



JUNOS® Software for EX Series Ethernet Switches, Release 10.0: Layer 3 Protocols

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, California 94089

USA

408-745-2000

www.juniper.net

Revision 1
Published: 2009-11-04

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.

JUNOS® Software for EX Series Ethernet Switches, Release 10.0: Layer 3 Protocols

Copyright © 2009, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Writing:

Editing:

Illustration:

Cover Design:

Revision History

4 November 2009—Revision 1

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

END USER LICENSE AGREEMENT

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

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer’s principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer’s principal office is located outside the Americas) (such applicable entity being referred to herein as “Juniper”), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software (“Customer”) (collectively, the “Parties”).
2. **The Software.** In this Agreement, “Software” means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. “Software” also includes updates, upgrades and new releases of such software. “Embedded Software” means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.
3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:
 - a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.
 - b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.
 - c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer’s use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer’s use of the Software shall be subject to all such limitations and purchase of all applicable licenses.
 - d. For any trial copy of the Software, Customer’s right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.
 - e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer’s enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

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

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

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.
7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.
8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. 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

About This Topic Collection	ix
How to Use This Guide	ix
List of EX Series Guides for JUNOS Release 10.0	ix
Downloading Software	x
Documentation Symbols Key	xi
Documentation Feedback	xii
Requesting Technical Support	xiii
Self-Help Online Tools and Resources	xiii
Opening a Case with JTAC	xiii

Part 1

Layer 3 Protocols

Chapter 1

Layer 3 Protocols	3
Layer 3 Protocols—Overview	3
Layer 3 Protocols Supported on EX Series Switches	3
Layer 3 Protocols Not Supported on EX Series Switches	4
Configuring Layer 3 Protocols	6
Configuring BGP Sessions (J-Web Procedure)	6
Configuring an OSPF Network (J-Web Procedure)	10
Configuring a RIP Network (J-Web Procedure)	14
Configuring Static Routing (CLI Procedure)	18
Configuring Static Routing (J-Web Procedure)	19
Verifying Layer 3 Protocols Configuration	20
Monitoring BGP Routing Information	20
Monitoring OSPF Routing Information	22
Monitoring RIP Routing Information	25
Monitoring Routing Information	26

About This Topic Collection

- How to Use This Guide on page ix
- List of EX Series Guides for JUNOS Release 10.0 on page ix
- Downloading Software on page x
- Documentation Symbols Key on page xi
- Documentation Feedback on page xii
- Requesting Technical Support on page xiii

How to Use This Guide

Complete documentation for the EX Series product family is provided on webpages at http://www.juniper.net/techpubs/en_US/release-independent/information-products/pathway-pages/ex-series/product/index.html. We have selected content from these webpages and created a number of EX Series guides that collect related topics into a book-like format so that the information is easy to print and easy to download to your local computer.

The release notes are at

http://www.juniper.net/techpubs/en_US/junos10.0/information-products/topic-collections/release-notes/10.0/junos-release-notes-10.0.pdf.

List of EX Series Guides for JUNOS Release 10.0





Title	Description
<i>Complete Hardware Guide for EX3200 and EX4200 Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX3200 and EX4200 switches
<i>Complete Hardware Guide for EX8208 Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX8208 switches
<i>Complete Hardware Guide for EX8216 Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX8216 switches
<i>Complete Software Guide for JUNOS® Software for EX Series Switches, Release 10.0</i>	Software feature descriptions, configuration examples, and tasks for JUNOS Software for EX Series switches

Title	Description
Software Topic Collections	Software feature descriptions, configuration examples and tasks, and reference pages for configuration statements and operational commands (This information also appears in the <i>Complete Software Guide</i> .)
<i>JUNOS® Software for EX Series Switches, Release 10.0: Access Control</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Alarms and System Log Messages</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Configuration and File Management</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Class of Service</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Device Security</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Ethernet Switching</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Interfaces</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Layer 3 Protocols</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: MPLS</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Multicast</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Network Management and Monitoring</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Port Security</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Routing Policy and Packet Filtering</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Spanning-Tree Protocols</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: System Setup</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: User and Access Management</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Virtual Systems</i>	

Downloading Software

You can download JUNOS Software for EX Series switches from the Download Software area at <http://www.juniper.net/customers/support/>. To download the software, you must have a Juniper Networks user account. For information about obtaining an account, see <http://www.juniper.net/entitlement/setupAccountInfo.do>.

Documentation Symbols Key

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.

