



# **NSM Configuration Guide for EX Series Devices**

*2010.1*

**Juniper Networks, Inc.**

1194 North Mathilda Avenue  
Sunnyvale, California 94089

USA

408-745-2000

**[www.juniper.net](http://www.juniper.net)**

Part Number: 530-028689-01, Revision 1  
Published: 2010-03-28

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

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

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

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

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

Juniper Networks, 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. JUNOSe 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 Administration Guide*

Copyright © 2010, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Writing: Vinita Kurup, Praveen G R, S Muthuramalingam, Remya Naroth

Editing: Cindy Martin, Joan Hiraki

Cover Design: Edmonds Design

Revision History

March 25, 2010— Revision 1

The information in this document is current as of the date listed in the revision history.

## END USER LICENSE AGREEMENT

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

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

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

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

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

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

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

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

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

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

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

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.
7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.
8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.
9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.
10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.
11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.
12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.
13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.
14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, 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 présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).



# Table of Contents

	<b>About This Guide</b>	<b>xi</b>
	Objectives .....	xi
	Audience .....	xi
	Conventions .....	xii
	Documentation .....	xiii
	Requesting Technical Support .....	xiv
	Self-Help Online Tools and Resources .....	xv
	Opening a Case with JTAC .....	xv
<b>Part 1</b>	<b>Managing EX-series Switches with NSM</b>	
<b>Chapter 1</b>	<b>Configuring User Access and Authentication</b>	<b>3</b>
	Configuring RADIUS Authentication (NSM Procedure) .....	3
	Configuring TACACS+ Authentication (NSM Procedure) .....	4
	Configuring Authentication Order (NSM Procedure) .....	5
	Configuring User Access (NSM Procedure) .....	6
	Configuring Login Classes .....	6
	Configuring User Accounts .....	7
	Configuring Template Accounts (NSM Procedure) .....	7
	Creating a Remote Template Account .....	8
	Creating a Local Template Account .....	9
<b>Chapter 2</b>	<b>Configuring Chassis</b>	<b>11</b>
	Configuring Aggregated Devices (NSM Procedure) .....	11
	Configuring Chassis Alarms (NSM Procedure) .....	12
	Configuring Routing Engine Redundancy (NSM Procedure) .....	13
<b>Chapter 3</b>	<b>Configuring Class of Service</b>	<b>15</b>
	Configuring CoS Classifiers (NSM Procedure) .....	15
	Configuring CoS Code Point Aliases (NSM Procedure) .....	17
	Configuring CoS Drop Profile (NSM Procedure) .....	19
	Configuring CoS Forwarding Classes (NSM Procedure) .....	21
	Configuring CoS Interfaces (NSM Procedure) .....	22
	Configuring CoS Rewrite Rules (NSM Procedure) .....	28

	Configuring CoS Schedulers (NSM Procedure) .....	31
	Configuring CoS and Applying Scheduler Maps (NSM Procedure) .....	32
<b>Chapter 4</b>	<b>Configuring Ethernet Switching Options</b>	<b>35</b>
	Configuring Port Mirroring to Analyze Traffic on EX-series Switches (NSM Procedure) .....	35
	Configuring Redundant Trunk Links (NSM Procedure) .....	36
	Configuring Port Security (NSM Procedure) .....	37
	Configuring Static IP (NSM Procedure) .....	39
	Configuring VoIP (NSM Procedure) .....	40
<b>Chapter 5</b>	<b>Configuring Firewall Filters</b>	<b>43</b>
	Configuring a Firewall Filter .....	43
	Configuring a Policer for a Firewall Filter .....	46
<b>Chapter 6</b>	<b>Configuring Policy Options</b>	<b>49</b>
	Configuring an AS Path in a BGP Routing Policy (NSM Procedure) .....	49
	Configuring an AS Path Group in a BGP Routing Policy (NSM Procedure) .....	50
	Configuring a Community for use in BGP Routing Policy Conditions (NSM Procedure) .....	51
	Configuring a BGP Export Policy Condition (NSM Procedure) .....	52
	Configuring Flap Damping to Reduce the Number of BGP Update Messages (NSM Procedure) .....	53
	Configuring a Routing Policy Statement (NSM Procedure) .....	55
	Configuring Prefix List (NSM Procedure) .....	56
<b>Chapter 7</b>	<b>Configuring Routing Options</b>	<b>59</b>
	Configuring Maximum Prefixes (NSM Procedure) .....	59
	Configuring Multicast (NSM Procedure) .....	61
	Configuring Multipath (NSM Procedure) .....	64
	Configuring Options (NSM Procedure) .....	65
	Configuring Route Resolution (NSM Procedure) .....	66
	Configuring Routing Table Groups (NSM Procedure) .....	67
	Configuring Routing Tables (NSM Procedure) .....	69
	Configuring Source Routing (NSM Procedure) .....	71
	Configuring Static Routes (NSM Procedure) .....	72
	Configuring Generated Routes (NSM Procedure) .....	73
	Configuring Graceful Restart (NSM Procedure) .....	74
	Configuring Forwarding Table (NSM Procedure) .....	75
	Configuring Flow Route (NSM Procedure) .....	77
	Configuring Fate Sharing (NSM Procedure) .....	79
	Configuring Martian Addresses (NSM Procedure) .....	80
	Configuring Interface Routes (NSM Procedure) .....	82
	Configuring Instance Export (NSM Procedure) .....	83

	Configuring Instance Import (NSM Procedure) .....	83
	Configuring Confederation (NSM Procedure) .....	84
	Configuring Maximum Paths (NSM Procedure) .....	85
<b>Chapter 8</b>	<b>Configuring Protocols</b>	<b>87</b>
	Configuring the BFD Protocol (NSM Procedure) .....	87
	Configuring BGP (NSM Procedure) .....	88
	Configuring 802.1X Authentication (NSM Procedure) .....	91
	Configuring 802.1X Interface Settings .....	91
	Configuring Static MAC Bypass .....	93
	Configuring GVRP (NSM Procedure) .....	93
	Configuring IGMP (NSM Procedure) .....	94
	Configuring IGMP Snooping on EX-series Switches (NSM Procedure) .....	96
	Configuring LLDP (NSM Procedure) .....	97
	Configuring LLDP-MED (NSM Procedure) .....	98
	Configuring MSTP (NSM Procedure) .....	99
	Configuring OSPF (NSM Procedure) .....	101
	Configuring RIP (NSM Procedure) .....	105
	Configuring RSTP on EX-series Switches (NSM Procedure) .....	107
	Configuring STP (NSM Procedure) .....	108
	Configuring VSTP (NSM Procedure) .....	110
	Configuring VRRP (NSM Procedure) .....	112
<b>Chapter 9</b>	<b>Configuring PoE</b>	<b>115</b>
	Configuring Power over Ethernet (NSM Procedure) .....	115
<b>Chapter 10</b>	<b>Configuring SNMP</b>	<b>117</b>
	Configuring Basic System Identification for SNMP (NSM Procedure) .....	117
	Configuring SNMP Views (NSM Procedure) .....	118
	Configuring SNMP Communities (NSM Procedure) .....	119
	Configuring SNMP Trap Groups (NSM Procedure) .....	121
<b>Chapter 11</b>	<b>Configuring Virtual LANs</b>	<b>123</b>
	Configuring VLANs (NSM Procedure) .....	123
<b>Chapter 12</b>	<b>Configuring a Virtual Chassis</b>	<b>125</b>
	Configuring a Virtual Chassis .....	125
	Configuring a Virtual Chassis with a Preprovisioned Configuration File .....	125
	Add a Member to a Virtual Chassis .....	126

**Part 2**

**Index**

---

Index .....131

# About This Guide

- Objectives on page xi
- Audience on page xi
- Conventions on page xii
- Documentation on page xiii
- Requesting Technical Support on page xiv

## 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.

NSM uses the technology developed for Juniper Networks ScreenOS to enable and simplify management support for previous and future versions of ScreenOS. By integrating management of all Juniper Networks security devices, NSM enhances the overall security of the Internet gateway.

This guide explains how to configure EX-series devices. Use this guide in conjunction with the NSM Online Help, which provides step-by-step instructions for many of the processes described in this document.



**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 intended for system administrators responsible for the security infrastructure of their organization. Specifically, this book discusses concepts of interest to firewall and VPN administrators, network/security operations center administrators; and system administrators responsible for user permissions on the network.

## 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 xii defines notice icons used in this guide.

**Table 1: Notice Icons**





Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

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

**Table 2: Text Conventions**

Convention	Description	Examples
<b>Bold typeface like this</b>	<ul style="list-style-type: none"><li>■ Represents commands and keywords in text.</li><li>■ Represents keywords</li><li>■ Represents UI elements</li></ul>	<ul style="list-style-type: none"><li>■ Issue the <b>clock source</b> command.</li><li>■ Specify the keyword <b>exp-msg</b>.</li><li>■ Click <b>User Objects</b></li></ul>
<b>Bold typeface like this</b>	Represents text that the user must type.	user input
<b>fixed-width font</b>	Represents information as displayed on the terminal screen.	<pre>host1# show ip ospf Routing Process OSPF 2 with Router ID 5.5.0.250 Router is an area Border Router (ABR)</pre>
Key names linked with a plus (+) sign	Indicates that you must press two or more keys simultaneously.	Ctrl + d

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

Convention	Description	Examples
<i>Italics</i>	<ul style="list-style-type: none"> <li>■ Emphasizes words</li> <li>■ Identifies variables</li> </ul>	<ul style="list-style-type: none"> <li>■ The product supports two levels of access, <i>user</i> and <i>privileged</i>.</li> <li>■ <i>clusterID</i>, <i>ipAddress</i>.</li> </ul>
The angle bracket (>)	Indicates navigation paths through the UI by clicking menu options and links.	<b>Object Manager &gt; User Objects &gt; Local Objects</b>

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

**Table 3: Syntax Conventions**

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

## Documentation

Table 4 on page xiii describes documentation for the NSM.

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

Book	Description
<i>Network and Security Manager Installation Guide</i>	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.

**Table 4: Network and Security Manager Publications (continued)**

Book	Description
<i>Network and Security Manager Administration Guide</i>	<p>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.</p> <p>This guide is intended for application administrators or those individuals responsible for owning the server and security infrastructure and configuring the product for multi-user systems. It is also intended for device configuration administrators, firewall and VPN administrators, and network security operation center administrators.</p>
<i>Network and Security Manager Configuring ScreenOS and IDP Devices Guide</i>	Provides details about configuring the device features for all supported ScreenOS and IDP platforms.
<i>Network and Security Manager Online Help</i>	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.
<i>Network and Security Manager API Guide</i>	Provides complete syntax and description of the SOAP messaging interface to NSM.
<i>Network and Security Manager Release Notes</i>	<p>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.</p> <p>Release notes are included on the corresponding software CD and are available on the Juniper Networks Website.</p>
<i>Configuring Infranet Controllers Guide</i>	Provides details about configuring the device features for all supported Infranet Controllers.
<i>Configuring Secure Access Devices Guide</i>	Provides details about configuring the device features for all supported Secure Access Devices.
<i>Configuring EX-series Switches Guide</i>	Provides details about configuring the device features for all supported EX-series platforms .
<i>Configuring J-series Services Routers and SRX-series Services Gateways Guide</i>	Provides details about configuring the device features for all supported J-series Services Routers and SRX-series Services Gateways.
<i>M-series and MX-series Devices Guide</i>	Provides details about configuring the device features for M-series and MX-series platforms.

## 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 postsales 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> .
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/> .
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

### **Self-Help Online Tools and Resources**

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

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

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

### **Opening a Case with JTAC**

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

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

For international or direct-dial options in countries without toll-free numbers, visit us at <http://www.juniper.net/support/requesting-support.html>



## Part 1

# Managing EX-series Switches with NSM

The chapters in Part 1 of the Release 2009.1 version of the *NSM Configuration Guide for EX Series Devices* provide an overview of the management system and describe how to configure features for EX Series devices.



**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.

---

Part 1 contains the following chapters:

- Configuring User Access and Authentication on page 3
- Configuring Chassis on page 11
- Configuring Class of Service on page 15
- Configuring Ethernet Switching Options on page 35
- Configuring Firewall Filters on page 43
- Configuring Policy Options on page 49
- Configuring Routing Options on page 59
- Configuring Protocols on page 87
- Configuring PoE on page 115
- Configuring SNMP on page 117
- Configuring Virtual LANs on page 123
- Configuring a Virtual Chassis on page 125



## Chapter 1

# Configuring User Access and Authentication

This section contains the following:

- Configuring RADIUS Authentication (NSM Procedure) on page 3
- Configuring TACACS+ Authentication (NSM Procedure) on page 4
- Configuring Authentication Order (NSM Procedure) on page 5
- Configuring User Access (NSM Procedure) on page 6
- Configuring Template Accounts (NSM Procedure) on page 7

## Configuring RADIUS Authentication (NSM Procedure)

---

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

To configure RADIUS authentication:

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

**Table 5: RADIUS Authentication Configuration Details**

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

- Related Topics**
- Configuring TACACS+ Authentication (NSM Procedure) on page 4
  - Configuring Authentication Order (NSM Procedure) on page 5
  - Configuring User Access (NSM Procedure) on page 6

## Configuring TACACS+ Authentication (NSM Procedure)

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

To configure TACACS+ authentication:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab and then double-click the device for which you want to configure TACACS+ authentication.
3. Click the **Configuration** tab. In the configuration tree, select **System > TACACS+ Server**.
4. Add or modify TACACS+ settings as specified in Table 6 on page 4.
5. Click one:
  - **New**—Adds a new TACACS+ server.
  - **OK**—Saves the changes.
  - **Cancel**—Cancels the modifications.

**Table 6: TACACS+ Authentication Configuration Details**

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

**Table 6: TACACS+ Authentication Configuration Details** (continued)

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

- Related Topics**
- Configuring RADIUS Authentication (NSM Procedure) on page 3
  - Configuring Authentication Order (NSM Procedure) on page 5
  - Configuring User Access (NSM Procedure) on page 6

## 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 3
  - Configuring TACACS + Authentication (NSM Procedure) on page 4
  - Configuring User Access (NSM Procedure) on page 6

## Configuring User Access (NSM Procedure)

---

This section includes the following topics:

- Configuring Login Classes on page 6
- Configuring User Accounts on page 7

### Configuring Login Classes

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

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

To configure login classes:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab and then double-click the device for which you want to configure a login class.
3. Click the **Configuration** tab. In the configuration tree, select **System > Login > Class**.
4. Add or modify login class settings as specified in Table 7 on page 6.
5. Click one:
  - **New**—Adds a new login class.
  - **OK**—Saves the changes.
  - **Cancel**—Cancels the modifications.

**Table 7: Login Class Authentication Configuration Details**

Option	Function	Your Action
Name	Specifies a name for the login class.	Enter a name for the login class.
Allow Commands	Specifies the operational mode commands that members of a login class can use.	Enter the command name enclosed in quotation marks. For example, <b>“request system reboot”</b> .
<b>Login &gt; Class &gt; Permissions</b>		
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 8 on page 7.
5. Click one:
  - **New**—Adds a new user account.
  - **OK**—Saves the changes.
  - **Cancel**—Cancels the modifications.

**Table 8: User Authentication Configuration Details**

Option	Function	Your Action
Name	Identifies the user with a unique name.	Enter a unique name for the user.
Class	Specifies the user's login class.	Select the class name.
<b>Login &gt; User &gt; Authentication</b>		
Plain Text Password Value	Specifies the user's password.	Enter the plain text password for the user.

- Related Topics**
- Configuring RADIUS Authentication (NSM Procedure) on page 3
  - Configuring TACACS+ Authentication (NSM Procedure) on page 4
  - Configuring Authentication Order (NSM Procedure) on page 5

## 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 8
- Creating a Local Template Account on page 9

## Creating a Remote Template Account

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

By default, JUNOS software with enhanced services uses the remote template account when:

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

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

To create a remote template account:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab and then double-click the device for which you want to create a remote template account.
3. Click the **Configuration** tab. In the configuration tree, select **System > Login > User**.
4. Add or modify login class settings as specified in Table 9 on page 8.
5. Click one:
  - **New**—Creates a new remote template account.
  - **OK**—Saves the changes.
  - **Cancel**—Cancels the modifications.

**Table 9: Remote Template Account Details**

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

## Creating a Local Template Account

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

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

To create a local template account:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab and then double-click the device for which you want to create a local template account.
3. Click the **Configuration** tab. In the configuration tree, select **System > Login > User**.
4. Add or modify login class settings as specified in Table 10 on page 9.
5. Click one:
  - **New**—Creates a new local template account.
  - **OK**—Saves the changes.
  - **Cancel**—Cancels the modifications.

