK—To save the changes.
- Cancel—To cancel the modifications.
Table 171: 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 <strong>Application profile</strong> next to CoS.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add new entry</strong> next to Application Profile.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Name</strong> box, enter the profile name.</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>application-profile</strong>.</td>
</tr>
<tr>
<td></td>
<td>6. Click <strong>Ftp</strong> next to application profile.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>8. Expand <strong>Ftp</strong>.</td>
</tr>
<tr>
<td></td>
<td>9. Click <strong>Data</strong> next to Ftp.</td>
</tr>
<tr>
<td></td>
<td>10. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>11. In the <strong>Dscp</strong> box, enter the DSCP value or alias.</td>
</tr>
<tr>
<td></td>
<td>12. In the <strong>Forwarding Class</strong> box, enter the forwarding class.</td>
</tr>
<tr>
<td></td>
<td>13. Click <strong>Sip</strong> next to Ftp.</td>
</tr>
<tr>
<td></td>
<td>14. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>15. Expand <strong>Sip</strong>.</td>
</tr>
<tr>
<td></td>
<td>16. Click <strong>Video</strong> next to Sip.</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>Dscp</strong> box, enter the name assigned to a set of CoS markers.</td>
</tr>
<tr>
<td></td>
<td>19. In the <strong>Forwarding Class</strong> box, enter the name of the target application.</td>
</tr>
<tr>
<td></td>
<td>20. Click <strong>Voice</strong> next to Sip.</td>
</tr>
<tr>
<td></td>
<td>21. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>22. In the <strong>Dscp</strong> box, enter the DSCP mapping that is applied to the packets.</td>
</tr>
<tr>
<td></td>
<td>23. In the <strong>Forwarding Class</strong> box, enter the name of the target application.</td>
</tr>
</tbody>
</table>

M-series and MX-series Devices

352 Configuring Class of Service (NSM Procedure)
### Table 171: CoS Configuration Details (continued)

<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 CoS.</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 rule the router uses when applying this service.</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>—Match on input to interface.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>output</strong>—Match on output from interface.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>input–output</strong>—Match on input to or output from interface.</td>
</tr>
<tr>
<td></td>
<td>6. Expand <strong>rule</strong>.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>Term</strong> next to rule.</td>
</tr>
<tr>
<td></td>
<td>8. Click <strong>Add new entry</strong> 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>
<tr>
<td></td>
<td>11. Expand <strong>term</strong>.</td>
</tr>
<tr>
<td></td>
<td>12. Click <strong>From</strong> next to term.</td>
</tr>
<tr>
<td></td>
<td>13. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>14. Expand <strong>From</strong>.</td>
</tr>
<tr>
<td></td>
<td>15. From the listed match conditions, select the ones that are applicable for CoS.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>16. Expand <strong>Then</strong>.</td>
</tr>
<tr>
<td></td>
<td>17. Click <strong>Reflexive</strong> next to Then.</td>
</tr>
<tr>
<td></td>
<td>18. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>reflexive</strong>—To apply the equivalent opposing CoS action to flows in the opposite direction.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>reverse</strong>—To define the CoS behavior for flows in the reverse direction.</td>
</tr>
<tr>
<td></td>
<td>a. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>b. In the <strong>Dscp</strong> box, enter the DSCP mapping that is applied to the packets.</td>
</tr>
<tr>
<td></td>
<td>c. In the <strong>Forwarding Class</strong> box, enter the forwarding class to which packets are assigned.</td>
</tr>
<tr>
<td></td>
<td>d. From the <strong>Application Profile</strong> list, select the identifier for the application profile.</td>
</tr>
<tr>
<td></td>
<td>e. Select the <strong>Syslog</strong> check box to enable system logging.</td>
</tr>
</tbody>
</table>
Table 171: CoS 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></td>
</tr>
<tr>
<td>1. Click Rule-Set next to Cos.</td>
<td></td>
</tr>
<tr>
<td>2. Click Add new entry next to Rule-Set.</td>
<td></td>
</tr>
<tr>
<td>3. In the Name box, enter the identifier for the collection of rules that constitute this rule set.</td>
<td></td>
</tr>
<tr>
<td>4. In the Comment box, enter the comment.</td>
<td></td>
</tr>
<tr>
<td>5. Expand Rule-Set.</td>
<td></td>
</tr>
<tr>
<td>6. Click Rule next to rule-set.</td>
<td></td>
</tr>
<tr>
<td>7. Click Add new entry next to Rule.</td>
<td></td>
</tr>
<tr>
<td>8. From the Name list, select the identifier for the collection of terms that constitute this rule.</td>
<td></td>
</tr>
<tr>
<td>9. In the Comment box, enter the comment.</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics
- Configuring Service Interface Pools (NSM Procedure) on page 393
- Configuring a Service Set (NSM Procedure) on page 394

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 172 on page 355.
5. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
### Table 172: IDS Configuration Details

<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 Ids.  
2. Click **Add new entry** next to Rule.  
3. In the **Name** box, enter the identifier for the collection of terms that constitute this rule.  
4. In the **Comment** box, enter the comment.  
5. From the **Match Direction** list, select the direction in which the rule match is applied.  
   - **input**—To apply the rule match on input.  
   - **output**—To apply the rule match on output.  
   - **input-output**—To apply the rule match bidirectionally.  
6. Expand **rule**.  
7. Click **Term** next to rule.  
8. Click **Add new entry** next to Term.  
9. In the **Name** box, enter the Identifier for the term.  
10. In the **Comment** box, enter the comment. |
| Specify input conditions for the IDS term. | 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>
<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 172: 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 173 on page 359.
6. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.
Table 173: 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 327
- Configuring a Service Set (NSM Procedure) on page 394
- Configuring Service Interface Pools (NSM Procedure) on page 393

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 174 on page 361.

5. Click one:
   - OK—to save the changes.
   - Cancel—to cancel the modifications.
### Table 174: NAT Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Enable multicast filters on Ethernet interfaces when IPv6 NAT is used for neighbor discovery. | 1. Click **Ipv6 Multicast Interfaces** next to Nat.  
2. Click **Add new entry** next to Ipv6 Multicast Interfaces.  
3. From the **Name list**, select **All** to enable filters on all interfaces.  
4. Select **Interface name** to enable filters on a specific interface only.  
5. In the **Comment** box, enter the comment.  
6. Select the **Disable** check box to disable filters on the specified interfaces. |
| Specify the NAT name and properties. | 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. |
| 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. |
## Table 174: NAT Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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 |

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 174: 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 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 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 327
- Configuring Service Interface Pools (NSM Procedure) on page 393
- Configuring PGCP (NSM Procedure) on page 363

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 364
- Configuring H248 Options Properties (NSM Procedure) on page 367
- Configuring H248 Properties (NSM Procedure) on page 373
- Configuring H248 Timers (NSM Procedure) on page 385
- Configuring the Monitor (NSM Procedure) on page 386
- Configuring Overload Control (NSM Procedure) on page 387
- Configuring Session Mirroring (NSM Procedure) on page 388
- Configuring Media Service (NSM Procedure) on page 388
- Configuring a Rule (NSM Procedure) on page 389
- Configuring Rule Set (NSM Procedure) on page 390
- Configuring Session Mirroring (NSM Procedure) on page 390
- Configuring Traceoptions (NSM Procedure) on page 391
- Configuring Virtual Interface (NSM Procedure) on page 392
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 364
- Configuring Data Inactivity Detection (NSM Procedure) on page 365
- Configuring Gateway Controller (NSM Procedure) on page 366
- Configuring Graceful Restart (NSM Procedure) on page 366

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 175 on page 364.
6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.