Text and Syntax Conventions		
Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the <code>configure</code> command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> ■ Introduces important new terms. ■ Identifies book names. ■ Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> ■ A policy <i>term</i> is a named structure that defines match conditions and actions. ■ <i>JUNOS System Basics Configuration Guide</i> ■ RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Plain text like this	Represents names of configuration statements, commands, files, and directories; IP addresses; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> ■ To configure a stub area, include the <code>stub</code> statement at the [edit <code>protocols ospf area area-id</code>] hierarchy level. ■ The console port is labeled <code>CONSOLE</code>.

Text and Syntax Conventions		
Convention	Description	Examples
< > (angle brackets)	Enclose optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> ■ In the Logical Interfaces box, select All Interfaces. ■ To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select Protocols > Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. Send e-mail to techpubs-comments@juniper.net with the following:

- Document URL or title
- Page number if applicable
- Software version
- Your name and company

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <http://www.juniper.net/customers/support/downloads/710059.pdf> .
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/> .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

For international or direct-dial options in countries without toll-free numbers, see [http://www.juniper.net/support/requesting support.html](http://www.juniper.net/support/requesting_support.html) .

Part 1

Layer 3 Protocols

- Layer 3 Protocols on page 3

Chapter 1

Layer 3 Protocols

- Layer 3 Protocols—Overview on page 3
- Configuring Layer 3 Protocols on page 6
- Verifying Layer 3 Protocols Configuration on page 20

Layer 3 Protocols—Overview

- Layer 3 Protocols Supported on EX Series Switches on page 3
- Layer 3 Protocols Not Supported on EX Series Switches on page 4

Layer 3 Protocols Supported on EX Series Switches

EX Series switches support the JUNOS layer 3 features and configuration statements listed in Table 1 on page 3:

Table 1: Supported JUNOS Layer 3 Protocol Statements and Features

Protocol	Notes	For More Information
BGP	Fully supported.	See the <i>JUNOS Software Routing Protocols Configuration Guide</i> at http://www.juniper.net/techpubs/software/junos/ .
BFD	Fully supported.	See the <i>JUNOS Software Routing Protocols Configuration Guide</i> at http://www.juniper.net/techpubs/software/junos/ .
ICMP	Fully supported.	See the <i>JUNOS Software Routing Protocols Configuration Guide</i> at http://www.juniper.net/techpubs/software/junos/ .
IGMPv1, v2 and v3	Fully supported.	See the <i>JUNOS Software Multicast Configuration Guide</i> at http://www.juniper.net/techpubs/software/junos/ .
IS-IS	Supported, with the exceptions noted in “Layer 3 Protocols Not Supported on EX Series Switches” on page 4.	See the <i>JUNOS Software Routing Protocols Configuration Guide</i> at http://www.juniper.net/techpubs/software/junos/ .
MPLS	Supported, with the exceptions noted in “Layer 3 Protocols Not Supported on EX Series Switches” on page 4.	See the <i>JUNOS MPLS Applications Configuration Guide</i> at http://www.juniper.net/techpubs/software/junos/ .

Table 1: Supported JUNOS Layer 3 Protocol Statements and Features (continued)

Protocol	Notes	For More Information
OSPFv1, v2 and v3	Supported, with the exceptions noted in “Layer 3 Protocols Not Supported on EX Series Switches” on page 4.	See the <i>JUNOS Software Routing Protocols Configuration Guide</i> at http://www.juniper.net/techpubs/software/junos/ .
PIM	Supported, with the exception of IPv6.	See the <i>JUNOS Software Multicast Configuration Guide</i> at http://www.juniper.net/techpubs/software/junos/ .
RIP	Fully supported.	See the <i>JUNOS Software Routing Protocols Configuration Guide</i> at http://www.juniper.net/techpubs/software/junos/ .
RIPng	Fully supported.	See the <i>JUNOS Software Routing Protocols Configuration Guide</i> at http://www.juniper.net/techpubs/software/junos/ .
SNMP	Fully supported.	See the <i>JUNOS Software Network Management Configuration Guide</i> at http://www.juniper.net/techpubs/software/junos/ .
VRRP	Fully supported with exception of IPv6 support of VRRP on routed VLAN interfaces.	See High Availability Features for EX Series Switches Overview. See also the <i>JUNOS Software High Availability Guide</i> at http://www.juniper.net/techpubs/software/junos/ .