**Table 10: Local Template Account Details**

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

- Related Topics**
- Configuring RADIUS Authentication (NSM Procedure) on page 3
  - Configuring TACACS+ Authentication (NSM Procedure) on page 4
  - Configuring Authentication Order (NSM Procedure) on page 5



## Chapter 2

# Configuring Chassis

This section contains the following:

- Configuring Aggregated Devices (NSM Procedure) on page 11
- Configuring Chassis Alarms (NSM Procedure) on page 12
- Configuring Routing Engine Redundancy (NSM Procedure) on page 13

### Configuring Aggregated Devices (NSM Procedure)

---

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

To configure the aggregated devices on the router:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Chassis > Aggregated Devices**.
4. Add or modify the settings as specified in Table 11 on page 12.
5. Click one:
  - OK—Saves the changes.
  - Cancel—Cancels the modifications.

**Table 11: Aggregated Devices Configuration Details**

Task	Your Action
Configure properties for Ethernet aggregated devices.	<ol style="list-style-type: none"><li>1. Click <b>Ethernet</b> next to Aggregated Devices.</li><li>2. Enter the number of aggregated logical devices available to the router. Range: 1 through 256 devices</li><li>3. Click <b>Lacp</b> next to Ethernet.</li><li>4. In the <b>System Priority</b> box, enter the priority for the aggregated Ethernet system.</li><li>5. Click <b>Link Protection</b> next to Lacp.</li><li>6. Select the <b>Non Revertive</b> 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.</li></ol>
Configure properties for sonet aggregated devices.	<ol style="list-style-type: none"><li>1. Click <b>Sonet</b> next to Aggregated Devices.</li><li>2. From the <b>Device Count</b> list, select the number of aggregated logical devices available to the router. Range: 1 through 16 Devices</li></ol>

- Related Topics**
- Configuring Chassis Alarms (NSM Procedure) on page 12
  - Configuring a T640 Router on a Routing Matrix (NSM Procedure)
  - Configuring Routing Engine Redundancy (NSM Procedure) on page 13
  - Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors (NSM Procedure)

## Configuring Chassis Alarms (NSM Procedure)

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

To configure chassis alarm on the router:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Chassis > Alarm**.
4. Add or modify the alarm settings as specified in Table 12 on page 13.
5. Click one:
  - OK—Saves the changes.
  - Cancel—Cancels the modifications.

**Table 12: Chassis Alarms Configuration Details**

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

- Related Topics**
- Configuring Aggregated Devices (NSM Procedure) on page 11
  - Configuring Chassis FPC (NSM Procedure)
  - Configuring Routing Engine Redundancy (NSM Procedure) on page 13

## Configuring Routing Engine Redundancy (NSM Procedure)

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

To configure routing engine redundancy in NSM:

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

**Table 13: Chassis Redundancy Configuration Details**

Task	Your Action
Configure redundancy options.	<ol style="list-style-type: none"> <li>1. In the <b>Comment</b> box, enter the comment.</li> <li>2. From the <b>keepalive</b> list, select the time before the backup router takes mastership when it detects loss of the keepalive signal. Range: 2 through 10,000</li> </ol>
Instruct the backup router to take mastership if it detects hard disk errors or a loss of a keepalive signal from the master Routing Engine.	<ol style="list-style-type: none"> <li>1. Click <b>Failover</b> next to Redundancy.</li> <li>2. In the <b>Comment</b> box, enter the comment.</li> <li>3. Select the type of failover.</li> </ol>

**Table 13: Chassis Redundancy Configuration Details** (continued)

Task	Your Action
For routing platforms with two Routing Engines, configure a master Routing Engine to switch over gracefully to a backup Routing Engine without interruption to packet forwarding.	<ol style="list-style-type: none"><li>1. Click <b>Graceful Switchover</b> next to Redundancy.</li><li>2. In the <b>Comment</b> box, enter the comment.</li></ol>
Sets the function of the Routing Engine for the specified slot. By default, the Routing Engine in slot 0 is the master Routing Engine and the Routing Engine in slot 1 is the backup Routing Engine.	<ol style="list-style-type: none"><li>1. Click <b>Routing Engine</b> next to Redundancy.</li><li>2. From the <b>Name</b> list, select the slot number.</li><li>3. In the <b>Comment</b> box, enter the comment.</li><li>4. Select the function of the Routing Engine for the specified slot.</li><li>5. Select one of the following:<ul style="list-style-type: none"><li>■ <b>master</b>—To configure the routing engine to be the master.</li><li>■ <b>backup</b>—To configure the routing engine to be the backup.</li><li>■ <b>disabled</b>—To disable the routing engine.</li></ul></li></ol>

- Related Topics**
- Configuring Aggregated Devices (NSM Procedure) on page 11
  - Configuring a T640 Router on a Routing Matrix (NSM Procedure)
  - Configuring a Routing Engine to Reboot or Halt on Hard Disk Errors (NSM Procedure)

## Chapter 3

# Configuring Class of Service

This section contains the following:

- Configuring CoS Classifiers (NSM Procedure) on page 15
- Configuring CoS Code Point Aliases (NSM Procedure) on page 17
- Configuring CoS Drop Profile (NSM Procedure) on page 19
- Configuring CoS Forwarding Classes (NSM Procedure) on page 21
- Configuring CoS Interfaces (NSM Procedure) on page 22
- Configuring CoS Rewrite Rules (NSM Procedure) on page 28
- Configuring CoS Schedulers (NSM Procedure) on page 31
- Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 32

### 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 14 on page 16.
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 14: Configuring and Applying Behavior Aggregate Classifiers**

Task	Action
Configure behavior aggregate classifiers for DiffServ CoS.	<ol style="list-style-type: none"> <li>1. Click <b>Add new entry</b> next to Dscp.</li> <li>2. In the Name box, type the name of the behavior aggregate classifier—for example, <b>ba-classifier</b>.</li> <li>3. In the Import box, type the name of the default DSCP map.</li> </ol>
Configure a best-effort forwarding class classifier.	<ol style="list-style-type: none"> <li>1. Click <b>Add new entry</b> next to Forwarding class.</li> <li>2. In the Class name box, type the name of the previously configured best-effort forwarding class—for example, <b>be-class</b>.</li> <li>3. Click <b>Add new entry</b> next to Loss priority.</li> <li>4. From the Loss val list, select <b>high</b>.</li> <li>5. Click <b>Add new entry</b> next to Code points.</li> <li>6. In the Value box, type the value of the high-priority code point for best-effort traffic—for example, <b>00001</b>.</li> <li>7. Click <b>OK</b> three times.</li> </ol>
Configure an expedited forwarding class classifier.	<ol style="list-style-type: none"> <li>1. Click <b>Add new entry</b> next to Forwarding class.</li> <li>2. In the Class name box, type the name of the previously configured expedited forwarding—for example, <b>class-ef-class</b>.</li> <li>3. Click <b>Add new entry</b> next to Loss priority.</li> <li>4. From the Loss val list, select <b>high</b>.</li> <li>5. Click <b>Add new entry</b> next to Code points.</li> <li>6. In the Value box, type the value of the high-priority code point for expedited forwarding traffic—for example, <b>101111</b>.</li> <li>7. Click <b>OK</b> three times.</li> </ol>

**Table 14: Configuring and Applying Behavior Aggregate Classifiers** (continued)

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

- Related Topics**
- Configuring CoS Code Point Aliases (NSM Procedure) on page 17
  - Configuring CoS Drop Profile (NSM Procedure) on page 19
  - Configuring CoS Forwarding Classes (NSM Procedure) on page 21
  - Configuring CoS Interfaces (NSM Procedure) on page 22
  - Configuring CoS Rewrite Rules (NSM Procedure) on page 28
  - Configuring CoS Schedulers (NSM Procedure) on page 31
  - Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 32

## 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 15 on page 18
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 15: Configuring Code Point Aliases**

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

- Related Topics**
- Configuring CoS Classifiers (NSM Procedure) on page 15
  - Configuring CoS Drop Profile (NSM Procedure) on page 19
  - Configuring CoS Forwarding Classes (NSM Procedure) on page 21
  - Configuring CoS Interfaces (NSM Procedure) on page 22
  - Configuring CoS Rewrite Rules (NSM Procedure) on page 28
  - Configuring CoS Schedulers (NSM Procedure) on page 31
  - Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 32

## 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 16 on page 19.
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 16: Drop Profile Configuration Fields**

Option	Function	Your Action
Drop Profile		

**Table 16: Drop Profile Configuration Fields** (continued)

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

- Related Topics**
- Configuring CoS Classifiers (NSM Procedure) on page 15
  - Configuring CoS Code Point Aliases (NSM Procedure) on page 17
  - Configuring CoS Forwarding Classes (NSM Procedure) on page 21
  - Configuring CoS Interfaces (NSM Procedure) on page 22
  - Configuring CoS Rewrite Rules (NSM Procedure) on page 28
  - Configuring CoS Schedulers (NSM Procedure) on page 31
  - Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 32

## 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 17 on page 21.
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 17: Assigning Forwarding Classes to Output Queues**

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

**Table 17: Assigning Forwarding Classes to Output Queues** (continued)

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

- Related Topics**
- Configuring CoS Classifiers (NSM Procedure) on page 15
  - Configuring CoS Code Point Aliases (NSM Procedure) on page 17
  - Configuring CoS Drop Profile (NSM Procedure) on page 19
  - Configuring CoS Interfaces (NSM Procedure) on page 22
  - Configuring CoS Rewrite Rules (NSM Procedure) on page 28
  - Configuring CoS Schedulers (NSM Procedure) on page 31
  - Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 32

## 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 18 on page 23.
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 18: Interfaces Configuration Fields**

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

**Table 18: Interfaces Configuration Fields** (continued)

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

**Table 18: Interfaces Configuration Fields** (continued)

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

**Table 18: Interfaces Configuration Fields** (continued)

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

**Table 18: Interfaces Configuration Fields** (continued)

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

- Related Topics**
- Configuring CoS Classifiers (NSM Procedure) on page 15
  - Configuring CoS Code Point Aliases (NSM Procedure) on page 17
  - Configuring CoS Drop Profile (NSM Procedure) on page 19
  - Configuring CoS Forwarding Classes (NSM Procedure) on page 21
  - Configuring CoS Rewrite Rules (NSM Procedure) on page 28
  - Configuring CoS Schedulers (NSM Procedure) on page 31
  - Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 32

## Configuring CoS Rewrite Rules (NSM Procedure)

---

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

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

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

To configure CoS rewrite rules:

1. In the navigation tree, select **Device Manager > Devices**
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure CoS rewrite rules.
3. Click the **Configuration** tab. In the configuration tree, expand **Class of Service**
4. Select **Rewrite Rules**.
5. Add or modify settings as specified in Table 19 on page 28.
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 19: Configuring and Applying Rewrite Rules**

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

---

**Table 19: Configuring and Applying Rewrite Rules** (continued)

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

**Table 19: Configuring and Applying Rewrite Rules** (continued)

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

- Related Topics**
- Configuring CoS Classifiers (NSM Procedure) on page 15
  - Configuring CoS Code Point Aliases (NSM Procedure) on page 17
  - Configuring CoS Drop Profile (NSM Procedure) on page 19
  - Configuring CoS Forwarding Classes (NSM Procedure) on page 21
  - Configuring CoS Interfaces (NSM Procedure) on page 22
  - Configuring CoS Schedulers (NSM Procedure) on page 31
  - Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 32

## 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 20 on page 31.
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 20: Configuring Schedulers**

Task	Action
Specify the buffer size.	<ol style="list-style-type: none"> <li>1. Click the <b>Add New</b> icon.</li> <li>2. Expand <b>Buffer Size</b>.</li> <li>3. Select <b>Percent</b>.</li> <li>4. Under Percent, select the appropriate option:               <ul style="list-style-type: none"> <li>■ To specify no buffer size, select <b>None</b>.</li> <li>■ To specify buffer size as a percentage of the total buffer, select <b>percent</b> and type an integer from 1 through 100.</li> <li>■ To specify buffer size as the remaining available buffer, select <b>remainder</b>.</li> </ul> </li> <li>5. Click <b>OK</b>.</li> </ol>

**Table 20: Configuring Schedulers (continued)**

Task	Action
Configure drop profile map.	<ol style="list-style-type: none"><li>1. Click the <b>Add New</b> icon.</li><li>2. Select <b>drop-profile-map</b>.</li><li>3. In the Loss Priority box, select the required loss priority—for example, <b>high</b>.</li><li>4. In the Protocol box, select the type of protocol—for example, <b>any</b>.</li><li>5. In the Drop Profile box, select the previously configured drop profile.</li><li>6. Click <b>OK</b>.</li></ol>
Specify the transmit rate.	<ol style="list-style-type: none"><li>1. Click the <b>Add New</b> icon.</li><li>2. Expand <b>Transmit Rate</b>.</li><li>3. Select <b>Rate</b>.</li><li>4. Under Rate, select the appropriate option:<ul style="list-style-type: none"><li>■ To not specify transmit rate, select <b>None</b>.</li><li>■ To enforce a specific transmission rate, select <b>rate</b> and type the transmission rate that you want to enforce.</li><li>■ To specify a percentage of transmission capacity, select <b>percent</b> and type an integer from 1 through 100.</li><li>■ To specify the remaining transmission capacity, select <b>remainder</b>.</li></ul></li><li>5. Click <b>OK</b>.</li></ol>

- Related Topics**
- Configuring CoS Classifiers (NSM Procedure) on page 15
  - Configuring CoS Code Point Aliases (NSM Procedure) on page 17
  - Configuring CoS Drop Profile (NSM Procedure) on page 19
  - Configuring CoS Forwarding Classes (NSM Procedure) on page 21
  - Configuring CoS Interfaces (NSM Procedure) on page 22
  - Configuring CoS Rewrite Rules (NSM Procedure) on page 28
  - Configuring CoS and Applying Scheduler Maps (NSM Procedure) on page 32

## 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 21 on page 33.
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 21: Assigning Forwarding Classes to Output Queues**

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

**Table 21: Assigning Forwarding Classes to Output Queues** (continued)

Task	Action
Apply the scheduler map to an interface.	<ol style="list-style-type: none"><li data-bbox="581 384 1425 415">1. Select <b>Interfaces &gt; Interface</b> and click <b>Add new entry</b>.</li><li data-bbox="581 426 1425 457">2. In the Interface name box, type the name of the interface—for example, <b>ge-0/0/0</b>.</li><li data-bbox="581 468 1425 499">3. Select <b>Unit</b> and click <b>Add new entry</b>.</li><li data-bbox="581 510 1425 541">4. In the Unit name box, select the logical interface unit number—for example, <b>0</b>.</li><li data-bbox="581 552 1425 604">5. In the Scheduler map box, type the name of the previously configured scheduler map—for example, <b>diffserv-cos-map</b>.</li><li data-bbox="581 615 1425 653">6. Click <b>OK</b>.</li></ol>

- Related Topics**
- Configuring CoS Classifiers (NSM Procedure) on page 15
  - Configuring CoS Code Point Aliases (NSM Procedure) on page 17
  - Configuring CoS Drop Profile (NSM Procedure) on page 19
  - Configuring CoS Forwarding Classes (NSM Procedure) on page 21
  - Configuring CoS Interfaces (NSM Procedure) on page 22
  - Configuring CoS Rewrite Rules (NSM Procedure) on page 28
  - Configuring CoS Schedulers (NSM Procedure) on page 31

## Chapter 4

# Configuring Ethernet Switching Options

This section contains the following:

- Configuring Port Mirroring to Analyze Traffic on EX-series Switches (NSM Procedure) on page 35
- Configuring Redundant Trunk Links (NSM Procedure) on page 36
- Configuring Port Security (NSM Procedure) on page 37
- Configuring Static IP (NSM Procedure) on page 39
- Configuring VoIP (NSM Procedure) on page 40

## Configuring Port Mirroring to Analyze Traffic on EX-series Switches (NSM Procedure)

---

You configure port mirroring in order to copy packets so that you can analyze traffic using a protocol analyzer application. You can mirror traffic entering or exiting an interface, or entering a VLAN. You can send the mirrored packets to a local interface to monitor traffic locally or to a VLAN to monitor traffic remotely.

Mirroring a high volume of traffic can be performance intensive for the switch. Therefore, you should disable port mirroring when you are not using it and select specific input interfaces in preference to using the `all` keyword. You can also limit the amount of mirrored traffic by using a firewall filter or the `ratio` keyword to mirror only a selection of packets.