### Table 175: Virtual BGF Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a virtual BGF on the router</td>
<td>1. In the Name box, enter the identifier of the virtual BGF.</td>
</tr>
<tr>
<td></td>
<td>2. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. In the Gateway Address box, enter the IP address of the virtual BGF that you are configuring on the router.</td>
</tr>
<tr>
<td></td>
<td>4. From the Gateway Port list, select the port number of the virtual BGF that you are configuring on the router.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 65,535</td>
</tr>
<tr>
<td></td>
<td>5. From the Cleanup Timeout list, select the interval before inactivity detection starts.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 65,535 seconds</td>
</tr>
<tr>
<td></td>
<td>6. From the Service State list, select the service state of the virtual BGF.</td>
</tr>
<tr>
<td></td>
<td>7. From the Max Concurrent Calls list, select the Maximum number of concurrent calls on the virtual BGF.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 10,000</td>
</tr>
</tbody>
</table>
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 176 on page 365.
6. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.

### Table 176: Data Inactivity Detection Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure data inactivity detection | 1. Expand **Gateway**.  
                                  2. Click **Data Inactivity Detection** next to Gateway.  
                                  3. In the Comment box, enter the comment.  
                                  4. From the **Inactivity Delay** list, select the time interval before checking for media inactivity.  
                                      Range: 0 through 3600 seconds  
                                      Default: 5  
                                  5. From the **Latch Deadlock delay** list, select the time interval before checking for data packets.  
                                      Range: 0 through 3600 seconds  
                                  6. Select the **Send Notification on Delay** check box to send an inactivity notification immediately when no media packets are detected during a delay period that precedes checking for media inactivity.  
                                  7. From the **Inactivity Duration** list, select the time during which no packets are received.  
                                      Range: 5 through 86400 seconds  
                                      Default: 30  
                                  8. Select the **Stop Detection On Drop** check box to configure the BGF to stop inactivity detection when a gate action is set to drop. |

| Change the service state of inactive terminations | 1. Expand **Data Detection**.  
                                                     2. Click **Report Service Change** next to Data Inactivity Detection.  
                                                     3. In the Comment box, enter the comment.  
                                                     4. From the **Service Change Type** list, select the method and reason used in changing the service state of the termination to active in order to curtail sending of inactivity messages  
                                                        - **forced-906**—if the service is to be terminated using a forced termination method with reason code 906 (loss of lower layer connectivity).  
                                                        - **forced-910**—if the service is to be terminated using a forced termination with reason code 910 (media capability failure). |
**Configuring Gateway Controller (NSM Procedure)**

You can configure a gateway controller either as a remote controller or as a local controller. Configure the gateway controller as a remote controller if you are using an external gateway controller and configure the gateway controller as a local controller if you are using a border signaling gateway (BSG).

To configure gateway controller in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in Table 177 on page 366.
6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.

**Table 177: Gateway Controller Configuration Details**

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a gateway controller.</td>
<td>1. Click <strong>Add new entry</strong> next to Gateway.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Gateway Controller</strong> next to gateway.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add new entry</strong> next to Gateway Controller.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Name</strong> box, enter the name of the gateway controller or BSG.</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>Controller Address</strong> box, enter the IP address of the gateway controller.</td>
</tr>
<tr>
<td></td>
<td>7. From the <strong>Controller Port</strong> list, select the port number of the gateway controller.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>8. Expand <strong>gateway-controller</strong>.</td>
</tr>
<tr>
<td></td>
<td>9. Click <strong>Interim Ah Scheme</strong>.</td>
</tr>
<tr>
<td></td>
<td>10. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>11. From the <strong>Algorithm</strong> list, select the algorithm used for the interim AH scheme.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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 178 on page 367.

6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.

### Table 178: 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 Add new entry next to Gateway.</td>
</tr>
<tr>
<td></td>
<td>2. Click Graceful Restart 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 Synchronization Time list, select the maximum time allowed for the synchronization procedure with the PIC or DPC. Range: 0 through 300</td>
</tr>
<tr>
<td></td>
<td>5. From the Maximum Synchronization Mismatches list, select the maximum number of mismatches allowed during the synchronization procedure with the PIC or DPC. Range: 0 through 20000</td>
</tr>
<tr>
<td></td>
<td>6. Select the No Synchronization 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 367
- Changing Encoding Defaults (NSM Procedure) on page 368
- Configuring Service Change (NSM Procedure) on page 369

### 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 179 on page 368.
6. Click one:
   - OK—To save the changes.
Table 179: H248 Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure options that affect virtual BGF H.248 behavior. | 1. Click **Add new entry** next to Gateway.  
2. Click **H248 Options** next to gateway.  
3. In the **Comment** box, enter the comment.  
4. Select the **Audit Observed Events Returns** option to enable a history of media inactivity events to be viewed by the gateway controller. |

Changing Encoding Defaults (NSM Procedure)

You can change the encoding defaults using this option.

To configure encoding defaults in NSM:
1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Gateway**.
5. Add or modify the settings as specified in Table 180 on page 368.
6. Click one:  
   ■ **OK**—To save the changes  
   ■ **Cancel**—To cancel the modifications

Table 180: Encoding Defaults Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Change encoding defaults. | 1. Click **Add new entry** next to Gateway.  
2. Click **H248 Options** next to gateway.  
3. Expand **H248 Options**.  
4. Click **Encoding** next to H248 Options.  
5. In the **Comment** box, enter the comment.  
6. Select the **No Dscp Bit Mirroring** check box to disable mirroring of DSCP bits.  
7. Select the **Use Lower Case** check box to configure upper-case encoding for H.248 messages. |
Configuring Service Change (NSM Procedure)

Service change specifies the method and reason that the virtual BGF includes in ServiceChange commands that it sends to the gateway controller when the state of a control association, virtual interface, or context changes. See the following topics:

- Configuring Context Indications (NSM Procedure) on page 369
- Configure Control Association Indications (NSM Procedure) on page 370
- Configuring Virtual Interface Indications (NSM Procedure) on page 372

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 181 on page 369.
6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.