- Related Topics**
- Layer 3 Protocols Not Supported on EX Series Switches on page 4
 - EX Series Switch Software Features Overview

Layer 3 Protocols Not Supported on EX Series Switches

EX Series switches do not support the JUNOS Layer 3 protocols and features listed in Table 2 on page 4:

Table 2: JUNOS Layer 3 Protocol Statements and Features That Are Not Supported

Feature	Configuration Statements Not Supported on EX Series Switches
DVMRP	■ dvmrp and subordinate statements
Flow aggregation (cflowd)	■ cflow and subordinate statements
GRE	■ Not supported
IPSec	■ [edit services] statements related to IPSec

Table 2: JUNOS Layer 3 Protocol Statements and Features That Are Not Supported (continued)

Feature	Configuration Statements Not Supported on EX Series Switches
IS-IS: <ul style="list-style-type: none"> ■ ES-IS ■ IPv6 in multicast routing protocols 	<ul style="list-style-type: none"> ■ <code>cls-routing</code> statement ■ <code>ipv6-multicast</code> statement ■ <code>isp-interval</code> statement ■ <code>label-switched-path</code> statement ■ <code>isp-lifetime</code> statement ■ <code>te-metric</code> statement
Layer 2 Tunneling Protocol (L2TP)	<ul style="list-style-type: none"> ■ <code>l2tp</code> and subordinate statements
Logical routers	<ul style="list-style-type: none"> ■ <code>logical-routers</code> and subordinate statements
MLD	<ul style="list-style-type: none"> ■ <code>mld</code> and all subordinate statements
MPLS: <ul style="list-style-type: none"> ■ Fast Reroute (FRR) ■ Label Distribution Protocol (LDP) ■ Layer 3 VPNs ■ Multiprotocol BGP (MP-BGP) for VPN-IPv4 family ■ Pseudowire emulation (PWE3) ■ Routing policy statements related to Layer 3 VPNs and MPLS ■ Virtual Private LAN Service (VPLS) 	<ul style="list-style-type: none"> ■ <code>ldp</code> and all subordinate statements
Network Address Translation (NAT)	<ul style="list-style-type: none"> ■ <code>nat</code> and subordinate statements ■ Policy statements related to NAT
OSPF	<ul style="list-style-type: none"> ■ <code>demand-circuit</code> statement ■ <code>label-switched-path</code> and subordinate statements ■ <code>neighbor</code> statement within an OSPF area ■ <code>peer-interface</code> and subordinate statements within an OSPF area ■ <code>sham-link</code> statement ■ <code>te-metric</code> statement
PIM: <ul style="list-style-type: none"> ■ IPv6 	<ul style="list-style-type: none"> ■ <code>inet6</code> family
Routing instances: <ul style="list-style-type: none"> ■ Routing instance forwarding 	<ul style="list-style-type: none"> ■ <code>l2vpn</code> and subordinate statements ■ <code>ldp</code> and subordinate statements ■ <code>vpls</code> and subordinate statements

Table 2: JUNOS Layer 3 Protocol Statements and Features That Are Not Supported (continued)

Feature	Configuration Statements Not Supported on EX Series Switches
SAP and SDP	<ul style="list-style-type: none"> ■ <code>sap</code> and all subordinate statements
General routing options in the routing-options hierarchy: <ul style="list-style-type: none"> ■ MPLS and label-switched-paths 	<ul style="list-style-type: none"> ■ <code>auto-export</code> and subordinate statements ■ <code>dynamic-tunnels</code> and subordinate statements ■ <code>lsp-next-hop</code> and subordinate statements ■ <code>multicast</code> and subordinate statements ■ <code>p2mp-lsp-next-hop</code> and subordinate statements ■ <code>route-distinguisher-id</code> statement
Traffic sampling and forwarding in the forwarding-options hierarchy	<ul style="list-style-type: none"> ■ <code>accounting</code> and subordinate statements ■ <code>family mpls</code> and <code>family multiservice</code> under <code>hash-key</code> hierarchy ■ Under monitoring <code>group-name</code> family <code>inet</code> output hierarchy: <ul style="list-style-type: none"> ■ <code>cflowd</code> statement ■ <code>export-format-cflowd-version-5</code> statement ■ <code>flow-active-timeout</code> statement ■ <code>flow-export-destination</code> statement ■ <code>flow-inactive-timeout</code> statement ■ <code>interface</code> statement ■ <code>port-mirroring</code> statement (On EX Series switches, port mirroring is implemented using the <code>analyzer</code> statement.) ■ <code>sampling</code> and subordinate statements

- Related Topics**
- Layer 3 Protocols Supported on EX Series Switches on page 3
 - EX Series Switch Software Features Overview

Configuring Layer 3 Protocols

- Configuring BGP Sessions (J-Web Procedure) on page 6
- Configuring an OSPF Network (J-Web Procedure) on page 10
- Configuring a RIP Network (J-Web Procedure) on page 14
- Configuring Static Routing (CLI Procedure) on page 18
- Configuring Static Routing (J-Web Procedure) on page 19

Configuring BGP Sessions (J-Web Procedure)

You can use the J-Web interface allows you to create BGP peering sessions on a routing device.