**NOTE:** Only one analyzer can be enabled on an EX-series switch. To create additional analyzers, first disable any existing analyzers.



**NOTE:** Interfaces used as input or output for a port mirror analyzer must be configured as family `ethernet-switching`.

---

To mirror interface traffic or VLAN traffic on the switch to an interface on the switch:

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 **Ethernet Switching Options**.
4. Select **Analyzer**.

5. Click the Add icon.
6. Add/modify member settings for the interface as specified in Table 22 on page 36.



**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 22: Analyzer Configuration Fields**

Field	Function	Your Action
<b>Input</b>		
Ingress	Specifies interfaces or VLANs for which entering traffic is mirrored.	Click <b>Add</b> and select Port or VLAN. Next, select the interfaces or VLANs.
Egress	Specifies interfaces for which traffic exiting the interfaces is mirrored.	Click <b>Add</b> to add egress interfaces.
<b>Output</b>		
Interface	Specifies the interface on which traffic exiting is mirrored.	Select the interface.
Vlan	Specifies the VLAN on which traffic exiting is mirrored.	Select the interface.

## Configuring Redundant Trunk Links (NSM Procedure)

Simplify the convergence configuration in a typical enterprise network by configuring a primary link and a secondary link on trunk ports. If the primary link fails, the secondary link automatically takes over without waiting for normal STP convergence.

To configure redundant trunk links:

1. In the navigation tree, select **Device Manager > Devices**. In Device Manager, select the device for which you want to configure redundant trunk links.
2. In the Configuration tree, expand **Ethernet Switching Options**.
4. Select **Redundant Trunk Group > Group**.
5. Click the Add icon.
6. Add/modify settings as specified in Table 25 on page 38.  
Add/modify settings for the VLAN as specified in Table 23 on page 37.



**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 23: Redundant Trunk Group Settings**

Option	Function	Your Action
Name	Specifies the name for the redundant trunk group.	Enter the name.
Interface	Specifies the interface that must be part of the redundant trunk group.	<ol style="list-style-type: none"> <li>1. Select <b>Interface</b>.</li> <li>2. Click <b>Add</b>.</li> <li>3. Specify the interface.</li> <li>4. Select <b>Primary</b> if the interface must be the primary link.</li> <li>5. Click <b>OK</b>.</li> </ol>

## Configuring Port Security (NSM Procedure)

Ethernet LANs are vulnerable to attacks such as address spoofing and Layer 2 denial of service (DoS) on network devices. Port security features such as DHCP snooping, DAI (dynamic ARP inspection), MAC limiting, and MAC move limiting, as well as trusted DHCP server, help protect the access ports on your switch against the losses of information and productivity that can result from such attacks.

To configure port security:

1. In the navigation tree, select **Device Manager > Devices**. In Device Manager, select the device for which you want to configure port security.
2. In the Configuration tree, expand **Ethernet Switching Options**.
4. Select **Secure Access Port > Interface** or **VLAN**.
5. Click the Add icon.
6. Add/modify settings for the interface as specified in Table 25 on page 38.  
Add/modify settings for the VLAN as specified in Table 24 on page 37.



**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 24: Port Security Settings on VLANs**

Option	Function	Your Action
Name	Specifies the VLAN.	Enter the VLAN name.

**Table 24: Port Security Settings on VLANs (continued)**

Option	Function	Your Action
DHCP Snooping	Allows the switch to monitor and control DHCP messages received from untrusted devices connected to the switch. Builds and maintains a database of valid IP addresses/MAC address bindings. (By default, access ports are untrusted and trunk ports are trusted.)	Select to enable DHCP snooping on a specified VLAN or all VLANs.
ARP Inspection	Uses information in the DHCP snooping database to validate ARP packets on the LAN and protect against ARP cache poisoning.	Select to enable ARP inspection on a specified VLAN or all VLANs. (Configure any port on which you do not want ARP inspection to occur as a trusted DHCP server port.)
MAC Move Limit	Prevents hosts whose MAC addresses have not been learned by the switch from accessing the network. Specifies the number of times per second that a MAC address can move to a new interface.	Select the MAC Move Limit Option. Select the required number.
MAC Movement Action	Specifies the action to be taken if the MAC move limit is exceeded.	Select one: <ul style="list-style-type: none"> <li>■ Log—Generate a system log entry, an SNMP trap, or an alarm.</li> <li>■ Drop—Drop the packets and generate a system log entry, an SNMP trap, or an alarm.</li> <li>■ Shutdown—Block data traffic on the interface and generate an alarm.</li> <li>■ None— No action to be taken.</li> </ul>

**Table 25: Port Security on Interfaces**

Option	Function	Your Action
Interface	Specifies trusting DHCP packets on the selected interface. By default trunk ports are <b>dhcp-trusted</b> .	Select to enable DHCP trust.
Allowed MAC List	Specifies the MAC addresses that are allowed for the interface.	To add a MAC address: <ol style="list-style-type: none"> <li>1. Click <b>Add</b>.</li> <li>2. Enter the MAC address.</li> <li>3. Click <b>OK</b>.</li> </ol>
MAC Limit	Specifies the number of MAC addresses that can be learned on a single Layer 2 access port. This option is not valid for trunk ports.	Enter the required number.

**Table 25: Port Security on Interfaces** (continued)

Option	Function	Your Action
MAC Limit Action	Specifies the action to be taken if the MAC limit is exceeded. This option is not valid for trunk ports.	Select one: <ul style="list-style-type: none"> <li>■ Log—Generate a system log entry, an SNMP trap, or an alarm.</li> <li>■ Drop—Drop the packets and generate a system log entry, an SNMP trap, or an alarm.</li> <li>■ Shutdown—Block data traffic on the interface and generate an alarm.</li> <li>■ None— No action to be taken.</li> </ul>
static ip	Specifies the static ip address for the interface.	Enter the following: <ul style="list-style-type: none"> <li>■ Name</li> <li>■ Vlan</li> <li>■ Mac</li> </ul>

## Configuring Static IP (NSM Procedure)

The static IP feature enables you to associate a fixed IP address and a static media access control (MAC) address or hardware address with a VLAN associated with an interface. The VLAN and the MAC addresses are configured for the associated interface, which in turn is associated with a device.

To configure static IP 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 **Static** and select **VLAN**.
5. Add/Modify as specified in Table 26 on page 40.
6. Click one:
  - OK—To save the changes.
  - Cancel—To cancel 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* for more information.

**Table 26: Static Configuration Fields**

Option	Function	Your Action
VLAN	Specifies the VLAN to be configured for static IP.	<ol style="list-style-type: none"><li>1. Expand <b>Static</b> tree and select <b>VLAN</b>.</li><li>2. Click the <b>New</b> button or select a VLAN and click <b>Edit</b> button in <b>VLAN</b> interface.</li><li>3. Enter the name of the VLAN and the comment.</li><li>4. Click <b>OK</b>.</li></ol>
Mac	Media access control (MAC) address, or hardware address, for the device connected to the specified interface.	<ol style="list-style-type: none"><li>1. Expand <b>Static</b> tree and select <b>VLAN</b>.</li><li>2. Click the <b>New</b> button or select a VLAN and click <b>Edit</b> button in <b>VLAN</b> interface.</li><li>3. Expand <b>VLAN</b> tree and select <b>Mac</b>.</li><li>4. Click the <b>New</b> button or select a Mac and click <b>Edit</b> button in <b>Mac</b> interface.</li><li>5. Specify the name, comment and the next hop.</li><li>6. Click <b>OK</b>.</li></ol>

## Configuring VoIP (NSM Procedure)

Voice over IP (VoIP) refers to voice communications over the internet or other packet switched networks. The VoIP feature enables you to configure voice over IP for interfaces.

To configure VoIP 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 **Ethernet Switching Options** and select **VoIP**.
5. Expand **VoIP** tree and select **Interfaces**
6. Add or modify as specified in Table 27 on page 41.
7. Click one:
  - **OK**—To save the changes.
  - **Cancel**—To cancel 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 for more information.

**Table 27: VoIP Configuration Fields**

Option	Function	Your Action
Name	Specifies the interface name.	<ol style="list-style-type: none"> <li>1. Click the New button or select an interface and click on Edit button in <b>Interface</b>.</li> <li>2. Enter the interface name in the <b>Name</b> box or select from the list.</li> </ol>
Comment	Specifies the comment for the interface to which the VoIP is assigned.	<ol style="list-style-type: none"> <li>1. Click the New button or select an interface and click on Edit button in <b>Interface</b>.</li> <li>2. Enter the comment in the <b>Comment</b> box.</li> </ol>
VLAN	Specifies the VLAN to be assigned to the interface.	<ol style="list-style-type: none"> <li>1. Click the New button or select an interface and click on Edit button in <b>Interface</b>.</li> <li>2. Enter the VLAN address in the <b>VLAN</b> box.</li> </ol>
Forwarding Class	Specifies the forwarding class to which the interface is assigned.	<ol style="list-style-type: none"> <li>1. Click the New button or select an interface and click on Edit button in <b>Interface</b>.</li> <li>2. Enter the forwarding class in the <b>Forwarding Class</b> box.</li> </ol>



## Chapter 5

# Configuring Firewall Filters

This section contains the following:

- Configuring a Firewall Filter on page 43
- Configuring a Policer for a Firewall Filter on page 46

### Configuring a Firewall Filter

---

You configure firewall filters on EX-series switches to control traffic that enters ports on the switch or enters and exits VLANs on the network and Layer 3 (routed) interfaces. To configure a firewall filter you must configure the filter and then apply it to a port, VLAN, or Layer 3 interface.

To configure a firewall filter and apply it to an interface:

1. In the navigation tree, select Device Manager > Devices. In Device Manager, select the device for which you want to configure firewall filters.
2. In the configuration tree, expand **Firewall**.
3. Expand **Ethernet Switching** and click **Filter**.
4. Click **Add New Entry** to add a firewall filter.
5. Perform the configuration tasks described in Table 28 on page 43.



**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 28: Create a New Term**

Option	Function	Your Action
Term Name	Specifies the name of the term.	Enter a name.
ICMP Type	Specifies the ICMP packet type field. Typically, you specify this match in conjunction with the protocol match to determine which protocol is being used on the port.	Select the option from the list.

---

**Table 28: Create a New Term (continued)**

ICMP Code	Specifies more specific information than icmp-type. Because the value's meaning depends upon the associated icmp-type, you must specify icmp-type along with icmp-code. The keywords are grouped by the ICMP type with which they are associated.	Select one: <ul style="list-style-type: none"><li>■ Parameter-problem</li><li>■ Redirect</li><li>■ Time-exceeded</li><li>■ Unreachable</li></ul>
Fragment Flags	Specifies the IP fragmentation flags. <b>NOTE:</b> Fragment flags is supported on ingress ports, VLANs, and router interfaces.	Select either the option <b>is-fragment</b> or enter a combination of fragment flags.
TCP Flags	Specifies one or more TCP flags. <b>NOTE:</b> TCP flags is supported on ingress ports, VLANs, and router interfaces.	Select either the option <b>tcp-initial</b> or enter a combination of TCP flags.
IP Precedence	Specifies IP precedence. The options are: assured forwarding, best-effort, expedited-forwarding, network-control. <b>NOTE:</b> IP precedence and DSCP number cannot be specified together for the same term.	Select the option from the list.
Interface	Specifies the interface association.	Select the interface from the list.
Ether Type	Specifies the ethernet type field of a packet. <b>NOTE:</b> This option is not applicable for a Routing filter.	Select one: <ul style="list-style-type: none"><li>■ Arp</li><li>■ Dot 1q</li></ul>
dot1q-tag	Specifies the tag field in the Ethernet header. Values can be from 1 through 4095. <b>NOTE:</b> This option is not applicable for a Routing filter.	Enter the required number.

**Table 28: Create a New Term (continued)**

Dot 1q User Priority	<p>Specifies the user-priority field of the tagged Ethernet packet. User-priority values can be 0–7.</p> <p>In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed)</p> <ul style="list-style-type: none"> <li>■ background (1)—Background</li> <li>■ best-effort (0)—Best effort</li> <li>■ controlled-load (4)—Controlled load</li> <li>■ excellent-load (3)—Excellent load</li> <li>■ network-control (7)—Network control reserved traffic</li> <li>■ standard (2)—Standard or Spare</li> <li>■ video (5)—Video</li> <li>■ voice (6)—Voice</li> </ul> <p><b>NOTE:</b> This option is not applicable for a Routing filter.</p>	Enter a number or the corresponding text synonym.
DSCP Number	<p>Specifies the Differentiated Services code point (DSCP). The DiffServ protocol uses the type-of-service (ToS) byte in the IP header. The most significant six bits of this byte form the DSCP.</p>	Select the DSCP number from the list.
VLAN	<p>Specifies the VLAN to be associated.</p> <p><b>NOTE:</b> This option is not applicable for a Routing filter.</p>	Enter the VLAN name
TTL Value	<p>Specifies the time-to-live value.</p> <p><b>NOTE:</b> This option is applicable for a Routing filter.</p>	Enter a value.
Packet Length	<p>Specifies the length of the packet.</p> <p><b>NOTE:</b> This option is applicable for a Routing filter.</p>	Enter a value.
<b>Action</b>		
Counter Name	<p>Specifies the count of the number of packets that pass this filter, term, or policer.</p>	Enter a value.

**Table 28: Create a New Term (continued)**

Forwarding Class	Classifies the packet into one of the following forwarding classes: <ul style="list-style-type: none"><li>■ assured-forwarding</li><li>■ best-effort</li><li>■ expedited-forwarding</li><li>■ network-control</li><li>■ user-defined</li></ul>	Select the option from the list.
Loss Priority	Specifies the Packet Loss Priority. <b>NOTE:</b> Forwarding Class and Loss Priority should be specified together for the same term.	Enter the value.
Analyzer	Specifies whether to perform port-mirroring on packets. Port-mirroring copies all packets seen on one switch port to a network monitoring connection on another switch port.	Select the analyzer from the list.

## 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 29 on page 47.



**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 29: Configuring a Policer for a Firewall Filter**

Task	Action
Create the policer for expedited forwarding, and give the policer a name—for example, ef-policer.	Select <b>Policer</b> and click <b>Add new entry</b> .  In the Policer name box, type <b>ef-policer</b> .
Set the burst limit for the policer—for example, 2k.	1. Select <b>If exceeding</b> .
Set the bandwidth limit or percentage for the bandwidth allowed for this type of traffic—for example, use a bandwidth percent of 10.	2. In the Burst Size Limit box, type a limit for the burst size allowed—for example, 2k. 3. Select <b>Bandwidth Limit</b> , select <b>bandwidth-limit</b> . 4. In the box, type 10. 5. Click <b>OK</b> .
Enter the loss priority for packets exceeding the limits established by the policer—for example, high.	1. Select <b>Then</b> . 2. In the <b>Comment</b> field, enter <b>high</b> . 3. Click <b>OK</b> .



## Chapter 6

# Configuring Policy Options

This section contains the following:

- Configuring an AS Path in a BGP Routing Policy (NSM Procedure) on page 49
- Configuring an AS Path Group in a BGP Routing Policy (NSM Procedure) on page 50
- Configuring a Community for use in BGP Routing Policy Conditions (NSM Procedure) on page 51
- Configuring a BGP Export Policy Condition (NSM Procedure) on page 52
- Configuring Flap Damping to Reduce the Number of BGP Update Messages (NSM Procedure) on page 53
- Configuring a Routing Policy Statement (NSM Procedure) on page 55
- Configuring Prefix List (NSM Procedure) on page 56

### **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 30 on page 50.
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 30: AS Path Configuration Details**

Option	Function	Your Action
Name	Specifies the name of the AS path.	Enter a name.
Comment	Specifies the comment for the AS path.	Enters a comment.
Path	Specifies the AS path (as an AS number) to be included in the routing policy.	Enter an AS path.

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

Autonomous System (AS) path group consists of multiple AS paths. You can define match conditions based on the AS path groups. You can create named AS paths under an AS path group and then include the AS path group in a routing policy.