Table 181: 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 182 on page 371.
6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
### Table 182: Control Association Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the method and reason that the virtual BGF includes in</td>
<td>1. Click <strong>Add new entry</strong> next to Gateway.</td>
</tr>
<tr>
<td>Registration Request ServiceChange commands when it attempts to</td>
<td>2. Click <strong>H248 Options</strong> next to gateway.</td>
</tr>
<tr>
<td>reregister with the gateway controller or register with a new</td>
<td>3. Expand <strong>H248 Options</strong>.</td>
</tr>
<tr>
<td>gateway controller after the control association is disconnected.</td>
<td>4. Click <strong>Service Change</strong> next to H248 Options.</td>
</tr>
<tr>
<td></td>
<td>5. Expand <strong>Service Change</strong>.</td>
</tr>
<tr>
<td></td>
<td>6. Click <strong>Control Association Indications</strong> next to Service Change.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>8. Expand <strong>Control Association Indications</strong>.</td>
</tr>
<tr>
<td></td>
<td>9. Click <strong>Disconnect</strong> next to Control Association Indications.</td>
</tr>
<tr>
<td></td>
<td>10. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>11. From the <strong>Reconnect</strong> list, select the method and reason that the</td>
</tr>
<tr>
<td></td>
<td>virtual BGF includes in Registration Request ServiceChange commands when</td>
</tr>
<tr>
<td></td>
<td>it attempts to reregister with the gateway controller or register with a</td>
</tr>
<tr>
<td></td>
<td>new gateway controller after the control association is disconnected.</td>
</tr>
<tr>
<td></td>
<td>12. From the <strong>Controller Failure</strong> list, select the method and reason</td>
</tr>
<tr>
<td></td>
<td>that the virtual BGF includes in Registration Request ServiceChange</td>
</tr>
<tr>
<td></td>
<td>commands when it attempts to reregister with the gateway controller or</td>
</tr>
<tr>
<td></td>
<td>register with a new gateway controller after the control association is</td>
</tr>
<tr>
<td></td>
<td>disconnected.</td>
</tr>
<tr>
<td>Specify the method and reason that the virtual BGF includes in</td>
<td>1. Click <strong>Down</strong> next to Control Association.</td>
</tr>
<tr>
<td>Unregistration Messages in ServiceChange commands that it sends to</td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td>the gateway controller when a control association transitions to</td>
<td>3. From the <strong>Administrative</strong> list, select the method and reason that the</td>
</tr>
<tr>
<td>Out-of-Service because of a failure.</td>
<td>virtual BGF includes in Unregistration Messages in ServiceChange commands</td>
</tr>
<tr>
<td></td>
<td>that it sends to the gateway controller when a control association</td>
</tr>
<tr>
<td></td>
<td>transitions to Out-of-Service because of an administrative operation.</td>
</tr>
<tr>
<td></td>
<td>4. From the <strong>Failure</strong> list, select the method and reason that the virtual</td>
</tr>
<tr>
<td></td>
<td>BGF includes in Unregistration or Notification Messages in ServiceChange</td>
</tr>
<tr>
<td></td>
<td>commands when a control association transitions to Out-of-Service.</td>
</tr>
<tr>
<td></td>
<td>5. From the <strong>Graceful</strong> list, select the method and reason that the virtual</td>
</tr>
<tr>
<td></td>
<td>BGF includes in Notification ServiceChange commands that it sends to the</td>
</tr>
<tr>
<td></td>
<td>gateway controller when the control association transitions from In-Service</td>
</tr>
<tr>
<td></td>
<td>to Out-of-Service-Graceful.</td>
</tr>
</tbody>
</table>
Table 182: 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 in ServiceChange 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 183 on page 373.
6. Click one:  
   - **OK**—To save the changes.  
   - **Cancel**—To cancel the modifications.
Table 183: Virtual Interface Indications Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the method and reason that the virtual BGF includes in</td>
<td>1. Click <a href="#">Add new entry</a> next to Gateway.</td>
</tr>
<tr>
<td>ServiceChange commands that it sends to the gateway controller</td>
<td>2. Click <a href="#">H248 Options</a> next to gateway.</td>
</tr>
<tr>
<td>when the state of the virtual interface changes to Out-of-Service.</td>
<td>3. Expand <a href="#">H248 Options</a>.</td>
</tr>
<tr>
<td></td>
<td>4. Click <a href="#">Service Change</a> next to H248 Options.</td>
</tr>
<tr>
<td></td>
<td>5. Expand <a href="#">Service Change</a>.</td>
</tr>
<tr>
<td></td>
<td>6. Click <a href="#">Virtual Interface Indications</a> next to Service Change.</td>
</tr>
<tr>
<td></td>
<td>7. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>8. Expand <a href="#">Virtual Interface Indications</a>.</td>
</tr>
<tr>
<td></td>
<td>9. Click <a href="#">Virtual Interface Down</a> next to Virtual Interface Indications.</td>
</tr>
<tr>
<td></td>
<td>10. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>11. From the Graceful list, select the method and reason that the virtual</td>
</tr>
<tr>
<td></td>
<td>BGF includes in Notification ServiceChange commands that it sends to the</td>
</tr>
<tr>
<td></td>
<td>gateway controller when the control association transitions from In-Service</td>
</tr>
<tr>
<td></td>
<td>to Out-of-Service-Graceful.</td>
</tr>
<tr>
<td></td>
<td>12. From the Administrative list, select the method and reason that the</td>
</tr>
<tr>
<td></td>
<td>virtual BGF includes in Unregistration Messages in ServiceChange commands</td>
</tr>
<tr>
<td></td>
<td>that it sends to the gateway controller when a control association</td>
</tr>
<tr>
<td></td>
<td>transitions to Out-of-Service because of an administrative operation.</td>
</tr>
<tr>
<td></td>
<td>13. From the Failure list, select the method and reason that the virtual</td>
</tr>
<tr>
<td></td>
<td>BGF includes in Unregistration or Notification Messages in ServiceChange</td>
</tr>
<tr>
<td></td>
<td>commands when a control association transitions to Out-of-Service.</td>
</tr>
<tr>
<td></td>
<td>14. From the Link Loss list, select the method and reason that the virtual</td>
</tr>
<tr>
<td></td>
<td>BGF includes in Service-Interruption ServiceChange commands that it sends</td>
</tr>
<tr>
<td></td>
<td>to the gateway controller when the virtual interface transitions to</td>
</tr>
<tr>
<td></td>
<td>Out-of-Service because of a link loss.</td>
</tr>
<tr>
<td>Specifying the ServiceChange command that the virtual BGF sends</td>
<td>1. Click <a href="#">Virtual Interface Up</a> next to Virtual Interface Indications.</td>
</tr>
<tr>
<td>to the gateway controller when the state of the virtual interface</td>
<td>2. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td>changes to In-Service.</td>
<td>3. From the Warm list, select the method and reason that the virtual BGF</td>
</tr>
<tr>
<td></td>
<td>includes in Service-Restoration ServiceChange commands that it sends to the</td>
</tr>
<tr>
<td></td>
<td>gateway controller when a virtual interface transitions to In-Service.</td>
</tr>
<tr>
<td></td>
<td>4. From the Cancel Graceful list, select the method and reason that the</td>
</tr>
<tr>
<td></td>
<td>virtual BGF includes in Notification ServiceChange commands that it sends</td>
</tr>
<tr>
<td></td>
<td>to the gateway controller when the control association transitions from the</td>
</tr>
<tr>
<td></td>
<td>Draining state to the Forwarding state.</td>
</tr>
</tbody>
</table>

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 374
- Configuring Base Root (NSM Procedure) on page 374
- Configuring Differentiated Services (NSM Procedure) on page 377
- Configuring Event Timestamp Notification (NSM Procedure) on page 377
- Hanging Termination Detection (NSM Procedure) on page 378
- Configuring Inactivity Timer (NSM Procedure) on page 379
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 184 on page 374.
6. Click one:
   - **OK**—To save the changes
   - **Cancel**—To cancel the modifications

### Table 184: 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 185 on page 376.
6. Click one:
   ■ OK—To save the changes.
   ■ Cancel—To cancel the modifications.
### Table 185: 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.  
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 Mg 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 29,000 milliseconds |
| 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 186 on page 377.
6. Click one:
   ■ OK—To save the changes.
   ■ Cancel—To cancel the modifications.

Table 186: 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.  
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 187 on page 378.
6. Click one:
Table 187: Event Timestamp Notification Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure event timestamp notification.</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 Event Timestamp Notification 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 Request Timestamp list, select whether time stamp information is made available to the gateway controller or is suppressed.</td>
</tr>
<tr>
<td></td>
<td>■ Select requested to enable gateway controller access to time stamp information for notifications.</td>
</tr>
<tr>
<td></td>
<td>■ Select suppressed to disable gateway controller access to time stamp information for notifications.</td>
</tr>
<tr>
<td></td>
<td>■ Select autonomous 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 188 on page 379.
6. Click one:
   ■ OK—To save the changes.
   ■ Cancel—To cancel the modifications.
Table 188: 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>3. Expand H248 Properties</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 Timer 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 189 on page 380.
6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
## 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 190 on page 381.
6. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.