To configure an AS path group for a BGP routing policy in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Policy Options**.
5. Select **As Path Group**.
6. Add or modify the parameters as specified in Table 31 on page 51.
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 31: AS Path Group Configuration Details**

Option	Function	Your Action
Name	Specifies the name of the AS path group.	Enter a name.
Comment	Specifies the comment for the AS path group.	Enter a comment.
As Path	Specifies an AS path to be included in the AS path group. Specifies the name and comment for the AS path and specifies the path as an AS path number.	<ol style="list-style-type: none"> <li>1. Select <b>As Path</b>.</li> <li>2. Click the <b>New</b> button or select an AS path and click the <b>Edit</b> button.</li> <li>3. Specify the name, comment and path.</li> <li>4. Click <b>OK</b>, then click <b>OK</b> again.</li> </ol>

## 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 32 on page 52.
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 32: Community Configuration Details**

Option	Function	Your Action
Name	Specifies the name of the community.	Enter the name.
Comment	Specifies the comment for the community.	Enter the comment.
Invert Match	Enables you to invert the results for the community expression.	Select the check-box if you want to invert the results. Clear the check-box if you do not want to invert the results.
Members	Specifies one or more community members.	<ol style="list-style-type: none"><li>1. Select <b>Members</b>.</li><li>2. Click the <b>New</b> button or select a member and click the <b>Edit</b> button.</li><li>3. Enter the member community.</li><li>4. Click <b>OK</b>, then click <b>OK</b> again.</li></ol>

## 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 33 on page 53.
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 33: Condition Configuration Details**

Option	Function	Your Action
Name	Specifies the name of the condition.	Enter a name.
Comment	Specifies the comment for the condition.	Enter a comment.
Route Active On	Enables you to specify the policy condition based on the existing routes and the corresponding route tables.	<ol style="list-style-type: none"> <li>Select <b>Route Active On</b>.</li> <li>Select one: <ul style="list-style-type: none"> <li>None—No policy condition based on routes need to be specified.</li> <li>if-route-exists—Specify the policy condition based on the routes. Enter the comment, route and the corresponding routing table.</li> </ul> </li> <li>Click <b>OK</b>.</li> </ol>

## 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:

- In the navigation tree, select **Device Manager > Devices**.
- In the **Devices** list, double-click the device to select it.
- Click the **Configuration** tab.
- In the configuration tree, expand **Policy Options**.
- Select **Damping**.

6. Add or modify the parameters as specified in Table 34 on page 54.
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 34: Damping Configuration Details**

Option	Function	Your Action
Name	Specifies the name of the damping parameter setting.	Enter a name.
Comment	Specifies the comment for the damping parameter setting.	Enter a comment.
Disable	Enables you to disable damping on a per-prefix basis. Any damping state that is present in the routing table for a prefix is deleted if damping is disabled.	Select the check-box to disable damping. Clear the check-box to enable damping.
Half Life	Indicates the time in minutes interval after which the accumulated figure-of-merit value is reduced by half if the route remains stable. Figure-of-merit values correlate to the probability of future instability of a device. Routes with higher figure-of-merit values are suppressed for longer periods of time.	Enter the time limit in minutes or select it from the list.
Reuse	Indicates the figure-of-merit value below which a suppressed route can be used again.	Enter the value or select it from the list.
Suppress	Indicates the figure-of-merit value above which a route is suppressed for use or inclusion in advertisements.	Enter the value or select it from the list.
Max Suppress	Indicates the maximum time in minutes that a route can be suppressed no matter how unstable it has been.	<ol style="list-style-type: none"> <li>1. Enter the time limit or select it from the list.</li> <li>2. Click OK.</li> </ol>

## 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 35 on page 55.
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 35: Configuring Policy Statement Fields**

Option	Function	Your Action
Name	Specifies the name of the policy statement.	<ol style="list-style-type: none"> <li>1. Click the <b>New</b> button or select a policy statement and click <b>Edit</b> button.</li> <li>2. Select <b>policy-statement</b> .</li> <li>3. Specify the name.</li> </ol>
Comment	Specifies the comment for the policy statement.	<ol style="list-style-type: none"> <li>1. Click the <b>New</b> button or select a policy statement and click <b>Edit</b> button.</li> <li>2. Select <b>policy-statement</b> .</li> <li>3. Specify the comment.</li> </ol>

**Table 35: Configuring Policy Statement Fields (continued)**

Option	Function	Your Action
From	Enables you to define the criteria that an incoming route must match. You can specify one or more match conditions. If you specify more than one, all conditions must match the route for a match to occur.	<ol style="list-style-type: none"> <li>1. Click the New button or select a policy statement and click Edit button.</li> <li>2. Expand <b>policy-statement</b> tree and select <b>From</b>.</li> <li>3. Enter the From criteria.</li> <li>4. Expand <b>From</b> tree and specify the match conditions.</li> </ol>
Term	Indicates the term to be configured for the routing policy. You can create one or more terms for a routing policy. Each term comprises of match conditions and the corresponding actions.	<ol style="list-style-type: none"> <li>1. Click the New button or select a policy statement and click Edit button.</li> <li>2. Expand <b>policy-statement</b> tree and select <b>Term</b>.</li> <li>3. Click the New button or select a term and click Edit button.</li> <li>4. Enter the term name, comment and the match conditions and actions.</li> </ol>
Then	Enables you to define the action to be taken in the case of a match or mismatch between the packets and From and To conditions.	<ol style="list-style-type: none"> <li>1. Click the New button or select a policy statement and click Edit button.</li> <li>2. Expand <b>policy-statement</b> tree and select <b>Then</b>.</li> <li>3. Specify the parameters for Then criteria.</li> <li>4. Expand <b>Then</b> tree and specify the actions for each match condition.</li> </ol>
To	Enables you to define the criteria that an outgoing route must match. You can specify one or more match conditions. If you specify more than one, all conditions must match the route for a match to occur.	<ol style="list-style-type: none"> <li>1. Click the New button or select a policy statement and click Edit button.</li> <li>2. Expand <b>policy-statement</b> tree and select <b>To</b>.</li> <li>3. Enter the To criteria.</li> <li>4. Expand <b>To</b> tree and specify the match conditions.</li> </ol>

## 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 36 on page 57.
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 36: Configuring Prefix List Fields**

Field	Function	Your Action
Name	Specifies the name of the prefix list.	<ol style="list-style-type: none"> <li>1. Click the New button or select a prefix list and click Edit button.</li> <li>2. Select <b>prefix-list</b> .</li> <li>3. Specify the name.</li> </ol>
Comment	Specifies the comment for the prefix list.	<ol style="list-style-type: none"> <li>1. Click the New button or select a prefix list and click Edit button.</li> <li>2. Select <b>prefix-list</b> .</li> <li>3. Specify the comment.</li> </ol>
Apply Path	Indicates that the prefix list should include all IP prefixes pointed to by a defined path.	<ol style="list-style-type: none"> <li>1. Click the New button or select a prefix list and click Edit button.</li> <li>2. Select <b>prefix-list</b> .</li> <li>3. Specify the path.</li> </ol>
Prefix List Item	Specifies the prefix list item.	<ol style="list-style-type: none"> <li>1. Click the New button or select a prefix list and click Edit button.</li> <li>2. Expand <b>prefix-list</b> tree and select <b>Prefix List Item</b>.</li> <li>3. Specify the name and comment.</li> </ol>



## Chapter 7

# Configuring Routing Options

This section contains the following:

- Configuring Maximum Prefixes (NSM Procedure) on page 59
- Configuring Multicast (NSM Procedure) on page 61
- Configuring Multipath (NSM Procedure) on page 64
- Configuring Options (NSM Procedure) on page 65
- Configuring Route Resolution (NSM Procedure) on page 66
- Configuring Routing Table Groups (NSM Procedure) on page 67
- Configuring Routing Tables (NSM Procedure) on page 69
- Configuring Source Routing (NSM Procedure) on page 71
- Configuring Static Routes (NSM Procedure) on page 72
- Configuring Generated Routes (NSM Procedure) on page 73
- Configuring Graceful Restart (NSM Procedure) on page 74
- Configuring Forwarding Table (NSM Procedure) on page 75
- Configuring Flow Route (NSM Procedure) on page 77
- Configuring Fate Sharing (NSM Procedure) on page 79
- Configuring Martian Addresses (NSM Procedure) on page 80
- Configuring Interface Routes (NSM Procedure) on page 82
- Configuring Instance Export (NSM Procedure) on page 83
- Configuring Instance Import (NSM Procedure) on page 83
- Configuring Confederation (NSM Procedure) on page 84
- Configuring Maximum Paths (NSM Procedure) on page 85

### **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 37 on page 60.
7. Click one:
  - **OK**—To save the changes.
  - **Cancel**—To cancel the modifications.
  - **Apply**—To apply the routing option settings.



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

**Table 37: Configuring Maximum Prefixes Fields**

Option	Function	Your Action
Comment	Specifies the comment for the maximum prefix limit.	Enter the comment.
Limit	Indicates the maximum number of route prefixes. If this limit is reached, a warning is triggered and additional routes are rejected.	Enter limit value or select from the list.
Log Interval	Indicates the minimum time interval (in seconds) between log messages.	Enter the log interval value or select from the list.
Threshold	Specifies what is to be done when the routing table reaches the maximum prefix value. The options are: <ul style="list-style-type: none"> <li>■ <b>None</b>—No action is to be taken.</li> <li>■ <b>threshold</b>—You can configure a percentage for the maximum number of prefixes, which when installed, triggers the warning.</li> <li>■ <b>log-only</b>—Sets the prefix limit as an advisory limit. An advisory limit triggers only a warning, and additional routes are not rejected.</li> </ul>	<ol style="list-style-type: none"> <li>1. Expand the <b>Maximum Prefixes</b> tree and select <b>Threshold</b>.</li> <li>2. Select the option button.</li> </ol>

## 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 38 on page 61.
7. Click one:
  - **OK**—To save the changes.
  - **Cancel**—To cancel the modifications.
  - **Apply**—To apply the routing option settings.



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

**Table 38: Configuring Multicast Fields**

Option	Function	Your Action
Comment	Specifies the comment for the multicast configuration.	Enter the comment.
Backup Pe Group	Enables you to configure a backup provider edge (PE) group for ingress PE device redundancy when point-to-multipoint (P2MP) label-switched paths (LSPs) are used for multicast distribution.	<ol style="list-style-type: none"> <li>1. Expand the <b>Multicast</b> tree and select <b>Backup Pe Group</b>.</li> <li>2. Click the <b>New</b> button or select a group and click the <b>Edit</b> button.</li> <li>3. Configure the PE group name, local address, and backup address.</li> </ol>

**Table 38: Configuring Multicast Fields** (continued)

Option	Function	Your Action
Flow Map	<p>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 .</p>	<ol style="list-style-type: none"> <li>1. Expand the <b>Multicast</b> tree and select <b>Flow Map</b>.</li> <li>2. Click the <b>New</b> button or select a flow map and click the <b>Edit</b> button.</li> <li>3. Configure the following to create and define a flow map: <ul style="list-style-type: none"> <li>■ Enter the flow map name and comment.</li> <li>■ <b>Bandwidth</b>—Specify the bandwidth property of the multicast flow map.</li> <li>■ <b>Forwarding Cache</b>—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.</li> <li>■ <b>Policy</b>—Specify the flow map policies.</li> <li>■ <b>Redundant Sources</b>—Specify the addresses for use as backup sources for multicast flows defined by a flow map.</li> </ul> </li> </ol>
Forwarding Cache	<p>Enables you to configure multicast forwarding cache properties. These properties include threshold suppression and reuse limits, and timeout values.</p> <p>You can specify a value for the threshold to suppress new multicast forwarding cache entries and an optional reuse value for the threshold at which the device begins to create new multicast forwarding cache entries. If you configure both reuse and suppression values, configure a reuse value that is less than the suppression value. The suppression value is mandatory. If you do not specify the optional reuse value, then the number of multicast forwarding cache entries is limited to the suppression value. A new entry is created as soon as the number of multicast forwarding cache entries falls below the suppression value. You can also specify a timeout value for all multicast forwarding cache entries.</p>	<ol style="list-style-type: none"> <li>1. Expand the <b>Multicast</b> tree and select <b>Forwarding Cache</b>.</li> <li>2. Configure the timeout and threshold values.</li> </ol>

**Table 38: Configuring Multicast Fields** (continued)

Option	Function	Your Action
Interface	Enables you to configure the interfaces for multicast properties on which you plan to manage the maximum bandwidth.	<ol style="list-style-type: none"> <li>Expand the <b>Multicast</b> tree and select <b>Interface</b>.</li> <li>Configure the interface and the bandwidth.</li> </ol>
Rpf Check Policy	<p>Multicast reverse path forwarding (RPF) checks are used to prevent multicast routing loops. Routing loops are particularly debilitating in multicast applications because packets are replicated with each pass around the routing loop.</p> <p>You can apply policies for disabling reverse-path forwarding (RPF) checks on arriving multicast packets.</p>	<ol style="list-style-type: none"> <li>Expand the <b>Multicast</b> tree and select <b>Rpf Check Policy</b>.</li> <li>Click the <b>New</b> button or select a policy and click the <b>Edit</b> button.</li> <li>Enter the RPF check policy name.</li> </ol>
Scope	Enables you to configure multicast scoping to limit multicast traffic by configuring it to an administratively defined topological region. Multicast scoping controls the propagation of multicast messages—both multicast group joins upstream toward a source and data forwarding downstream. Scoping can relieve stress on scarce resources, such as bandwidth, and improve privacy or scaling properties.	<ol style="list-style-type: none"> <li>Expand the <b>Multicast</b> tree and select <b>Scope</b>.</li> <li>Configure the scope and the interface for the multicast.</li> </ol>
Scope Policy	Enables you to configure multicast scoping policy. A multicast scope policy contains a set of device interfaces on which you are configuring scoping and the scope's address range configured as a series of device filters.	<ol style="list-style-type: none"> <li>Expand the <b>Multicast</b> tree and select <b>Scope Policy</b>.</li> <li>Specify the scope policy for the multicast group.</li> </ol>
Ssm Groups	Enables you to configure source-specific multicast (SSM) groups. SSM is a service model that identifies session traffic by both source and group address. Using SSM, a client can receive multicast traffic directly from the source. To deploy SSM successfully, you need an end-to-end multicast-enabled network and applications that use an Internet Group Management Protocol version 3 (IGMPv3).	<ol style="list-style-type: none"> <li>Expand the <b>Multicast</b> tree and select <b>Ssm Groups</b>.</li> <li>Click the <b>New</b> button or select a group and click the <b>Edit</b> button.</li> <li>Specify the address range of the SSM group.</li> </ol>
Ssm Map	SSM mapping translate IGMPv1 or IGMPv2 membership reports to an IGMPv3 report allowing you to support an SSM network without requiring all hosts to support IGMPv3.	<ol style="list-style-type: none"> <li>Expand the <b>Multicast</b> tree and select <b>Ssm Map</b>.</li> <li>Click the <b>New</b> button or select an SSM map and click the <b>Edit</b> button.</li> <li>Specify the SSM policy for the SSM map and the source address.</li> </ol>

**Table 38: Configuring Multicast Fields** (continued)

Option	Function	Your Action
Traceoptions	Defines tracing options for the multicast group. You can also set up the file management and access control parameters .	<ol style="list-style-type: none"><li>1. Expand the <b>Multicast</b> tree and select the <b>Traceoptions</b> tab.</li><li>2. Set up the file and flag parameters.</li></ol>

## Configuring Multipath (NSM Procedure)

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

To configure multipath load balancing in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Multipath**.
6. Enter the parameters as specified in Table 39 on page 64.
7. Click one:
  - **OK**—To save the changes.
  - **Cancel**—To cancel the modifications.
  - **Apply**—To apply the routing option settings.



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

**Table 39: Configuring Multipath Fields**

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

**Table 39: Configuring Multipath Fields** (continued)

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

## 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 40 on page 66.
7. Click one:
  - **OK**—To save the changes.
  - **Cancel**—To cancel the modifications.
  - **Apply**—To apply the routing option settings.



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

**Table 40: Configuring Options Fields**

Option	Function	Your Action
Comment	Specifies the comment for the message option.	Enter the comment.
Mark	Specifies the mark for the option.	Enter the mark value or select from the list.
Syslog	Enables you to configure the generation of system log messages for a particular severity level and all higher levels.	<ol style="list-style-type: none"><li>1. Expand the <b>Options</b> tree and select <b>Syslog</b>.</li><li>2. Select the severity levels for system log messages.</li></ol>

## Configuring Route Resolution (NSM Procedure)

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

To configure a route resolution table in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Resolution**.
6. Add or modify the parameters as specified in Table 41 on page 67.
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 41: Route Resolution Fields**

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

## 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 42 on page 68.
7. Click one:

- OK—To save the changes.
- Cancel—To cancel the modifications.
- Apply—To apply the routing option settings.