### Table 189: Inactivity Timer Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the inactivity</td>
<td>1. Click <strong>Add new entry</strong> next to Gateway.</td>
</tr>
<tr>
<td>timeout event.</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>Inactivity Timer</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. Expand <strong>Inactivity Timer</strong>.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>Inactivity Timeout</strong> next to Inactivity Timer.</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>Detect</strong> check box to specify the BGF detects inactivity timeout events received from the BGF by default.</td>
</tr>
<tr>
<td></td>
<td>10. Expand <strong>Inactivity Timeout</strong>.</td>
</tr>
<tr>
<td>Configure maximum inactivity</td>
<td>1. Click <strong>Maximum Inactivity Time</strong> next to Inactivity Timeout.</td>
</tr>
<tr>
<td>time.</td>
<td>2. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>3. From the <strong>Default</strong> list, select the default value for the maximum inactivity time.</td>
</tr>
<tr>
<td></td>
<td>Range: 100 through 65,535 (10-millisecond units)</td>
</tr>
</tbody>
</table>
Table 190: Notification Behavior Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the default frequency for sending media inactivity</td>
<td>1. Click <strong>Add new entry</strong> next to Gateway.</td>
</tr>
<tr>
<td>notifications for regulated events.</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>Notification Behavior</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. Expand <strong>Notification Behavior</strong>.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>Notification Regulation</strong> next to Notification Behavior.</td>
</tr>
<tr>
<td></td>
<td>8. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>9. In the <strong>Default</strong> box, enter the default frequency for sending media inactivity notifications for regulated events.</td>
</tr>
</tbody>
</table>

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 191 on page 382.     
6. Click one:                                                            
   ■ **OK**—To save the changes.                                          
   ■ **Cancel**—To cancel the modifications.                              
Table 191: 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.  
4. Click Segmentation next to H248 properties.  
5. In the Comment box, enter the comment.  
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 |
| Set default, maximum, and minimum values for the MGC segmentation timer value property of the segmentation package. | 1. Click Mgc Segmentation Timer next to Segmentation.  
2. In the Comment box, enter the comment.  
3. From the Default list, select the default time within which the virtual BGF waits to receive outstanding message segments from the gateway controller after it receives the SegmentationCompleteToken.  
   Range: 500 through 30,000 milliseconds |

Configuring Traffic Management (NSM Procedure)

You can configure traffic management of the gate stream and the RTP Control Protocol (RTCP) stream. The parameters for the RTCP stream take effect only when the gate is a 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 192 on page 384.
6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
Table 192: 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.  
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.  
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 192: Traffic Management Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Configure the sustained data rate for streams of any protocol, including RTP. | 1. Click **Sustained Data Rate** next to Traffic Management.  
2. In the **Comment** box, enter the comment.  
3. From the **Default** list, select the default value for sustained data rate.  
   Range: 125 through 4,294,967,295 bytes per second  
4. Expand **Sustained Data Rate**.  
5. Click **Rtcp** next to Sustained Data Rate.  
6. In the **Comment** box, enter the comment.  
7. Expand **Rtcp**.  
8. Click **Percentage** next to Rtcp.  
9. Select one of the following:  
   - percentage— if the value entered is a percentage of the RTP’s gate rate.  
   - fixed-value— if the value entered is a fixed number of bits per second.  
   Range: 0 through 2147483647 |

**Configuring H248 Timers (NSM Procedure)**

You can configure H.248 timers for the PGCP connection using the H248 Timers option.

To configure H248 timers in NSM:

1. In the navigation tree select **Device Manager > Devices**.  
2. In the **Devices** list, double-click the device to select it.  
3. In the **Configuration** tab, expand **Services > Pgcp**.  
4. Select **Gateway**.  
5. Add or modify the settings as specified in Table 193 on page 386.  
6. Click one:  
   - OK—To save the changes.  
   - Cancel—To cancel the modifications.
Table 193: H248 Timers Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure H248</td>
<td>1. Click <strong>Add new entry</strong> next to Gateway.</td>
</tr>
<tr>
<td>Timers.</td>
<td>2. Click <strong>H248 Timers</strong> next to gateway.</td>
</tr>
<tr>
<td>In the <strong>Comment</strong></td>
<td>3. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td>box, enter the</td>
<td>4. From the <strong>Maximum Waiting Delay</strong> list, select the maximum time the</td>
</tr>
<tr>
<td>comment.</td>
<td>virtual BGF waits before contacting a new gateway controller when the</td>
</tr>
<tr>
<td></td>
<td>connection to the controlling gateway controller is lost.</td>
</tr>
<tr>
<td></td>
<td>Range: 100 through 3000000 milliseconds</td>
</tr>
<tr>
<td></td>
<td>Default: 3000</td>
</tr>
<tr>
<td></td>
<td>5. From the <strong>Tmax Retransmission Delay</strong> list, select the duration of the</td>
</tr>
<tr>
<td></td>
<td>delay before the BGF considers the gateway controller to be down.</td>
</tr>
<tr>
<td></td>
<td>Range: 1000 through 600000 milliseconds</td>
</tr>
<tr>
<td></td>
<td>Default: 25000</td>
</tr>
<tr>
<td></td>
<td>6. From the <strong>Initial Average Ack Delay</strong> 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 <strong>Maximum Net Propagation Delay</strong> list, select the duration of</td>
</tr>
<tr>
<td></td>
<td>the 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 194 on page 387.
6. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.
### Table 194: 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 195 on page 387.
6. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.

### Table 195: 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 196 on page 388.
6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.

**Table 196: Session Mirroring Configuring Details**

<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 197 on page 389.
6. Click one:
- OK—To save the changes.
- Cancel—To cancel the modifications.

### Table 197: Media Service Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure media service.</td>
<td>1. Click <strong>Add new entry</strong> next to Media Service.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Name</strong> box, enter the identifier for the media service name.</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>Nat Pool</strong> box, enter the identifier for the NAT address pool.</td>
</tr>
</tbody>
</table>

### 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 198 on page 389.
6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.

### Table 198: Configuring Rule

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a rule.</td>
<td>1. Click <strong>Add new entry</strong> next to Rule.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Name</strong> box, enter the identifier for the rule.</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>Gateway</strong> list, select the identifier of the virtual BGF.</td>
</tr>
<tr>
<td></td>
<td>5. Expand <strong>rule</strong>.</td>
</tr>
<tr>
<td></td>
<td>6. Click <strong>Media Service</strong> next to rule.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>Add new entry</strong> next to Media Service.</td>
</tr>
<tr>
<td></td>
<td>8. In the <strong>New media-service</strong> window, enter the identifier for the media service name.</td>
</tr>
</tbody>
</table>
**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 199 on page 390.
6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.

**Table 199: Configuring Rule Set**

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a rule set</td>
<td>1. Click Add new entry next to Rule Set.</td>
</tr>
<tr>
<td></td>
<td>2. In the Name box, enter the identifier for the collection of rules that make up this rule set.</td>
</tr>
<tr>
<td></td>
<td>3. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>4. Expand rule-set.</td>
</tr>
<tr>
<td></td>
<td>5. Click Rule next to rule-set.</td>
</tr>
<tr>
<td></td>
<td>6. Click Add new entry next to Rule.</td>
</tr>
<tr>
<td></td>
<td>7. From the Name list, select the identifier for the rule.</td>
</tr>
<tr>
<td></td>
<td>8. In the Comment box, enter the comment.</td>
</tr>
</tbody>
</table>

**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 200 on page 391.
6. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
Table 200: Session Mirroring Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure session mirroring.</td>
<td>1. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>2. Select the Disable Session Mirroring check box to disable session mirroring on the BGF.</td>
</tr>
<tr>
<td></td>
<td>3. Expand Session Mirroring</td>
</tr>
<tr>
<td></td>
<td>4. Click Delivery Function next to Session Mirroring.</td>
</tr>
<tr>
<td></td>
<td>5. Click Add new entry next to Delivery Function.</td>
</tr>
<tr>
<td></td>
<td>6. In the Name box, enter the name of the delivery function that receives the session mirroring information.</td>
</tr>
<tr>
<td></td>
<td>7. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>8. In the Destination Address box, enter the address of the server to which the BGF sends session-mirroring information.</td>
</tr>
<tr>
<td></td>
<td>9. From the Destination Port list, select the port on the delivery function server that receives session-mirroring information. Range: 0 through 65535</td>
</tr>
<tr>
<td></td>
<td>10. In the Network Operator Id box, enter the network operator ID. The ID can be up to five characters.</td>
</tr>
<tr>
<td></td>
<td>11. In the Source Address box, enter the address of the interface on which the BGF sends session-mirroring data to the delivery function.</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>14. Click Memory Management next to delivery-function.</td>
</tr>
<tr>
<td></td>
<td>15. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>16. From the Operational Mode list, select the operational mode.</td>
</tr>
</tbody>
</table>

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 201 on page 392. |
6. Click one: |
   ■ OK—To save the changes. |
   ■ Cancel—To cancel the modifications.
Table 201: Traceoptions Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure PGCP trace options.</td>
<td>1. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>2. Select the <strong>No Remote Trace</strong> check box to disable remote tracing.</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 which the tracing messages are written.</td>
</tr>
<tr>
<td></td>
<td>7. In the <strong>Size</strong> box, enter the size parameter (in bytes) to trigger rotation of files.</td>
</tr>
<tr>
<td></td>
<td>8. From the <strong>Files</strong> list, select the number of trace files.</td>
</tr>
<tr>
<td></td>
<td>9. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>world-readable</strong>—To allow all users to use the log file.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>no-world-readable</strong>—To disallow all users from using the log file.</td>
</tr>
<tr>
<td></td>
<td>10. In the <strong>Match</strong> box, enter the regular expression.</td>
</tr>
<tr>
<td></td>
<td>11. Click <strong>Flag</strong> next to Traceoptions.</td>
</tr>
<tr>
<td></td>
<td>12. Click <strong>Add new entry</strong> next to Flag.</td>
</tr>
<tr>
<td></td>
<td>13. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
</tbody>
</table>

**Configuring Virtual Interface (NSM Procedure)**

You can configure a virtual interface for the BGF using the Virtual Interface option.

To configure virtual interface in NSM:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Services > Pgcp**.
4. Select **Virtual Interface**.
5. Add or modify the settings as specified in Table 202 on page 393.
6. Click one:
   ■ **OK**—To save the changes.
   ■ **Cancel**—To cancel the modifications.
### Table 202: 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 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 instance.</td>
</tr>
<tr>
<td></td>
<td>13. In the <strong>Service Interface</strong> box, enter the name and logical interface number of the service Interface in <code>interface-name.unit-number</code> 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 203 on page 394.
6. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.
Table 203: Service Interface Pools Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a service interface pool</td>
<td>1. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td>for VPN aggregation for the BGF feature.</td>
<td>2. Expand Service Interface Pools.</td>
</tr>
<tr>
<td></td>
<td>3. Click Pool next to Service Interface Pools.</td>
</tr>
<tr>
<td></td>
<td>4. Click Add new entry next to Pool.</td>
</tr>
<tr>
<td></td>
<td>5. In the Name box, enter the name of the service interface pool.</td>
</tr>
<tr>
<td></td>
<td>6. In the Comment box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>7. Click Interface next to pool.</td>
</tr>
<tr>
<td></td>
<td>8. Click Add new entry next to interface.</td>
</tr>
<tr>
<td></td>
<td>9. In the Name box, enter the name and logical unit number of the service interface.</td>
</tr>
<tr>
<td></td>
<td>10. In the Comment box, enter the comment.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring a Service Set (NSM Procedure) on page 394
- Configuring Stateful Firewall (NSM Procedure) on page 398

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 204 on page 395.
6. Click one:
   - OK—Save the changes.
   - Cancel—Cancel the modifications.
### Table 204: 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. 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><strong>NOTE:</strong></td>
<td>The IDP profile is a list of IDP policies as defined in the <strong>Security &gt; Idp &gt; Idp policy</strong> 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 204: 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 204: 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. |
Table 204: Service Set Configuration Details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure generation of system log messages for the service set.</td>
<td>1. Click <strong>Syslog</strong> next to service-set.</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>Host</strong> next to Syslog.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Add new entry</strong> next to Host.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Name</strong> box, enter the name of the system logging utility host machine.</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>Facility Override</strong> list, select the name of the facility that overrides the default assignment.</td>
</tr>
<tr>
<td></td>
<td>8. In the <strong>Log Prefix</strong> box, enter the system logging prefix value.</td>
</tr>
<tr>
<td></td>
<td>9. Click <strong>Contents</strong> next to host.</td>
</tr>
<tr>
<td></td>
<td>10. From the <strong>Name</strong> list, select the service set.</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>Any</strong> list, select the system logging severity level.</td>
</tr>
</tbody>
</table>

Related Topics

- Configuring Service Interface Pools (NSM Procedure) on page 393
- Configuring Stateful Firewall (NSM Procedure) on page 398
- Configuring Intrusion Detection Service (NSM Procedure) on page 354

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 205 on page 399.
5. Click one:
   - **OK**—To save the changes.
   - **Cancel**—To cancel the modifications.
Table 205: Stateful Firewall Configuration Details

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define the rule.</td>
<td>1. Click <strong>Rule</strong> next to Stateful Firewall.</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</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>rule match is applied.</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>input</strong> to apply the rule match on the input side of the</td>
</tr>
<tr>
<td></td>
<td>interface.</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>output</strong> to apply the rule match on the output side of the</td>
</tr>
<tr>
<td></td>
<td>interface.</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>input-output</strong> to apply the rule match bidirectionally.</td>
</tr>
<tr>
<td></td>
<td>6. Click <strong>Term</strong> next to rule.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>Add new entry</strong> next to Term.</td>
</tr>
<tr>
<td></td>
<td>8. In the <strong>Name</strong> box, enter the identifier for the term.</td>
</tr>
<tr>
<td></td>
<td>9. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>10. Expand <strong>term</strong>.</td>
</tr>
<tr>
<td></td>
<td>11. Click <strong>From</strong> next to <strong>term</strong>.</td>
</tr>
<tr>
<td></td>
<td>12. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>13. Expand <strong>From</strong>.</td>
</tr>
<tr>
<td></td>
<td>14. From the listed match conditions, select the match condition for</td>
</tr>
<tr>
<td></td>
<td>stateful firewall.</td>
</tr>
<tr>
<td></td>
<td>- The match conditions listed are Application Sets, Applications,</td>
</tr>
<tr>
<td></td>
<td>Destination Address, Destination Address Range, Destination Prefix List,</td>
</tr>
<tr>
<td></td>
<td>Source Address, Source Address Range, and Source Prefix List.</td>
</tr>
<tr>
<td></td>
<td>15. Click <strong>Then</strong> next to <strong>term</strong>.</td>
</tr>
<tr>
<td></td>
<td>16. In the <strong>Comment</strong> box, enter the comment.</td>
</tr>
<tr>
<td></td>
<td>17. Select the <strong>Syslog</strong> check box to enable system logging.</td>
</tr>
<tr>
<td></td>
<td>18. Expand <strong>Then</strong>.</td>
</tr>
<tr>
<td></td>
<td>19. Click <strong>Accept</strong> next to <strong>Then</strong>.</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>Accept</strong> to accept the traffic and send it on to its</td>
</tr>
<tr>
<td></td>
<td>destination.</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>discard</strong> to not accept traffic or process it further.</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>reject</strong> to accept the traffic and return a rejection message.</td>
</tr>
<tr>
<td></td>
<td>20. Click <strong>Allow Ip Options</strong> next to <strong>Then</strong>.</td>
</tr>
<tr>
<td></td>
<td>21. Click <strong>Add new entry</strong> next to <strong>Allow Ip Options</strong>.</td>
</tr>
<tr>
<td></td>
<td>22. From the dropdown list, select the IP option name.</td>
</tr>
</tbody>
</table>
### Table 205: Stateful Firewall Configuration Details *(continued)*