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

**Table 42: Rib Group Fields**

Option	Function	Your Action
Name	Specifies the unique name for the routing table group.	<ol style="list-style-type: none"> <li>1. Expand the <b>Routing Options</b> tree and select <b>Rib Group</b>.</li> <li>2. Click the New button or select a routing table group and click the Edit button.</li> <li>3. Enter the name for the routing table group.</li> </ol>
Comment	Specifies the comment for the routing table group.	<ol style="list-style-type: none"> <li>1. Expand the <b>Routing Options</b> tree and select <b>Rib Group</b>.</li> <li>2. Click the New button or select a routing table group and click the Edit button.</li> <li>3. Enter the comment for the routing table group.</li> </ol>
Export Rib	Specifies the routing table from which the JUNOS software exports routing information.	<ol style="list-style-type: none"> <li>1. Expand the <b>Routing Options</b> tree and select <b>Rib Group</b>.</li> <li>2. Click the New button or select a routing table group and click the Edit button.</li> <li>3. Enter the name of the routing table.</li> </ol>
Import Policy	Enables you to apply one or more policies to routes imported into the routing table group.	<ol style="list-style-type: none"> <li>1. Expand the <b>rib-group</b> tree and select <b>Import Policy</b>.</li> <li>2. Set up the import policies for the routing table group.</li> </ol>

**Table 42: Rib Group Fields** (continued)

Option	Function	Your Action
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.	<ol style="list-style-type: none"> <li>1. Expand the <b>rib-group</b> tree and select <b>Import Policy</b>.</li> <li>2. Enter the name of the routing table.</li> </ol>

## 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 43 on page 70.
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 43: Rib Fields**

Option	Function	Your Action
Name	Specifies the unique name for the routing table.	<ol style="list-style-type: none"><li>1. Expand the <b>Routing Options</b> tree and select <b>Rib</b>.</li><li>2. Click the <b>New</b> button or select a routing table and click the <b>Edit</b> button.</li><li>3. Enter the name for the routing table.</li></ol>
Comment	Specifies the comment for the route resolution.	<ol style="list-style-type: none"><li>1. Expand the <b>Routing Options</b> tree and select <b>Rib</b>.</li><li>2. Click the <b>New</b> button or select a routing table and click the <b>Edit</b> button.</li><li>3. Enter the comment for the routing table.</li></ol>
Aggregate	Enables you to configure the aggregate routes for the routing table. Aggregation allows you to combine groups of routes with common addresses into a single entry in the routing table. This decreases the size of the routing table as well as the number of route advertisements sent by the router.	<ol style="list-style-type: none"><li>1. Expand the <b>Rib</b> tree and select <b>Aggregate</b>.</li><li>2. Select the global aggregate route options in <b>Defaults</b> and individual aggregate route options in <b>Route</b>.</li></ol>
Generate	Enables you to configure generated routes, which are used as routes of last resort in the routing table.	<ol style="list-style-type: none"><li>1. Expand the <b>Rib</b> tree and select <b>Generate</b>.</li><li>2. Select the default route to the destination address in <b>Defaults</b> and individually generated route options in <b>Route</b>.</li></ol>
Martians	Enables you to configure martian addresses in the routing table.	<ol style="list-style-type: none"><li>1. Expand the <b>Rib</b> tree and select <b>Martian</b>.</li><li>2. Enter the martian addresses.</li></ol>
Maximum Paths	Enables you to configure a limit for the number of routes installed in a routing table.	<ol style="list-style-type: none"><li>1. Expand the <b>Rib</b> tree and select <b>Maximum Paths</b>.</li><li>2. Enter the <b>Maximum Paths</b> and the <b>Threshold</b>.</li></ol>
Maximum Prefixes	Enables you to configure a limit for the number of routes installed in a routing table.	<ol style="list-style-type: none"><li>1. Expand the <b>Rib</b> tree and select <b>Maximum Prefixes</b>.</li><li>2. Set up the <b>Maximum Prefixes</b> and the <b>Threshold</b>.</li></ol>

**Table 43: Rib Fields** (continued)

Option	Function	Your Action
Multipath	Enables you to configure the multipath option in the routing table for load sharing between external BGP and internal BGP.	<ol style="list-style-type: none"> <li>Expand the Rib tree and select <b>Multipath</b>.</li> <li>Enter the multipath options.</li> </ol>
Static	Enables you to configure static routes to be installed in the routing table.	<ol style="list-style-type: none"> <li>Expand the Rib tree and select <b>Static</b>.</li> <li>Enter the global static route in <b>Defaults</b> and destination address of the static route in <b>Route</b>.</li> </ol>

## 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:

- In the navigation tree, select **Device Manager > Devices**.
- In the **Devices** list, double-click the device to select it.
- Click the **Configuration** tab.
- In the configuration tree, expand **Routing Options**.
- Select **Source Routing**.
- Enter the parameters as specified in Table 44 on page 71.
- 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 44: Source Routing Fields**

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

**Table 44: Source Routing Fields** (continued)

Option	Function	Your Action
Ip	Specifies the IPv4 addressing family for source routing.	Select the check box.
Ipv6	Specifies the IPv6 addressing family for source routing.	Select the check box.

## Configuring Static Routes (NSM Procedure)

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

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

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

To configure static routes for a routing table group in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Static**.
6. Add or modify the parameters as specified in Table 26 on page 40.
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 45: Static Fields**

Option	Function	Your Action
Comment	Specifies the comment for the static route.	Enter the comment.
Rib Group	Specifies the routing table group name for which the static route is configured.	Enter the name.
Defaults	Enables you to configure the global static route options. These options only set the global defaults and apply to all the configured static routes.	<ol style="list-style-type: none"> <li>1. Expand the <b>Static</b> tree and select <b>Defaults</b>.</li> <li>2. Enter the default route to the destination address.</li> </ol>
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 <b>Defaults</b> section.	<ol style="list-style-type: none"> <li>1. Expand the <b>Static</b> tree and select <b>Route</b>.</li> <li>2. Enter the individual route.</li> </ol>

## 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 46 on page 74.
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 46: Generated Routes Fields**

Option	Function	Your Action
Comment	Specifies the comment for the generated route.	Enter a comment.
Defaults	Enables you to specify globally generated route options. These are treated as global defaults and apply to all the generated routes you configure.	<ol style="list-style-type: none"> <li>1. Expand the <b>Generate</b> tree and select <b>Defaults</b>.</li> <li>2. Configure the default route options.</li> </ol>
Route	Enables you to configure individually generated routes. You can also configure globally generated route options. These options apply to the individual destination only and override any options you configured in Defaults.	<ol style="list-style-type: none"> <li>1. Expand the <b>Generate</b> tree and select <b>Route</b>.</li> <li>2. Configure the individual route options.</li> </ol>

## Configuring Graceful Restart (NSM Procedure)

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

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

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

To configure graceful restart in NSM:

1. In the navigation tree, select **Device Manager > Devices** .
2. In the **Devices** list, double click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Graceful Restart**.
6. Enter the parameters as specified in Table 47 on page 75.
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 47: Graceful Restart Fields**

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

## Configuring Forwarding Table (NSM Procedure)

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

To configure forwarding table in NSM:

1. In the navigation tree, select **Device Manager > Devices** .
2. In the **Devices** list, double click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.

5. Select **Forwarding Table**.
6. Add or modify the parameters as specified in Table 48 on page 76.
7. Click one:
  - **OK**—To save the changes.
  - **Cancel**—To cancel the modifications.
  - **Apply**—To apply the routing option settings.



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

**Table 48: Forwarding Table Fields**

Option	Function	Your Action
Comment	Specifies the comment for the forwarding table.	Enter a comment.
None	Specifies that no next- hop parameter is to be added to the forwarding table.	Select the option button.
indirect-next-hop	Specifies that the forwarding table supports indirectly connected next hops.	Select the option button to enable <b>indirect-next- hop</b> .
no-indirect-next-hop	Specifies that the forwarding table does not support indirectly connected next hops.	Select the option button to enable <b>no-indirect-next- hop</b> .
Unicast Reverse Path	Enables you to check path validity to protect the network from IP spoofing. A unicast reverse-path-forwarding (RPF) check performs a routing table lookup on an IP packet's source address and checks the incoming interface. The device determines whether the packet is arriving from a path that the sender would use to reach the destination. If the packet is from a valid path, the device forwards the packet to the destination address. If it is not from a valid path, the device discards the packet.	Select the path from the drop-down list.
Export	Enables you to apply one or more policies to routes being exported from the routing table into the forwarding table.	<ol style="list-style-type: none"> <li>1. Expand the <b>Forwarding Table</b> tree and select <b>Export</b>.</li> <li>2. Enter the export policies.</li> </ol>

## 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 49 on page 77.
7. Click one:
  - **OK**—To save the changes.
  - **Cancel**—To cancel the modifications.
  - **Apply**—To apply the routing option settings.



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

**Table 49: Flow Route Fields**

Option	Function	Your Action
Comment	Specifies the comment for the flow route.	Enter a comment.
<b>Route</b>		
Name	Specifies the name of the flow route.	<ol style="list-style-type: none"> <li>1. Expand the <b>Flow</b> tree and select <b>Route</b>.</li> <li>2. Click the <b>New</b> button or select a flow route and click the <b>Edit</b> button.</li> <li>3. Enter the flow route name.</li> </ol>

**Table 49: Flow Route Fields (continued)**

Option	Function	Your Action
Comment	Specifies the comment for the flow route.	<ol style="list-style-type: none"><li>1. Expand the <b>Flow</b> tree and select <b>Route</b>.</li><li>2. Click the New button or select a flow route and click the Edit button.</li><li>3. Enter the comment for the flow route.</li></ol>
Match	Specifies the conditions that the packet must match for the packet to be included in flow route. Match conditions are: <ul style="list-style-type: none"><li>■ Destination Port</li><li>■ DSCP</li><li>■ Fragment</li><li>■ Icmp Code</li><li>■ Icmp Type</li><li>■ Packet Length</li><li>■ Port</li><li>■ Protocol</li><li>■ Source Port</li><li>■ Tcp Flag</li></ul>	<ol style="list-style-type: none"><li>1. Expand the <b>Route</b> tree and select <b>Match</b>.</li><li>2. Enter a comment for <b>Comment</b>, a destination address for <b>Destination</b>, and a source address for <b>Source</b>.</li><li>3. Configure the match conditions.</li></ol>
Then	Enables you to specify the action to take if the packet matches the conditions you have configured in the flow route.	<ol style="list-style-type: none"><li>1. Expand the <b>Route</b> tree and select <b>Then</b>.</li><li>2. Configure the then conditions for the packet.</li></ol>
<b>Validation</b>		
Comment	Specifies a comment for the validation procedure. Flow routes are installed into the flow routing table only if they have been validated using the validation procedure.	<ol style="list-style-type: none"><li>1. Expand the <b>Flow</b> tree and select <b>Validation</b>.</li><li>2. Enter the comment for the validation procedure.</li></ol>
Traceoptions	Enables you to define tracing operations that track all routing protocol functionality in the device and specify that tracing results be saved in a log file. You can configure the tracing flag, filter, and the tracing policy.	<ol style="list-style-type: none"><li>1. Expand the <b>Validation</b> tree and select <b>Traceoptions</b>.</li><li>2. Expand the <b>Traceoptions</b> tree and configure the file and flag parameters, and the tracing policy.</li></ol>

## 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 50 on page 79.
7. Click one:
  - **OK**—To save the changes.
  - **Cancel**—To cancel the modifications.
  - **Apply**—To apply the routing option settings.



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

**Table 50: Fate Sharing Fields**

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

**Table 50: Fate Sharing Fields (continued)**

Option	Function	Your Action
Name	Specifies the name of the fate sharing group.	<ol style="list-style-type: none"> <li>1. Expand the <b>Fate Sharing</b> tree and select <b>Group</b>.</li> <li>2. Click the <b>New</b> button or select a group and click the <b>Edit</b> button.</li> <li>3. Enter the group name.</li> </ol>
Comment	Specifies the comment for the fate sharing group.	<ol style="list-style-type: none"> <li>1. Expand the <b>Fate Sharing</b> tree and select <b>Group</b>.</li> <li>2. Click the <b>New</b> button or select a group and click the <b>Edit</b> button.</li> <li>3. Enter the comment.</li> </ol>
Cost	Specifies the configurable cost attributed to each group, which represents the level of impact this group has on CSPF computations. The higher the cost, the less likely a backup path will share any objects in the group with the primary path.	<ol style="list-style-type: none"> <li>1. Expand the <b>Fate Sharing</b> tree and select <b>Group</b>.</li> <li>2. Click the <b>New</b> button or select a group and click the <b>Edit</b> button.</li> <li>3. Enter the cost or select a value from the list.</li> </ol>
From	Specifies the from address and to address for point-to-point link objects.	<ol style="list-style-type: none"> <li>1. Expand the <b>Group</b> tree and select <b>From</b>.</li> <li>2. Click the <b>New</b> button or select a group and click the <b>Edit</b> button.</li> <li>3. Specify the <b>From</b> address.</li> </ol>

## 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 51 on page 81.
7. Click one:

- OK—To save the changes.
- Cancel—To cancel the modifications.
- Apply—To apply the routing option settings.



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

**Table 51: Configuring Martian Address Fields**

Option	Function	Your Action
Address	Specifies the martian address or the destination prefix of a series of martian addresses that are to be allowed or disallowed.	<ol style="list-style-type: none"> <li>1. Click the New button or select a martian address and click the Edit button.</li> <li>2. Enter the address.</li> </ol>
Comment	Specifies the comment for the martian address.	<ol style="list-style-type: none"> <li>1. Click the New button or select a martian address and click the Edit button.</li> <li>2. Enter the comment for the martian address.</li> </ol>
Allow	Enables you to explicitly allow a subset of a range of addresses that are to be disallowed.	<ol style="list-style-type: none"> <li>1. Click the New button or select a martian address and click the Edit button.</li> <li>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.</li> <li>3. Clear the check box to disallow the addresses and mark them as a martian address.</li> </ol>
Exact	Specifies match criteria for the route's mask length with the martian address. The criteria are: <ul style="list-style-type: none"> <li>■ Exact</li> <li>■ Longer</li> <li>■ Orlonger</li> <li>■ Upto</li> <li>■ Through</li> <li>■ Prefix Length Range</li> </ul>	<ol style="list-style-type: none"> <li>1. Click the New button or select a martian address and click the Edit button.</li> <li>2. Expand the Martian tree and select <b>Exact</b>.</li> <li>3. Enter the match criteria.</li> </ol>

## 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 52 on page 82.
7. Click one:
  - **OK**—To save the changes.
  - **Cancel**—To cancel the modifications.
  - **Apply**—To apply the routing option settings.



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

---

**Table 52: Interface Routes Fields**

Option	Function	Your Action
Comment	Specifies the comment for the interface route.	Enter a comment.
Family	Specifies the address family as IPv4 or IPv6.	<ol style="list-style-type: none"><li>1. Expand the <b>Interface Routes</b> tree and select <b>Family</b>.</li><li>2. Click the <b>New</b> button or select a family name and click the <b>Edit</b> button.</li><li>3. Enter the family name and comment.</li><li>4. Set up the export policy and import policy.</li></ol>

---

**Table 52: Interface Routes Fields** (continued)

Option	Function	Your Action
Rib Group	Specifies the routing table groups to which interface routes are imported.	<ol style="list-style-type: none"> <li>1. Expand the <b>Interface Routes</b> tree and select <b>Rib Group</b>.</li> <li>2. Enter the comment and Inet.</li> </ol>

## 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 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 53 on page 85.
7. Click one:
  - **OK**—To save the changes.
  - **Cancel**—To cancel the modifications.
  - **Apply**—To apply the routing option settings.



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

**Table 53: Confederation Fields**

Option	Function	Your Action
Comment	Specifies the comment for the confederation.	Enter a comment.
Confederation As	Specifies the confederation AS number.	Enter a number from 1 through 65535.
Members	Specifies the AS number of the confederation member, allowing you to add members to the confederation.	<ol style="list-style-type: none"> <li>1. Expand the <b>Confederation</b> tree and select <b>Members</b>.</li> <li>2. Click the <b>New</b> button or select a member and click the <b>Edit</b> button.</li> <li>3. Enter the AS number of the member.</li> </ol>

## 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 54 on page 86.
7. Click one:
  - **OK**—To save the changes.
  - **Cancel**—To cancel the modifications.
  - **Apply**—To apply the routing option settings.



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

**Table 54: Configuring Maximum Paths Fields**

Option	Function	Your Action
Comment	Specifies the comment for the maximum path limit.	Enter the comment.
Limit	Indicates the maximum number of routes. If this limit is reached, a warning is triggered and additional routes are rejected.	Enter limit value or select a value from the list.
Log Interval	Indicates the minimum time interval (in seconds) between log messages.	Enter the log interval value or select a value from the list.
Threshold	Specifies what is to be done when the routing table reaches the maximum path value. The options are: <ul style="list-style-type: none"><li>■ None</li><li>■ threshold—Percentage of the maximum number of routes when installed, starts triggering the warning. You can configure a percentage of the Limit value that when reached starts triggering the warnings.</li><li>■ log-only—Sets the route limit as an advisory limit. An advisory limit triggers only a warning, and additional routes are not rejected.</li></ul>	<ol style="list-style-type: none"><li>1. Expand the <b>Maximum Paths</b> tree and select <b>Threshold</b>.</li><li>2. Select the radio-button..</li></ol>

## Chapter 8

# Configuring Protocols

This section contains the following:

- Configuring the BFD Protocol (NSM Procedure) on page 87
- Configuring BGP (NSM Procedure) on page 88
- Configuring 802.1X Authentication (NSM Procedure) on page 91
- Configuring GVRP (NSM Procedure) on page 93
- Configuring IGMP (NSM Procedure) on page 94
- Configuring IGMP Snooping on EX-series Switches (NSM Procedure) on page 96
- Configuring LLDP (NSM Procedure) on page 97
- Configuring LLDP-MED (NSM Procedure) on page 98
- Configuring MSTP (NSM Procedure) on page 99
- Configuring OSPF (NSM Procedure) on page 101
- Configuring RIP (NSM Procedure) on page 105
- Configuring RSTP on EX-series Switches (NSM Procedure) on page 107
- Configuring STP (NSM Procedure) on page 108
- Configuring VSTP (NSM Procedure) on page 110
- Configuring VRRP (NSM Procedure) on page 112

### 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 55 on page 88.
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 55: Configuring Bfd Fields**

Field	Function	Your Action
Comment	Specifies the comment for Bfd.	Enter the comment.
Traceoptions	Enables you to define tracing operations that track all routing protocol functionality in the device. You can configure the tracing flag, filter, and the tracing policy.	<ol style="list-style-type: none"> <li>1. Expand the <b>Bfd</b> tree and select <b>Traceoptions</b>.</li> <li>2. Expand the <b>Traceoptions</b> tree and set up the file and flag parameters.</li> </ol>

## 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 56 on page 89.
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 56: BGP Configuration Fields**

Field	Function	Your Action
General	The general parameters to be set up for applying BGP.	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree.</li> <li>2. Select <b>BGP</b> and select <b>General</b> tab.</li> <li>3. Specify the general parameters like comment, description, local address, hold time, etc.</li> </ol>
Path Selection	Enables you to specify the path selection criteria.	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree.</li> <li>2. Select <b>BGP</b> and select <b>Path Selection</b> tab.</li> <li>3. Set up the path selection parameters and med plus IGP.</li> </ol>
Traceoptions	Defines trace options for IGMP snooping.	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree.</li> <li>2. Select <b>BGP</b> and select <b>Traceoptions</b> tab.</li> <li>3. Set up the file and flag parameters.</li> </ol>
Metric Out	Enables you to specify the metric value to add to the routes transmitted to the neighbor.	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree.</li> <li>2. Select <b>BGP</b> and select <b>Metric Out</b> tab.</li> <li>3. Set up the metric value and minimum IGP.</li> </ol>
Multihop	If an EBGP peer is more than one hop away from the local router, you must specify the next hop to the peer so that the two systems can establish a BGP session. This type of session is called a multihop BGP session.	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree.</li> <li>2. Select <b>BGP</b> and select <b>Multihop</b> tab.</li> <li>3. Set up the comment, Ttl and specify whether the next hop has to be changed.</li> </ol>

**Table 56: BGP Configuration Fields** (continued)

Field	Function	Your Action
Advertise	Enables you to specify whether BGP should advertise the best route even if the routing table did not select it to be an active route.	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree.</li> <li>2. Select <b>BGP</b> and select <b>Advertise</b> tab.</li> <li>3. Specify whether Advertise has to be inactivated and set up the Advertise Peer As.</li> </ol>
Import	Enables you to apply one or more routing policies to routes being imported into the JUNOS routing table from BGP .	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree.</li> <li>2. Select <b>BGP</b> and select <b>Import</b> tab.</li> <li>3. Specify the export policies configured on the peer.</li> </ol>
Family	Enables you to configure protocol family information for the logical interface.	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree.</li> <li>2. Select <b>BGP</b> and select <b>Family</b> tab.</li> <li>3. Specify the Family and Inet parameters.</li> <li>4. Expand the <b>Inet</b> tree and set up the parameters.</li> </ol>
Authentication Settings	Enables you to specify the authentication settings for BGP.	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree.</li> <li>2. Select <b>BGP</b> and select <b>Authentication Settings</b> tab.</li> <li>3. Specify the authentication key, algorithm and key chain.</li> </ol>
Export	Enables you to apply one or more routing policies to routes being exported from the JUNOS routing table from BGP .	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree.</li> <li>2. Select <b>BGP</b> and select <b>Export</b> tab.</li> <li>3. Specify the export policies configured on the peer.</li> </ol>
Local As	Enables you to configure BGP with a different local autonomous session (AS) number for each BGP session	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree.</li> <li>2. Select <b>BGP</b> and select <b>Local As</b> tab.</li> <li>3. Enter the comment, as number, loop and specify whether it is private.</li> </ol>
Graceful Restart	Enables you to specify the graceful restart parameters.	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree.</li> <li>2. Select <b>BGP</b> and select <b>Graceful Restart</b> tab.</li> <li>3. Specify the graceful restart parameters.</li> </ol>

**Table 56: BGP Configuration Fields** (continued)

Field	Function	Your Action
Bfd Liveness Detection	Enables you to configure bidirectional forwarding detection (BFD) timers.	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree.</li> <li>2. Select <b>BGP</b> and select <b>Bfd Liveness Detection</b> tab.</li> <li>3. Specify the Bfd Liveness Detection parameters, Detection Time and Transmit Interval.</li> </ol>
Group	Enables you to configure BGP group.	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree.</li> <li>2. Select <b>BGP</b> and select <b>Group</b> tab.</li> <li>3. Click the <b>New</b> button or select a group and click <b>Edit</b> button.</li> <li>4. Enter all the group parameters.</li> </ol>

## Configuring 802.1X Authentication (NSM Procedure)

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

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

To configure 802.1X authentication:

- Specify 802.1X interface settings on the switch.
  - Specify the 802.1X exclusion list, used to specify which supplicants can bypass 802.1X authentication and be automatically connected to the LAN.
1. Configuring 802.1X Interface Settings on page 91
  2. Configuring Static MAC Bypass on page 93

### Configuring 802.1X Interface Settings

To configure 802.1X interface settings:

1. In the navigation tree, select **Device Manager > Devices**. In Device Manager, select the device for which you want to configure 802.1X settings.
2. In the Configuration tree, expand **Protocols > Dot1x**.
4. Select **Authenticator > Interface**.
5. Click the **Add** icon.
6. Add/modify member settings for the interface as specified in Table 57 on page 92.



**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 57: 802/1X Authentication for an Interface**

Option	Function	Your Action
Authentication Profile Name	Specifies the name for the profile.	Enter the name
Interface	Specifies the interface for which 802.1X authentication is being configured.	Select <b>Interface</b> . Click the Add icon.
Name	Specifies the interface name.	Enter the interface name.
Disable	Disables 802.1X authentication on the interface.	Select to disable authentication.
Supplicant	Specifies the mode to be adopted for supplicants: <ul style="list-style-type: none"><li>■ Single — allows only one host for authentication.</li><li>■ Multiple — allows multiple hosts for authentication. Each host is checked before being admitted to the network.</li><li>■ Single authentication for multiple hosts — Allows multiple hosts but only the first is authenticated.</li></ul>	Select the required mode.
Retries	Maximum number of retries	Select a value from the list.
Quiet Period	Specifies the port waiting time after an authentication failure.	Select a value from the list.
Transmit Period	Specifies the retransmit interval.	Select a value from the list.
Supplicant Timeout	Port timeout value for the response from the supplicant.	Select a value from the list.
Server Timeout	Port timeout value for the response from the RADIUS server	Select a value from the list.
Maximum Requests	Specifies the maximum number of authentication requests to be made to the server.	Select a value from the list.
Guest Vlan	Specifies the guest VLAN to move the interface to in case of an authentication failure.	Enter the VLAN name.
Reauthentication	Specifies enabling reauthentication on the selected interface.	Select <b>Reauthentication</b> .  Select one: <ul style="list-style-type: none"><li>■ none</li><li>■ reauthentication</li><li>■ no-reauthentication</li></ul>

## Configuring Static MAC Bypass

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

To configure the 802.1X exclusion:

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



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

---

## Configuring GVRP (NSM Procedure)

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

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

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

To configure GVRP:

1. In the navigation tree, select **Device Manager > Devices**. In Device Manager, select the device.
2. In the configuration tree, expand **Protocols**.
3. Select **GVRP**.
4. Click the Add icon.
5. Add/modify GVRP settings for the interface as specified in Table 58 on page 94.



**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 58: GVRP Configuration Fields**

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

## Configuring IGMP (NSM Procedure)

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

To configure IGMP in NSM:

1. In the navigation tree select **Device Manager > Devices** .
2. In the **Devices** list, double click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Protocols** and select **IGMP**.
5. Add/Modify the parameters as specified in Table 59 on page 95.
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 59: IGMP Configuration Fields**

Option	Function	Your Action
<b>IGMP</b>		
Comment	Specifies the comment for IGMP.	Enter a comment.
Query Interval	Defines how often the device sends general host-query messages.	Select the query interval.
Query Response Interval	Defines how long the query router/switch waits to receive a response to a host-query message from a host.	Enter the query response interval.
Query Last Member Interval	Defines how often the device sends group-specific query messages.	Enter the query last member interval.
Robust Count	Defines the number of intervals the device waits before removing a multicast group from the multicast forwarding table.	Select the robust count.
Accounting	Specifies whether accounting is enabled for IGMP.	Select to enable accounting.
Interfaces	Specifies the interface and the multicast group that has to be associated with IGMP.	<ol style="list-style-type: none"> <li>1. Expand the IGMP tree and select <b>Interfaces</b>.</li> <li>2. Click the New button or select an interface and click Edit button.</li> <li>3. Select <b>Disable</b> to disable IGMP on the interface.</li> <li>4. Select the version.</li> <li>5. Specify the <b>Ssm Map</b>.</li> <li>6. You can enable <b>Immediate Leave</b> and <b>Promiscuous Mode</b>.</li> <li>7. You can enable accounting on the interface.</li> <li>8. Select the option <b>Interface &gt; Static</b> to configure the multicast group to be associated with the interface.</li> </ol>

**Table 59: IGMP Configuration Fields** (continued)

Option	Function	Your Action
Traceoptions	Defines trace options for IGMP .	<ol style="list-style-type: none"><li>1. Expand <b>IGMP</b> tree and select <b>Traceoptions</b>.</li><li>2. Enter a comment for traceoptions.</li><li>3. Expand the <b>Traceoptions</b> tree, select <b>File</b> and set up the file parameters.</li><li>4. In the <b>Traceoptions</b> tree select <b>Flag</b> and set up or edit the file parameters.</li></ol>

## Configuring IGMP Snooping on EX-series Switches (NSM Procedure)

IGMP snooping regulates multicast traffic in a network. With IGMP snooping enabled, a LAN switch monitors the IGMP transmissions between a host (a network device) and a multicast router, keeping track of the multicast groups and associated member ports. The switch uses that information to make intelligent multicast-forwarding decisions and forward traffic to the intended destination interfaces.

You can configure IGMP snooping on one or more VLANs to allow the switch to examine IGMP packets and make forwarding decisions based on packet content. By default, IGMP snooping is disabled on a device.



**NOTE:** When IGMP snooping is enabled on a VLAN, traffic for a given group is flooded to all member ports until IGMP snooping discovers at least one member of the group in the given VLAN.

To enable IGMP snooping and configure individual options:

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**.
3. Select **IGMP Snooping > Vlan**.
4. Click the Add icon.
5. Add/modify member settings for the interface as specified in Table 60 on page 97.



**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 60: IGMP Snooping Configuration Fields**

Option	Function	Your Action
Name	Specifies the VLAN for which IGMP snooping is being enabled.	Click <b>Add</b> and select Port or VLAN. Next, select the interfaces or VLANs.
Query Interval	Specifies the query interval on the VLAN.	Select a value.
Query Last Member Interval	Specifies the last member query interval on the VLAN.	Select a value.
Query Response Interval	Specifies the query response interval on the VLAN.	Select a value.
Robust Count	Specifies the number of timeout intervals the switch waits before timing out a multicast group.	Select a value.
Immediate Leave	Immediately removes a multicast group membership from an interface when it receives a leave message from that interface and suppress the sending of any group-specific queries for the multicast group	Select the option to enable it.
Interface	Statically configure an interface as a switching interface toward a multicast router (the interface to receive multicast traffic).	<ol style="list-style-type: none"> <li>1. Select the VLAN.</li> <li>2. Select the option <b>Multicast Router Interface</b>.</li> <li>3. Select <b>Static &gt; Group</b>.</li> <li>4. Specify the group name to configure IGMP group membership on a port.</li> </ol>

## Configuring LLDP (NSM Procedure)

EX-series switches use Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) to learn and distribute device information on network links. The information allows the switch to quickly identify a variety of devices, resulting in a LAN that interoperates smoothly and efficiently.

To configure LLDP:

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 > LLDP**.
3. Add/modify LLDP settings as specified in Table 61 on page 98.



**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 61: LLDP Configuration Fields**

Option	Function	Your Action
Disable	Specifies whether LLDP must be disabled on the port.	Click to select the option.
Advertisement Interval	Specifies the frequency of outbound LLDP advertisements. You can increase or decrease this interval.	Select a value.
Transmit Delay	Specifies a delay-interval setting that the switch uses to delay transmitting successive advertisements. You can increase this interval to reduce the frequency of successive advertisements.	Select a value.
Hold Multiplier	Specifies the multiplier factor to be used by an LLDP-enabled switch to calculate the time-to-live (TTL) value for the LLDP advertisements it generates and transmits to LLDP neighbors.	Select a value.
Ptopo Configuration Trap Interval	Specifies the transmission of ptopo notifications..	Select a value.
Ptopo Configuration Maximum Hold Time	Specifies the desired time interval an agent maintains dynamic ptopo connection entries.	Select a value.
Interface	Specifies LLDP settings for the interface.	<ol style="list-style-type: none"><li>1. Select the interface.</li><li>2. Select the option <b>Multicast Router Interface</b>.</li><li>3. Select <b>Disable</b> if LLDP settings must be disabled on a specific interface.</li></ol>

## Configuring LLDP-MED (NSM Procedure)

Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) is an extension of LLDP. An EX-series switch uses LLDP-MED to support device discovery of VoIP telephones and to create location databases for these telephone locations for emergency services. The location information configured is used during emergency calls to identify the location of the LLDP-MED device.

To configure LLDP-MED:

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 > LLDP-MED**.
3. Add/modify LLDP—MED settings as specified in Table 62 on page 99.



**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 62: LLDP—MED Configuration Fields**

Option	Function	Your Action
Disable	Specifies whether LLDP must be disabled on the port.	Click to select the option.
Fast Start	Specifies the frequency at which LLDP-MED advertisements are sent from the switch in the first second after it has detected an LLDP-MED device.	Select a value.
Interface	Specifies LLDP—MED settings for the interface.	<ol style="list-style-type: none"> <li>1. Select the interface.</li> <li>2. Select <b>Disable</b> if LLDP—MED settings must be disabled on a specific interface.</li> </ol>

## Configuring MSTP (NSM Procedure)

Multiple Spanning Tree Protocol (MSTP) is used to create a loop-free topology in networks using multiple spanning tree regions, each region containing multiple spanning-tree instances (MSTIs). MSTIs provide different paths for different VLANs. This functionality facilitates better load sharing across redundant links.

MSTP supports up to 64 regions, each one capable of supporting 4094 MSTIs.

To configure MSTP:

1. In the navigation tree, select **Device Manager > Devices**. In Device Manager, select the device for which you want to configure a port mirror analyzer.
2. In the Configuration tree, expand **Protocols > MSTP**.
3. Add/modify MSTP settings as specified in Table 63 on page 100.