<table>
<thead>
<tr>
<th>Task</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Define the rule set.                                                 | 1. Click **Rule Set** next to Stateful Firewall.  
2. Click **Add new entry** next to Rule Set.  
3. In the **Name** box, enter the identifier for the collection of rules that constitute this rule set.  
4. In the **Comment** box, enter the comment.  
5. Click **Rule** next to rule-set.  
6. Click **Add new entry** next to Rule.  
7. From the **Name** list, select the identifier for the collection of terms that constitute this rule.  
8. In the **Comment** box, enter the comment. |

#### Related Topics
- Configuring Service Interface Pools (NSM Procedure) on page 393
- Configuring a Service Set (NSM Procedure) on page 394
Chapter 24

Configuring SNMP

- Configuring Basic System Identification for SNMP (NSM Procedure) on page 401
- Configuring SNMP Communities (NSM Procedure) on page 402
- Configuring SNMP Trap Groups (NSM Procedure) on page 404
- Configuring SNMP Views (NSM Procedure) on page 405

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 206 on page 401.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Name</strong></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><strong>Description</strong></td>
<td>Provides a description for the system.</td>
<td>Enter a description for the system. For example, type J4550 with 4 PIMs.</td>
</tr>
<tr>
<td><strong>Location</strong></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><strong>Contact</strong></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>

**Snmp > Engine Id**
## 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 207 on page 403.
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 207: 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>
<tr>
<td>Authorization</td>
<td>Specifies the type of access granted to the community. Access is authorized for SNMP Get, GetBulk, GetNext, and Set requests.</td>
<td>Select an access type for the community:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- None—No requests are enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>readonly</strong>—Enable Get, GetNext, and GetBulk requests. This option is enabled by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>read-write</strong>—Enable all requests, including Set requests. You must configure a view to enable Set requests.</td>
</tr>
<tr>
<td>Client List Name</td>
<td>Specifies a client list or prefix list to be assigned to an SNMP community.</td>
<td>1. Expand the Community tree and select <strong>Client List Name</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select a name.</td>
</tr>
<tr>
<td>Routing Instance</td>
<td>Specifies a routing instance for a community.</td>
<td>1. Expand the Community tree and select <strong>Routing Instance</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the New button or select an entry and click the Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Configure the following to create and define a routing instance:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Name</strong>—Enter a name for the routing instance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Comment</strong>—Enter a comment for the routing instance.</td>
</tr>
</tbody>
</table>

**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.”

---

Chapter 24: Configuring SNMP
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 208 on page 404.
8. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
   - Apply—To apply the SNMP settings.

Table 208: 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 208: 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 401
- Configuring SNMP Agents and Communities (NSM Procedure)
- Configuring SNMP Views (NSM Procedure) on page 405

**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 209 on page 406.
8. Click one:
   - OK—To save the changes.
   - Cancel—To cancel the modifications.
   - Apply—To apply the SNMP settings.

Table 209: 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 View tree and select oid.</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 MIB</td>
<td>Select exclude to exclude the subtree of MIB objects represented by the specified OID.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select include 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 401
- Configuring SNMP Agents and Communities (NSM Procedure)
- Configuring SNMP Trap Groups (NSM Procedure) on page 404
Part 4

Managing M-series and MX-series Devices

- Managing M-series and MX-series Devices Overview on page 409
- Viewing the M-series and MX-series Device Inventory in NSM and the CLI on page 411
- Topology Manager on page 417
Managing M-series and MX-series Devices

Overview

Managing M-series and MX-series Device Software Versions on page 409

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 411
■ Comparing Device Inventory in NSM and the CLI on page 412
M-series and MX-series Devices
Chapter 26

Viewing the M-series and MX-series Device Inventory in NSM and the CLI

- Viewing and Reconciling Device Inventory on page 411
- Comparing Device Inventory in NSM and the CLI on page 412

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 show 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 409
- Comparing Device Inventory in NSM and the CLI on page 412

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 412
- Viewing Device Inventory from the CLI on page 414

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 413.
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 413.)

![Figure 7: The Device Inventory Window](image)

**Figure 7: The Device Inventory Window**

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 414.)

![Figure 8: Viewing the Hardware Inventory](image)
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 412 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 412.

```
user@host> show chassis hardware
Hardware inventory:
<table>
<thead>
<tr>
<th>Item</th>
<th>Version</th>
<th>Part number</th>
<th>Serial number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis</td>
<td>REV 04</td>
<td>710-008920</td>
<td>CM0805</td>
<td>M10i</td>
</tr>
<tr>
<td>Midplane</td>
<td>REV 04</td>
<td>710-008920</td>
<td>CM0805</td>
<td>M10i Midplane</td>
</tr>
<tr>
<td>Power Supply</td>
<td>Rev 06</td>
<td>740-008537</td>
<td>5384103</td>
<td>AC Power Supply</td>
</tr>
<tr>
<td>Power Supply</td>
<td>Rev 06</td>
<td>740-008537</td>
<td>5384265</td>
<td>AC Power Supply</td>
</tr>
<tr>
<td>HCM 0</td>
<td>REV 03</td>
<td>710-010580</td>
<td>CM1272</td>
<td>M10i HCM</td>
</tr>
<tr>
<td>HCM 1</td>
<td>REV 03</td>
<td>710-010580</td>
<td>CM1187</td>
<td>M10i HCM</td>
</tr>
<tr>
<td>Routing Engine</td>
<td>REV 09</td>
<td>740-009459</td>
<td>1000602468</td>
<td>RE-5.0</td>
</tr>
<tr>
<td>CFEB 0</td>
<td>REV 09</td>
<td>750-010465</td>
<td>DK6820</td>
<td>Internet Processor II</td>
</tr>
<tr>
<td>FPC 0</td>
<td>REV 10</td>
<td>750-002971</td>
<td>CL0219</td>
<td>4x OC-3 SONET, MM</td>
</tr>
<tr>
<td>PIC 0</td>
<td>REV 11</td>
<td>750-002992</td>
<td>CM4540</td>
<td>4x F/E, 100 BASE-TX</td>
</tr>
</tbody>
</table>
```
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 409
■ Viewing and Reconciling Device Inventory on page 411
Chapter 27

Topology Manager

- Overview of the NSM Topology Manager on page 417
- Requisites for a Topology Discovery on page 417
- About the NSM Topology Manager Toolbar on page 418

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 417
- About the NSM Topology Manager Toolbar on page 418

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
3. 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 417
■ About the NSM Topology Manager Toolbar on page 418

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 417
- Requisites for a Topology Discovery on page 417
Part 5
Monitoring M-series and MX-series Devices

- Real Time Monitoring of M-series and MX-series on page 423
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 424
- Viewing Device Monitor Alarm Status on page 427
- Setting the Polling Interval For Device Alarm Status on page 428
Viewing Device Status

Table 210 on page 424 lists and describes device information that you can view through the Device Monitor.