**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 63: MSTP Configuration Fields**

Option	Function	Your Action
Disable	Specifies whether MSTP must be disabled on the port.	Click to select the option.
Configuration Name	Specifies the configuration name.	Type a name.
Revision Level	Specifies the configuration revision level.	Select a value.
Max Hops	Specifies the number of hops in a region before the BPDU is discarded.	Select a value.
Max Age	Specifies the maximum-aging time for all MST instances. The maximum aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.	Select a value.
Hello time	Specifies the hello time for all MST instances.	Select a value.
Forward Delay	Specifies the number of seconds a port waits before changing from its spanning-tree learning and listening states to the forwarding state.	Select a value.
Bridge Priority	Specifies the bridge priority.	Enter a value.
Bpdu Block on Edge	Specifies whether Bpdu blocks must be processed.	Select to enable the feature.

**Table 63: MSTP Configuration Fields** (continued)

Option	Function	Your Action
Interface	Specifies MSTP settings for the interface.	<ol style="list-style-type: none"> <li>1. Click the expand icon.</li> <li>2. Specify the interface name.</li> <li>3. Specify the port priority.</li> <li>4. Specify the path cost. MSTP uses the path cost when selecting an interface to place into the forwarding state. A lower path cost represents higher-speed transmission.</li> <li>5. Specify the mode. The link type can be shared or point-to-point.</li> <li>6. Select <b>Edge</b> to enable the feature.</li> <li>7. Select <b>No root port</b> if it is not specified.</li> <li>8. Click <b>OK</b>.</li> <li>9. Specify the <b>Bpdu timeout action</b>: <ul style="list-style-type: none"> <li>■ Block</li> <li>■ Alarm</li> </ul> </li> </ol>
Msti	Specifies MST instances settings for an interface or VLAN.	<ol style="list-style-type: none"> <li>1. Specify the Msti ID.</li> <li>2. Enter a comment.</li> <li>3. Specify the bridge priority.</li> <li>4. Click <b>OK</b>.</li> </ol>

## 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 64 on page 102.
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 64: OSPF Configuration Fields**

Option	Function	Your Action
OSPF		

**Table 64: OSPF Configuration Fields** (continued)

Option	Function	Your Action
Comment	Specifies the comment for OSPF.	1. Enter the comment.
Disable	Specifies whether to disable the OSPF configuration.	1. Specify whether to enable or disable OSPF. <ul style="list-style-type: none"> <li>■ To enable OSPF, clear the check box.</li> <li>■ To disable OSPF, select the check box.</li> </ul>
Prefix Export Limit	Configure a limit to the number of prefixes to be exported.	1. Enter the prefix export limit or select from the list.
Rib Group	Specifies the routing table group.	1. Select rib group from the list.
Route Type Community	Specifies an extended community value to encode the OSPF route type	1. Select route type community from the list.
Domain VPN Tag	Virtual private network (VPN) tag for OSPFv2 external routes generated by the provider edge (PE) router.	1. Enter the domain VPN tag or select from the list.
Preference	Specifies the route preference for OSPF internal routes.	1. Enter the preference or select from the list.
External Preference	Specifies the external route preference.	1. Enter the external route preference or select from the list.
Reference Bandwidth	Specifies the reference bandwidth used in calculating the default interface cost.	1. Enter the reference bandwidth.
No RFC 1583	Disable compatibility with RFC 1583. Disabling compatibility with RFC 1583 can prevent routing loops.	1. Specify whether to configure RFC 1583. <ul style="list-style-type: none"> <li>■ To enable compatibility with RFC 1583, clear the check box.</li> <li>■ To disable compatibility with RFC 1583, select the check box.</li> </ul>
No NSSA ABR	Disable compatibility with NSSA ABR.	1. Specify whether NSSA ABR has to be configured. <ul style="list-style-type: none"> <li>■ To enable NSSA ABR, clear the check box.</li> <li>■ To disable NSSA ABR, select the check the check box.</li> </ul>
Area	Enables you to set up the area details for OSPF.	

**Table 64: OSPF Configuration Fields** (continued)

Option	Function	Your Action
		<ol style="list-style-type: none"> <li>1. Expand the OSPF tree and select <b>Area</b>.</li> <li>2. Set up the area range, interface, sham link remote, stub and virtual link.</li> </ol>
Domain ID	Enables you to configure domain ID for the OSPF.	<ol style="list-style-type: none"> <li>1. Expand the OSPF tree and select <b>Domain ID</b>.</li> <li>2. Specify the domain ID.</li> </ol>
Export	Enables you to specify the export policies to be configured on the peer.	<ol style="list-style-type: none"> <li>1. Expand the OSPF tree and select <b>Export</b>.</li> <li>2. Specify the export policies.</li> </ol>
Graceful Restart	Enables you to specify the graceful restart parameters for OSPF.	<ol style="list-style-type: none"> <li>1. Expand the OSPF tree and select <b>Graceful Restart</b>.</li> <li>2. Set up the graceful restart parameters.</li> </ol>
Import	Enables you to specify the import policies to be configured on the peer.	<ol style="list-style-type: none"> <li>1. Expand the OSPF tree and select <b>Import</b>.</li> <li>2. Specify the import policies.</li> </ol>
Overload	Enables you to configure the local router so that it appears to be overloaded. You might do this when you want the router to participate in OSPF routing, but do not want it to be used for transit traffic.	<ol style="list-style-type: none"> <li>1. Expand the OSPF tree and select <b>Overload</b>.</li> <li>2. Specify the comment and timeout.</li> </ol>
Sham Link	Enables you to configure the local endpoint of a sham link.	<ol style="list-style-type: none"> <li>1. Expand the OSPF tree and select <b>Sham Link</b>.</li> <li>2. Enable the feature and specify the comment and local address.</li> </ol>
SPF Options	Enables you to configure options for running the shortest-path-first (SPF) algorithm. You can configure a delay for when to run the SPF algorithm after a network topology change is detected, the maximum number of times the SPF algorithm can run in succession, and a holddown interval after the SPF algorithm runs the maximum number of times.	<ol style="list-style-type: none"> <li>1. Expand the OSPF tree and select <b>SPF Options</b>.</li> <li>2. Specify the comment, delay, holddown and rapid runs.</li> </ol>

**Table 64: OSPF Configuration Fields** (continued)

Option	Function	Your Action
Traceoptions	Enables you to configure OSPF protocol level tracing options.	<ol style="list-style-type: none"> <li>1. Expand the OSPF tree and select Traceoptions.</li> <li>2. Expand the Traceoptions tree and set up the file and flag parameters.</li> </ol>

## 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 65 on page 106.
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 65: RIP Configuration Fields**

Option	Function	Your Action
RIP		
Comment	Specifies the comment for RIP.	1. Enter the comment.
Metric In	Specifies the metric to add to incoming routes when advertising into RIP routes that were learned from other protocols.	1. Specify the metric to add incoming routes.
Message Size	Specifies the number of route entries to be included in every RIP update message.	1. Enter the message size or select from the list.
Hold Down	Time period the expired route is retained in the routing table before being removed.	1. Enter the hold down value or select from the list.
Route Timeout	Specifies the route timeout interval for RIP.	1. Enter the route timeout or select from the list.
Update Interval	Enables you to configure an update time interval to periodically send out routes learned by RIP to neighbors.	1. Enter the update interval or select from the list.
Authentication Type	The type of authentication for RIP route queries received on an interface.	1. Select authentication type from the list.
Authentication Key	Authentication key for RIP route queries received on an interface.	1. Enter the authentication key.
Graceful Restart	Enables you to specify the graceful restart parameters for RIP.	1. Expand the <b>RIP</b> tree and select <b>Graceful Restart</b> . 2. Enable the feature and set up the graceful restart parameters.
Group	RIP neighbors that share an export policy and metric. The export policy and metric govern what routes to advertise to neighbors in a given group.	1. Expand the <b>RIP</b> tree and select <b>Group</b> . 2. Click the <b>New</b> button or select a group and click <b>Edit</b> button. 3. Set up the <b>Bfd Liveness Detection</b> , <b>Export</b> , <b>Import</b> and <b>Neighbor</b> for <b>RIP</b> .
Import	Enables you to specify the import policies to be configured on the peer.	1. Expand the <b>RIP</b> tree and select <b>Import</b> . 2. Specify the import policies.
Receive	Enables you to configure RIP receive options.	1. Expand the <b>RIP</b> tree and select <b>Receive</b> . 2. Specify the receive options.

**Table 65: RIP Configuration Fields** (continued)

Option	Function	Your Action
RIB Group	The routing table group.	<ol style="list-style-type: none"> <li>1. Expand the RIP tree and select Rib Group.</li> <li>2. Specify the comment and ribgroup name.</li> </ol>
Send	Enables you to configure RIP send options.	<ol style="list-style-type: none"> <li>1. Expand the RIP tree and select Send.</li> <li>2. Specify the send options.</li> </ol>
Traceoptions	Enables you to configure RIP protocol level tracing options.	<ol style="list-style-type: none"> <li>1. Expand the RIP tree and select Traceoptions.</li> <li>2. Expand the Traceoptions tree and set up the file and flag parameters.</li> </ol>

## Configuring RSTP on EX-series Switches (NSM Procedure)

EX-series switches use Rapid Spanning Tree Protocol (RSTP) to provide a loop-free topology. RSTP identifies certain links as point to point. When a point-to-point link fails, the alternate link can transition to the forwarding state. RSTP provides better reconvergence time than original STP because it uses protocol handshake messages rather than fixed timeouts. Eliminating the need to wait for timers to expire makes RSTP more efficient than STP.

To configure RSTP:

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 > RSTP**.
3. Add/modify RSTP settings as specified in Table 66 on page 107.



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

**Table 66: RSTP Configuration Fields**

Field	Function	Your Action
Disable	Specifies whether RSTP must be disabled on the port.	Click to select the option.
Bridge Priority	Specifies the bridge priority.	Enter a value.

**Table 66: RSTP Configuration Fields** (continued)

Field	Function	Your Action
Max Age	Specifies the maximum-aging time for all MST instances. The maximum aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.	Select a value.
Hello time	Specifies the hello time for all MST instances.	Select a value.
Forward Delay	Specifies the number of seconds a port waits before changing from its spanning-tree learning and listening states to the forwarding state.	Select a value.
Bpdu Block on Edge	Specifies whether Bpdu blocks must be processed.	Select to enable the feature.
Interface	Specifies MSTP settings for the interface and Bpdu timeout action.	<ol style="list-style-type: none"> <li>1. Click the expand icon.</li> <li>2. Specify the interface name.</li> <li>3. Specify the port priority.</li> <li>4. Specify the path cost. MSTP uses the path cost when selecting an interface to place into the forwarding state. A lower path cost represents higher-speed transmission.</li> <li>5. Specify the mode. The link type can be shared or point-to-point.</li> <li>6. Select <b>Edge</b> to enable the feature.</li> <li>7. Select <b>No root port</b> if it is not specified.</li> <li>8. Click <b>OK</b>.</li> <li>9. Specify the <b>Bpdu timeout action</b>: <ul style="list-style-type: none"> <li>■ Block</li> <li>■ Alarm</li> </ul> </li> </ol>

## Configuring STP (NSM Procedure)

Devices such as EX-series switches provide Layer 2 loop prevention through Spanning Tree Protocol (STP), Rapid Spanning Tree protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP). Configure BPDU protection on interfaces to prevent them from receiving BPDUs that could result in STP misconfigurations, which could lead to network outages.

To configure STP:

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 > STP**.
3. Add/modify STP settings as specified in Table 67 on page 109.



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

**Table 67: STP Configuration Fields**

Option	Function	Your Action
Disable	Specifies whether RSTP must be disabled on the port.	Click to select the option.
Bridge Priority	Specifies the bridge priority.	Enter a value.
Max Age	Specifies the maximum-aging time for all MST instances. The maximum aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.	Select a value.
Hello time	Specifies the hello time for all MST instances.	Select a value.
Forward Delay	Specifies the number of seconds a port waits before changing from its spanning-tree learning and listening states to the forwarding state.	Select a value.
Bpdu Block on Edge	Specifies whether Bpdu blocks must be processed.	Select to enable the feature.

**Table 67: STP Configuration Fields** (continued)

Option	Function	Your Action
Interface	Specifies MSTP settings for the interface and Bpdu timeout action.	<ol style="list-style-type: none"><li>1. Click the expand icon.</li><li>2. Specify the interface name.</li><li>3. Specify the port priority.</li><li>4. Specify the path cost. MSTP uses the path cost when selecting an interface to place into the forwarding state. A lower path cost represents higher-speed transmission.</li><li>5. Specify the mode. The link type can be shared or point-to-point.</li><li>6. Select <b>Edge</b> to enable the feature.</li><li>7. Select <b>No root port</b> if it is not specified.</li><li>8. Click <b>OK</b>.</li><li>9. Specify the <b>Bpdu timeout action</b>:<ul style="list-style-type: none"><li>■ Block</li><li>■ Alarm</li></ul></li></ol>

## 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 68 on page 111.
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 68: VSTP Configuration Fields**

Field	Function	Your Action
VSTP		
Comment	Specifies comment for OSPF.	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree and select <b>VSTP</b>.</li> <li>2. Enter the comment.</li> </ol>
Disable	Specifies whether to disable the VSTP configuration.	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree and select <b>VSTP</b>.</li> <li>2. Specify whether to disable VSTP.</li> </ol>
Bridge Priority	The bridge priority determines which bridge is elected as the root bridge. If two bridges have the same path cost to the root bridge, the bridge priority determines which bridge becomes the designated bridge for a LAN segment.	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree and select <b>VSTP</b>.</li> <li>2. Enter the bridge priority.</li> </ol>
Max Age	Specifies the maximum age of received protocol BPDUs.	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree and select <b>VSTP</b>.</li> <li>2. Enter the max age or select from the list.</li> </ol>
Hello Time	The time interval at which the root bridge transmits configuration BPDUs.	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree and select <b>VSTP</b>.</li> <li>2. Enter the hello time or select from the list.</li> </ol>
Forward Delay	Specifies how long a bridge interface remains in the listening and learning states before transitioning to the forwarding state.	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree and select <b>VSTP</b>.</li> <li>2. Enter the forward delay time or select from the list.</li> </ol>
Interface	Specifies the interface to be associated with VSTP.	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree.</li> <li>2. Select <b>VSTP</b> and expand the tree.</li> <li>3. Select <b>Interfaces</b>.</li> <li>4. Set up the priority, cost, mode, edge and specify whether the interface has to be disabled.</li> </ol>

**Table 68: VSTP Configuration Fields** (continued)

Field	Function	Your Action
Traceoptions	Enables you to configure VSTP level tracing options.	<ol style="list-style-type: none"><li>1. Expand the Protocol tree.</li><li>2. Select VSTP and expand the tree.</li><li>3. Select Traceoptions.</li><li>4. Set up the file and flag parameters.</li></ol>

### 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 69 on page 112.
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 69: VRRP Configuration Fields**

Field	Function	Your Action
VRRP		

**Table 69: VRRP Configuration Fields** (continued)

Field	Function	Your Action
Comment	Specifies comment for VRRP.	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree and select <b>VRRP</b>.</li> <li>2. Enter the comment.</li> </ol>
Startup Silent Period	Enables the system to ignore the Master Down Event when an interface transitions from the disabled state to the enabled state. It avoids an incorrect error alarm caused by delay or interruption of incoming VRRP advertisement packets during the interface startup phase.	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree and select <b>VRRP</b>.</li> <li>2. Enter the startup silent period or select from the list</li> </ol>
Traceoptions	Enables you to configure VRRP level tracing options.	<ol style="list-style-type: none"> <li>1. Expand the <b>Protocol</b> tree.</li> <li>2. Select <b>VRRP</b> and expand the tree.</li> <li>3. Select <b>Traceoptions</b>.</li> <li>4. Set up the file and flag parameters.</li> </ol>



## Chapter 9

# Configuring PoE

This section contains the following:

- Configuring Power over Ethernet (NSM Procedure) on page 115

### Configuring Power over Ethernet (NSM Procedure)

---

EX-series switch models provide either 8, 24, or 48 PoE ports, which supply electric power over the same ports that are used to connect network devices. These ports allow you to plug in devices that require both network connectivity and electric power, such as VoIP phones, WAPs, and some IP cameras.

The factory default configuration for EX-series switches specifies and enables PoE interfaces for the PoE ports.

To configure PoE:

1. In the navigation tree, select **Device Manager > Devices**. In Device Manager, select the device for which you want to configure PoE.
2. In the configuration tree, select **PoE**
3. Enter a value to set the guard band value. The default value is 0. Guard band Specifies the band to control power availability on the switch.
4. To add/modify PoE interface details, click **Add New Entry** and select **Interface**.
5. In the Interface screen, click the add or edit icon.
6. Add/modify PoE settings for the interface as specified in Table 70 on page 115
7. Click one:
  - OK—To save the changes.
  - Cancel—To cancel the modifications.

**Table 70: PoE Edit Settings**

Option	Description	Your Action
Name	Specifies the name for the interface.	Enter a name.
Disable	Specifies that PoE is enabled on the interface.	Select this option to disable PoE on the interface.

**Table 70: PoE Edit Settings** (continued)

Option	Description	Your Action
Priority	Lists the power priority (Low or High) configured on ports enabled for PoE.	Set the priority as <b>High</b> or <b>Low</b> .
Maximum Power	Specifies the maximum PoE wattage available to provision active PoE ports on the switch.	Select a value in watts. If no value is specified, the default is 15.4.
Telemetries	Enable logging of PoE power consumption with the default telemetries settings.	Select this option to log telemetries. Specify the following: <ul style="list-style-type: none"><li>■ Disable—Select to disable logging of telemetries.</li><li>■ Interval—The time interval for logging telemetries</li><li>■ Duration—The duration for which telemtries should be logged.</li></ul>

## Chapter 10

# Configuring SNMP

This section contains the following:

- Configuring Basic System Identification for SNMP (NSM Procedure) on page 117
- Configuring SNMP Views (NSM Procedure) on page 118
- Configuring SNMP Communities (NSM Procedure) on page 119
- Configuring SNMP Trap Groups (NSM Procedure) on page 121

### 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 71 on page 117.
5. Click one:
  - **OK**—Saves the changes.
  - **Cancel**—Cancels the modifications.

**Table 71: Basic System Identification Details**

Option	Function	Your Action
System Name	Specifies a system name for the device.	Enter the system name as a free-form text string.
Description	Provides a description for the system.	Enter a description for the system. For example, type <b>J4350 with 4 PIMs</b> .
Location	Specifies the system location information.	Enter the system location information (such as a lab name and a rack name).
Contact	Specifies the contact information for the system.	Enter the system contact information (such as a name and a phone number).

**Table 71: Basic System Identification Details** (continued)

Option	Function	Your Action
<b>Snmp &gt; Engine Id</b>		
Use Mac Address	Sets the engine ID to use the MAC address.	Select this option.

- Related Topics**
- Configuring SNMP Agents and Communities (NSM Procedure)
  - Configuring SNMP Trap Groups (NSM Procedure) on page 121
  - Configuring SNMP Views (NSM Procedure) on page 118

## 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 72 on page 119.
8. Click one:
  - **OK**—To save the changes.
  - **Cancel**—To cancel the modifications.
  - **Apply**—To apply the SNMP settings.

**Table 72: Configuring SNMP View Fields**

Option	Function	Your Action
Name	Specifies a name for the view.	Enter a name for the view.
Oid	Specifies an OID used to represent a subtree of MIB objects.	<ol style="list-style-type: none"> <li>Expand the <b>View</b> tree and select oid.</li> <li>Click the <b>New</b> button or select an OID and click the <b>Edit</b> button.</li> </ol>
Name	Specifies the MIB for the view.	Enter the OID of the MIB in either dotted-integer format or subtree-name format.
Include or Exclude	Specifies whether the view includes or excludes the MIB	<p>Select <b>exclude</b> to exclude the subtree of MIB objects represented by the specified OID.</p> <p>Select <b>include</b> to include the subtree of MIB objects represented by the specified OID.</p>

- Related Topics**
- Configuring Basic System Identification for SNMP (NSM Procedure) on page 117
  - Configuring SNMP Agents and Communities (NSM Procedure)
  - Configuring SNMP Trap Groups (NSM Procedure) on page 121

## 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:

- In the navigation tree, select **Device Manager > Devices**.
- In the **Devices** list, double-click the device to select it.
- Click the **Configuration** tab.
- In the configuration tree, expand **SNMP**.
- Select **Community**.
- Click the **Add** or **Edit** icon.
- Enter the parameters as specified in Table 73 on page 120.
- 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 73: Configuring Community Fields**

Option	Function	Your Action
Name	Specifies the name of the community.	Enter a name for the community.
Comment	Specifies the comment for the community.	Enter a comment.
View	Specifies the view associated with the community.	Enter a name for the view.
Authorization	Specifies the type of access granted to the community. Access is authorized for SNMP Get, GetBulk, GetNext, and Set requests.	Select an access type for the community: <ul style="list-style-type: none"> <li>■ None—No requests are enabled.</li> <li>■ read-only—Enable Get, GetNext, and GetBulk requests. This option is enabled by default.</li> <li>■ read-write—Enable all requests, including Set requests.</li> </ul> You must configure a view to enable Set requests.
Client List Name	Specifies a client list or prefix list to be assigned to an SNMP community.	<ol style="list-style-type: none"> <li>1. Expand the <b>Community</b> tree and select <b>Client List Name</b>.</li> <li>2. Select a name.</li> </ol>

**Table 73: Configuring Community Fields** (continued)

Option	Function	Your Action
Routing Instance	Specifies a routing instance for a community.	<ol style="list-style-type: none"> <li>1. Expand the <b>Community</b> tree and select <b>Routing Instance</b>.</li> <li>2. Click the <b>New</b> button or select an entry and click the <b>Edit</b> button.</li> <li>3. Configure the following to create and define a routing instance: <ul style="list-style-type: none"> <li>■ <b>Name</b>—Enter a name for the routing instance.</li> </ul> <p><b>NOTE:</b> On routers, to configure a routing instance within a logical system, specify the logical system name followed by the routing instance name. Use a slash ( / ) to separate the two names. To configure the default routing instance on a logical system, specify the logical system name followed by "default."</p> <ul style="list-style-type: none"> <li>■ <b>Comment</b>—Enter a comment for the routing instance.</li> </ul> </li> </ol>

**Related Topics** ■ Adding a Group of Clients to an SNMP Community

## 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 74 on page 122.
8. Click one:
  - **OK**—To save the changes.
  - **Cancel**—To cancel the modifications.
  - **Apply**—To apply the SNMP settings.

**Table 74: Configuring SNMP Trap Group Fields**

Option	Function	Your Action
Name	Specifies a name for the trap group.	Enter a name for the trap group.
Version	Specifies the version number of the SNMP trap group.	Select the version number for the SNMP trap group from the list.
Destination Port	Specifies the SNMP trap group port number.	Enter a trap group port number.
Routing Instance	Specifies a routing instance for trap targets.	Enter the name of the routing instance.
Categories	Defines the types of traps that are sent to the targets of the named trap group.	<ol style="list-style-type: none"> <li>1. Expand the <b>trap-group</b> tree and select <b>Categories</b>.</li> <li>2. Select the trap type.</li> </ol> <p><b>NOTE:</b> If you do not configure categories, all trap types are included in trap notifications.</p> <ol style="list-style-type: none"> <li>3. On routers, choose an Otn Alarm and a Sonet Alarm for your trap category.</li> </ol>
Targets	Specifies the IPv4 or IPv6 address of the systems to receive traps.	<ol style="list-style-type: none"> <li>1. Expand the <b>trap-group</b> tree and select <b>Targets</b>.</li> <li>2. Click the New button or select an OID and click the Edit button.</li> <li>3. Enter the IPv4 or IPv6 addresses of the system (do not enter hostnames).</li> </ol>

- Related Topics**
- Configuring Basic System Identification for SNMP (NSM Procedure) on page 117
  - Configuring SNMP Agents and Communities (NSM Procedure)
  - Configuring SNMP Views (NSM Procedure) on page 118

## Chapter 11

# Configuring Virtual LANs

This section contains the following:

- Configuring VLANs (NSM Procedure) on page 123

### Configuring VLANs (NSM Procedure)

---

EX-series switches use bridging and virtual LANs (VLANs) to connect network devices in a LAN—desktop computers, IP telephones, printers, file servers, wireless access points, and others—and to segment the LAN into smaller bridging domains.

To configure a VLAN:

1. In the navigation tree, select **Device Manager > Devices**. In Device Manager, select the device for which you want to configure VLANs.
2. In the Configuration tree, expand Vlan.
3. Select **Vlan**.
4. In the VLAN screen, click the add or edit icon.
5. Add/modify VLAN settings as specified in Table 75 on page 123
6. Click one:
  - OK—To save the changes.
  - Cancel—To cancel 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 for more information.

---

**Table 75: VLAN Edit Settings**

Option	Description	Your Action
Vlan Name	Specifies a unique name for the VLAN.	Enter a name.
Description	Describes the VLAN.	Enter a brief description for the VLAN.

**Table 75: VLAN Edit Settings** (continued)

Option	Description	Your Action
Vlan ID	The identifier for the VLAN.	Type a unique identification number from 1 through 4094. If no value is specified, it defaults to 0.
L3 Interface	Specifies the Layer 3 interface on trunk ports to allow the interface to transfer traffic between multiple VLANs.	Type the L3 interface.
Mac Limit	Specifies the MAC address limit.	Select a value from the list.
Mac Table Aging Time	Specifies the maximum time that an entry can remain in the forwarding table before it 'ages out'.	Type the number of seconds from 60 through 1000000.
Filter	Specifies the VLAN firewall filter that is applied to incoming and outgoing packets.	To specify an input and output filter: <ol style="list-style-type: none"><li>1. Click <b>Filter</b>.</li><li>2. Specify the filter to be used for incoming and outgoing packets.</li></ol>
Interface	Specifies the interface to be added to the VLAN.	To add an interface, click <b>Interface</b> . Specify the interface to be included as part of the VLAN.

## Chapter 12

# Configuring a Virtual Chassis

This section contains the following:

- Configuring a Virtual Chassis on page 125

## Configuring a Virtual Chassis

---

To take advantage of the scalability features of EX-4200 switches, you can configure a virtual chassis that includes up to 10 member switches. You can interconnect the member switches using the dedicated virtual chassis ports (VCPs) on the back of the switch. You do not have to configure the interface for the dedicated VCPs.

A virtual chassis can be configured with either:

- preprovisioned configuration—Allows you to deterministically control the member ID and role assigned to a member switch by tying it to its serial number.
  - nonprovisioned configuration—The master sequentially assigns a member ID to other member switches. The role is determined by the mastership priority value and other factors in the master election algorithm.
1. Configuring a Virtual Chassis with a Preprovisioned Configuration File on page 125
  2. Add a Member to a Virtual Chassis on page 126

### Configuring a Virtual Chassis with a Preprovisioned Configuration File

To configure a virtual chassis using a preprovisioned configuration:

1. Make a list of the serial numbers of all the switches to be connected as a virtual chassis.
2. Note the desired role (**routing-engine** or **linecard**) of each switch. If you configure the member with a **routing-engine** role, it is eligible to function as a master or backup. If you configure the member with a **linecard** role, it is not eligible to become a master or backup.
3. Interconnect the member switches using the dedicated VCPs on the rear panel of switches. See *Connecting a Virtual Chassis Cable to an EX4200 Switch*.



**NOTE:** Arrange the switches in sequence, either from top to bottom or from bottom to top (0–9).

---

4. Power on only the switch that you plan to use as the master switch (SWA-0). Do not power on the other switches at this time.
5. Run the EZ Setup program on SWA-0, specifying the identification parameters. See *Connecting and Configuring an EX Series Switch (CLI Procedure)* for details.



**NOTE:** The properties that you specify for SWA-0 apply to the entire virtual chassis, including all the member listed in the preprovisioned configuration file.

---

6. Specify all the members that you want to included in the virtual chassis, listing each switch's serial number with the desired member ID and the desired role:
7. Power on the member switches.



**NOTE:** You cannot modify the mastership-priority when you are using a preprovisioned configuration. The mastership priority values are generated automatically and controlled by the role that is assigned to the member switch in the configuration file. The two routing engines are assigned the same mastership priority value. However, the member that was powered on first has higher prioritization according to the master election algorithm. See *Understanding How the Master in a Virtual Chassis Configuration Is Elected*.

---

### **Add a Member to a Virtual Chassis**

To add a member switch to a virtual chassis:

1. In the navigation tree, select Device Manager > Devices. In Device Manager, select the device for which you want to add a member switch.
2. In the Configuration tree, expand Virtual Chassis.
3. Select Member.
4. Add/modify member settings for the interface as specified in Table 75 on page 123.
5. Click one:
  - OK—To save the changes.
  - Cancel—To cancel 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* for more information.

---

**Table 76: Virtual Chassis Configuration Fields**

Field	Function	Your Action
<b>Member Details</b>		
Name	Specifies the identifier for the member switch. The master switch assigns member IDs.	Select an identifier from the list. Select an ID from 0 through 9.
Mastership Priority	Specifies the mastership priority to be assigned to the member.	Select a number from 1 through 255, with 255 being the highest priority (128 is the default).
Role	Specifies the role to be assigned to the member.	Select the appropriate role.
Serial Number	Specifies the serial number of the member.	Enter the serial number.
No Management VLAN	If you want to reserve an individual member's management Ethernet port for local troubleshooting, you can remove that port from being part of the Virtual Management Ethernet (VME).	Click to disable management VLAN on the port.
Refresh	Refreshes the operational status of virtual chassis members.	Click to refresh the operational status.



## Part 2

# Index

- Index on page 131



# Index

## Symbols

802.1x authentication.....91

## A

aggregated devices, configuring.....11  
analyzer  
    Configuring.....35

## B

BGP  
    configuring.....88

## C

chassis alarms, configuring.....12  
classifiers  
    CoS.....15  
code point aliases.....17  
communities  
    configuring.....119  
confederation  
    configuring.....84  
configuring virtual chassis.....125  
configuring VLANs.....123  
CoS classifiers.....15  
CoS code point aliases.....17  
CoS drop profiles.....19  
CoS forwarding classes.....21  
CoS interfaces.....22  
CoS rewrite rules.....28  
CoS scheduler maps.....32  
CoS schedulers.....31  
customer support.....xiv  
    contacting JTAC.....xiv

## D

drop profiles.....19

## F

fate sharing  
    configuring.....79  
firewall filter  
    policer.....46  
firewall filters  
    configuring.....43  
flow  
    configuring.....77  
forwarding classes.....21  
forwarding table  
    configuring.....75

## G

generated routes  
    configuring.....73  
graceful restart  
    configuring.....74  
GVRP.....93

## I

IGMP  
    configuring.....94  
IGMP snooping.....96  
instance export  
    configuring.....83  
instance import  
    configuring.....83  
interface routes  
    configuring.....82

## L

LLDP.....97  
LLDP MED.....98

## M

martian addresses  
    configuring.....80  
maximum paths  
    configuring.....85

maximum prefixes	
configuring.....	59
MSTP.....	99
multicast	
configuring.....	61
multipath	
configuring.....	64

## O

Options	
configuring.....	65
OSPF.....	101

## P

policer	
configuring.....	46
Port Mirroring.....	35
port security	
configuring.....	37
protocols	
802.1x.....	91
BGP.....	88
GVRP.....	93
IGMP.....	94
IGMP snooping.....	96
LLDP.....	97
LLDP-MED.....	98
OSPF.....	101
protocols.....	107
RIP.....	105
STP.....	108
VRRP.....	112
VSTP.....	110
Protocols	
MSTP.....	99

## R

redundant trunk groups.....	36
resolution	
configuring.....	66
rewrite rules.....	28
rib	
configuring.....	69
rib groups	
configuring.....	67
RIP.....	105
routing engine redundancy, configuring.....	13
routing options	
confederation.....	84
fate sharing.....	79
flow.....	77
forwarding table.....	75
generated routes.....	73

graceful restart.....	74
instance export.....	83
instance import.....	83
interface routes.....	82
martian addresses.....	80
maximum paths.....	85
maximum prefixes.....	59
multicast.....	61
multipath.....	64
Options.....	65
resolution.....	66
rib.....	69
rib groups.....	67
source routing.....	71
Static Routes.....	72
RSTP.....	107

## S

scheduler maps.....	32
schedulers.....	31
secure access port.....	37
SNMP	
communities.....	119
trap groups.....	121
views.....	118
source routing	
configuring.....	71
static IP	
configuring.....	39
Static Routes	
configuring.....	72
STP.....	108
support, technical <i>See</i> technical support	

## T

technical support	
contacting JTAC.....	xiv
trap groups	
configuring.....	121

## V

views	
configuring.....	118
virtual chassis.....	125
virtual LAN.....	123
VLANs.....	123
VoIP	
configuring.....	40
VRRP.....	112
VSTP.....	110