Table 210: Device Status Information

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name assigned to the device in NSM.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain in NSM in which the device is managed.</td>
</tr>
<tr>
<td>Platform</td>
<td>Model number of the device.</td>
</tr>
<tr>
<td>OS Version</td>
<td>Operating system firmware version running on the device.</td>
</tr>
</tbody>
</table>
Table 210: Device Status Information

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Status</td>
<td>Current configuration status of the device in NSM:</td>
</tr>
<tr>
<td>■ None</td>
<td>No state has been set (does not show in Device Monitor).</td>
</tr>
<tr>
<td>■ Modeled</td>
<td>The device exists in NSM, but a connection to the device has not yet been established.</td>
</tr>
<tr>
<td>■ RMA</td>
<td>Equivalent to bringing the device into the Modeled state. RMA results from an administrator selection in the UI when a device goes down.</td>
</tr>
<tr>
<td>■ Waiting for 1st connect</td>
<td>NSM is waiting for the device to connect. You must enter a command on the device to make it connect to NSM.</td>
</tr>
<tr>
<td>■ Import Needed</td>
<td>You must import the configuration of the device into NSM. When you add a device for the first time, verify that your status indicates &quot;Import Needed&quot; 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>■ OS Version Adjustment Needed</td>
<td>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>■ Platform Mismatch</td>
<td>The device platform selected when adding the DMI device in NSM does not match the device itself. A device in this state cannot connect to NSM.</td>
</tr>
<tr>
<td>■ Device Firmware Mismatch</td>
<td>The OS version selected when adding a DMI device does not match the OS version running on the device itself.</td>
</tr>
<tr>
<td>■ Device Type Mismatch</td>
<td>The type of device specified when adding the device in NSM does not match the device itself. The device type might indicate whether the device is part of a vsys device, part of a cluster, or part of a virtual chassis. A device in this state cannot connect to NSM.</td>
</tr>
<tr>
<td>■ Detected duplicate serial number</td>
<td>The device has the same sequence number as another managed device. A device in this state cannot connect to NSM.</td>
</tr>
<tr>
<td>■ Update Needed</td>
<td>An update to this device is required.</td>
</tr>
<tr>
<td>■ Managed</td>
<td>The device is currently being managed by NSM.</td>
</tr>
<tr>
<td>■ Managed, In Sync</td>
<td>The physical device configuration is synced with the modeled configuration in NSM.</td>
</tr>
</tbody>
</table>
### Table 210: 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. |
| 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 210: Device Status Information (continued)

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

Related Topics

- About the Realtime Monitor on page 423
- Viewing Device Monitor Alarm Status on page 427
- Setting the Polling Interval For Device Alarm Status on page 428

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 423
- Viewing Device Status on page 424
- Setting the Polling Interval For Device Alarm Status on page 428

**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 423
- Viewing Device Status on page 424
- Viewing Device Monitor Alarm Status on page 427
Part 6
Index

- Index on page 431
M-series and MX-series Devices
index

a
access profile, configuring ............................................63
access profiles, L2TP
  AAA subscriber management
    RADIUS parameters, configuring ...............................58
  access profile, configuring .....................................49
  accounting order, configuring ...................................51
  accounting parameters, configuring .............................50
  authentication order, configuring ..............................52
  authorization order, configuring ...............................52
  client filter name, configuring ...................................54
  configuring ............................................................49
  L2TP client, configuring ...........................................53
  LDAP options, configuring ........................................55
  LDAP server, configuring .........................................56
  provisioning order, configuring ..................................57
  RADIUS parameters, configuring ................................60
  session limit, configuring ........................................62
  subscriber access management
    RADIUS, configuring .............................................61
accounting options
  class usage profile, configuring ................................65
  filter profile, configuring .......................................67
  interface profile, configuring ...................................68
  log file, configuring ...............................................66
  MIB profile, configuring .........................................70
  policy decision statistics profile, configuring ............69
  routing engine profile, configuring ...........................71
accounting options, configuring ..................................65
adaptive services PICs, configuring ..............................327
address family, specifying ..........................................191
aggregated devices, configuring ..................................89
alarm status
  setting polling intervals .........................................428
  viewing ...............................................................427
api
application, application set
  configuring ...........................................................73
authentication key updates, configuring ........................325
border signaling gateways, configuring ..........................328
bridge domain
  forwarding options, configuring ................................78
  IGMP snooping, configuring .......................................82
  layer 2 learning, forwarding, configuring ....................76
  logical interfaces, configuring ...................................79
  multicast snooping options, configuring ......................80
  VLAN ID, configuring .............................................87
bridge domain, configuring .........................................75
bridge domains properties
  configuring ..................................................................75

C
chassis alarms, configuring ...........................................90
chassis FPC, configuring ..............................................92
classifiers
  CoS .................................................................116
cli
  about .........................................................................7
code point aliases .....................................................118
communities
  configuring ............................................................402
confederation
  configuring ...........................................................297
container interfaces, configuring ..................................91
CoS classifiers .........................................................116
CoS code point aliases .............................................118
CoS drop profiles .....................................................119
CoS forwarding classes .............................................121
CoS forwarding policy, configuring ..............................123
CoS fragmentation maps, configuring ............................124
CoS host outbound traffic, configuring .........................126
CoS interfaces ..........................................................127
CoS restricted queue, configuring ................................137
CoS routing instances, configuring ...............................132
CoS scheduler maps ..................................................135
CoS schedulers ........................................................134
CoS tracing operations, configuring .............................138
CoS traffic control profiles, configuring .......................139
CoS translation table, configuring ...............................141
customer support .....................................................xxviii
  contacting JTAC ....................................................xxviii
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>data model, defined</td>
<td>11</td>
</tr>
<tr>
<td>device status</td>
<td>16</td>
</tr>
<tr>
<td>device configuration about</td>
<td>43</td>
</tr>
<tr>
<td>modeling</td>
<td>28</td>
</tr>
<tr>
<td>device groups planning for</td>
<td>29</td>
</tr>
<tr>
<td>using</td>
<td>29</td>
</tr>
<tr>
<td>device inventory reconciling</td>
<td>411</td>
</tr>
<tr>
<td>viewing</td>
<td>411</td>
</tr>
<tr>
<td>Device Monitor alarm status</td>
<td>427</td>
</tr>
<tr>
<td>device status information</td>
<td>424</td>
</tr>
<tr>
<td>device schemas about</td>
<td>12</td>
</tr>
<tr>
<td>devices adding multiple with discovery rules</td>
<td>29</td>
</tr>
<tr>
<td>importing with dynamic IP address</td>
<td>16</td>
</tr>
<tr>
<td>managed</td>
<td>25</td>
</tr>
<tr>
<td>modeling</td>
<td>28</td>
</tr>
<tr>
<td>DHCP agent authentication support, configuring</td>
<td>183</td>
</tr>
<tr>
<td>default configuration settings, overriding</td>
<td>185</td>
</tr>
<tr>
<td>group, configuring</td>
<td>184</td>
</tr>
<tr>
<td>name of a group, configuring</td>
<td>189</td>
</tr>
<tr>
<td>operations, configuring</td>
<td>190</td>
</tr>
<tr>
<td>relay option 60, configuring</td>
<td>186</td>
</tr>
<tr>
<td>relay option 82, configuring</td>
<td>188</td>
</tr>
<tr>
<td>DHCP agent, configuring</td>
<td>183</td>
</tr>
<tr>
<td>discovery rules</td>
<td>29</td>
</tr>
<tr>
<td>distributed data collection</td>
<td>13</td>
</tr>
<tr>
<td>DMI See distributed data collection</td>
<td></td>
</tr>
<tr>
<td>drop profiles</td>
<td>119</td>
</tr>
<tr>
<td>dynamic tunnels, configuring</td>
<td>298</td>
</tr>
<tr>
<td>edit routing-options command</td>
<td>18</td>
</tr>
<tr>
<td>event policy tracing, configuring</td>
<td>154</td>
</tr>
<tr>
<td>event policy, configuring</td>
<td>151</td>
</tr>
<tr>
<td>event script, configuring</td>
<td>148</td>
</tr>
<tr>
<td>fate sharing configuring</td>
<td>300</td>
</tr>
<tr>
<td>firewall filter any family type, configuring</td>
<td>157</td>
</tr>
<tr>
<td>bridge family type, configuring</td>
<td>159</td>
</tr>
<tr>
<td>ccc family type, configuring</td>
<td>161</td>
</tr>
<tr>
<td>inet family type, configuring</td>
<td>163</td>
</tr>
<tr>
<td>inet6 family type, configuring</td>
<td>168</td>
</tr>
<tr>
<td>mpls family type, configuring</td>
<td>172</td>
</tr>
<tr>
<td>policer</td>
<td>178</td>
</tr>
<tr>
<td>VPLS family type, configuring</td>
<td>175</td>
</tr>
<tr>
<td>flow configuring</td>
<td>302</td>
</tr>
<tr>
<td>forwarding accounting options, configuring</td>
<td>181</td>
</tr>
<tr>
<td>forwarding classes</td>
<td>121</td>
</tr>
<tr>
<td>forwarding table configuring</td>
<td>304</td>
</tr>
<tr>
<td>generated routes</td>
<td>329</td>
</tr>
<tr>
<td>gateway admission controller, configuring</td>
<td>329</td>
</tr>
<tr>
<td>message manipulation rules, configuring</td>
<td>334</td>
</tr>
<tr>
<td>new call usage policy set, configuring</td>
<td>339</td>
</tr>
<tr>
<td>new call usage policy, configuring</td>
<td>336</td>
</tr>
<tr>
<td>new transaction policy set, configuring</td>
<td>344</td>
</tr>
<tr>
<td>new transaction policy, configuring</td>
<td>340</td>
</tr>
<tr>
<td>service point, configuring</td>
<td>332</td>
</tr>
<tr>
<td>session policy decision function, configuring</td>
<td>331</td>
</tr>
<tr>
<td>SIP policies and timers, configuring</td>
<td>334</td>
</tr>
<tr>
<td>timers, configuring</td>
<td>345</td>
</tr>
<tr>
<td>traceoptions, configuring</td>
<td>345</td>
</tr>
<tr>
<td>gateway properties, configuring</td>
<td>328</td>
</tr>
<tr>
<td>gateway, configuring</td>
<td>329</td>
</tr>
<tr>
<td>helpers DNS packet forwarding, enabling</td>
<td>197</td>
</tr>
<tr>
<td>port, configuring</td>
<td>199</td>
</tr>
<tr>
<td>router/interface, configuring</td>
<td>194</td>
</tr>
<tr>
<td>tracing operations, configuring</td>
<td>201</td>
</tr>
<tr>
<td>traffic management, configuring</td>
<td>382</td>
</tr>
</tbody>
</table>
**I**  
ILMI protocol, configuring ........................................255  
inet family type  
   firewall filter, configuring ..................................163  
   prefix-specific actions, configuring ......................165  
   service filters, configuring ..................................166  
   simple filters, configuring ..................................167  
nexthop family type  
   firewall filter, configuring ..................................166  
   prefix-specific actions, configuring ......................169  
   service filters, configuring ..................................171  
instance export  
   configuring ......................................................306  
instance import  
   configuring ......................................................307  
interface routes  
   configuring ......................................................308  
interface set, configuring .......................................254  
interface trace options, configuring .........................235  
interfaces  
   logical interface properties, configuring .................212  
   properties, configuring .......................................207  
   receive bucket properties, configuring ..................210  
   tracing operations, configuring ............................210  
   traffic shaping profile, configuring .......................233  
   transitions, damping ..........................................209  
   transmit leaky bucket, configuring .........................211  
interfaces, configuring .........................................207  
intrusion detection service, configuring ....................354  
inventory  
   See device inventory  
IP addresses  
   configuring ......................................................17  

**J**  
Job Manager  
   about .................................................................33  
   displaying updating errors ..................................37  
   reviewing .........................................................35  
JUNOS software devices  
   adding multiple with discovery rules .....................29  
   configuring .......................................................44  
JUNOS software, upgrading .....................................409  

**L**  
label distribution protocol, configuring ......................266  
layer 2 address learning, configuring .........................257  
layer 2 circuit  
   local interface switching, configuring .....................258  
   neighbor interface, configuring ............................259  
   tracing ............................................................263  
layer 2 circuit, configuring .....................................258  
link management protocol, configuring .....................277  
load balancing  
   per-flow/per-prefix, configuring ...........................202  
   load balancing, configuring ..................................192  

**M**  
M-series devices  
   adding multiple with discovery rules .....................29  
   configuring .......................................................44  
   supported Internet routers ..................................15  
   managed devices ................................................25  
   martian addresses  
      configuring .....................................................309  
   maximum paths  
      configuring .....................................................310  
   maximum prefixes  
      configuring .....................................................311  
   MSTP .................................................................280  
   multicast  
      configuring .....................................................313  
   MX-series devices  
      adding multiple with discovery rules ..................29  
      configuring .....................................................44  
   supported Internet Services routers .......................15  

**N**  
navigation tree ......................................................7  
NetConf ..............................................................13  
network  
   connectivity, checking .......................................17, 18  
   ping command ...................................................17, 18  
   network address translation, configuring .................359  
   no-readvertise  
      option ............................................................18  
   NSM API ............................................................12  
   NSM architecture  
      distributed data collection ...............................7  
   NSM modules  
      Log Viewer ....................................................32  
      Realtime Monitor .............................................32, 423  
   NSM UI  
      about ............................................................7  
      navigation tree ................................................7  

**Index**
stateful firewall, configuring ........................................ ...398
static route .................................................................... 18
Static Routes
configuring ...................................................................... 321
status
device ........................................................................... 16
support, technical See technical support

T
T640 router, configuring ............................................. 98
TCP See Transmission Control Protocol
technical overview .......................................................... 3
technical support
contacting JTAC ..................................................... xxviii
Traceoptions
configuring ................................................................. 323
Transmission Control Protocol ..................................... 13
trap groups
configuring ................................................................uteur 404

U
unreachable workflow
importing device .......................................................... 16

V
views
configuring .................................................................. 405
VRRP ........................................................................... 294
VSTP ........................................................................... 295

W
workflows
supported ...................................................................... 26