NOTE: To configure BGP sessions a license must be installed on the EX Series switch.

To configure a BGP peering session:

1. Select **Configure > Routing > BGP**.
2. Click one:
 - **Add**—Adds a BGP group. Enter information into the configuration page, as described in Table 3 on page 7.
 - **Edit**—Modifies an existing BGP group. Enter information into the configuration page, as described in Table 3 on page 7.
 - **Delete**—Deletes an existing BGP group.
 - **Disable**—Disables BGP configuration.
3. To modify BGP global settings, click **Edit** in the Global Information section. Enter information as described in Table 4 on page 9.

Table 3: BGP Routing Configuration Summary

Field	Function	Your Action
General tab		
Group Type	Specifies whether the group is an internal BGP (IBGP) group or an external BGP (EBGP) group.	Select the option: Internal or External .
Group Name	Specifies the name for the group.	Type a new name or select and edit the name.
ASN	Sets the unique numeric identifier of the AS in which the routing device is configured.	Type the routing device's 32-bit AS number, in dotted decimal notation. If you enter an integer, the value is converted to a 32-bit equivalent. For example, if you enter 3 , the value assigned to the AS is 0.0.0.3 .
Preference	Specifies the degree of preference for an external route. The route with the highest local preference value is preferred.	Type or select and edit the value.
Cluster Id	Specifies the cluster identifier to be used by the route reflector cluster in an internal BGP group.	Type or select and edit the IPv6 or IPv4 address to be used as the identifier.
Description	Specifies the text description of the global, group, or neighbor configuration.	Type or select and edit the description.
Damping	Specifies whether route flap damping is enabled or not.	To enable route flap damping, select the checkbox. To disable route flap damping do not select the checkbox.
Advertise Inactive Routes	Specifies whether BGP advertises the best route even if the routing table did not select it to be an active route.	To enable advertising inactive routes, select the checkbox. To disable advertising inactive routes, do not select the checkbox.

Table 3: BGP Routing Configuration Summary (continued)

Field	Function	Your Action
Advertise Peer AS Routes	Specifies whether to disable the default behavior of suppressing AS routes.	To enable advertising peer AS routes, select the checkbox. To disable advertising peer AS routes, do not select the checkbox.
Neighbors tab		
Dynamic Neighbors	Configures a neighbor (peer).	Type the IPv4 address of the peer.
Static Neighbors	Configures the system's peers statically.	To configure a static neighbor: <ol style="list-style-type: none"> 1. Specify the IP address. 2. Specify the address of the local end of a BGP session. 3. Specify the degree of preference for an external route. 4. Enter a description. 5. Specify the hold-time value to use when negotiating a connection with the peer. 6. Specify how long a route must be present in the routing table before it is exported to BGP. Use this time delay to help bundle routing updates. 7. Select Passive if you do not want to send active open messages to the peer. 8. Select the option to compare the AS path of an incoming advertised route with the AS number of the BGP peer under the group and replace all occurrences of the peer AS number in the AS path with its own AS number before advertising the route to the peer. 9. Specify an import policy and export policy. 10. Click OK.
Policies tab		
Import Policy	Specifies one or more routing policies to routes being imported into the routing table from BGP.	Click Add to add an import policy. Select the policy and click OK . Click Move up or Move down to move the selected policy up or down the list of policies. Select the policy and click Remove .
Export Policy	Specifies one or more policies to routes being exported from the routing table into BGP.	Click Add to add an export policy. Select the policy and click OK . Click Move up or Move down to move the selected policy up or down the list of policies. Select the policy and click Remove .

Table 4: BGP Global Settings

Field	Function	Your Action
General tab		
Router ASN	Specifies the routing device's AS number.	Type or select and edit the value.
Router Identifier	Specify the routing device's IP address.	Type or select and edit the IP address.
BGP Status	Enables or disables BGP.	<ul style="list-style-type: none"> ■ To enable BGP, select Enabled. ■ To disable BGP, select Disabled.
Description	Describes of the global, group, or neighbor configuration.	Type or select and edit the description.
Confederation Number	Specifies the routing device's confederation AS number.	Type or select and edit the value.
Confederation Members	Specifies the AS numbers for the confederation members.	<p>To add a member AS number, click Add and enter the number in the Member ASN box. Click OK.</p> <p>To modify a confederation member's AS number, select the member click Edit and, enter the number and click OK.</p> <p>To delete a confederation member, select the member and click Remove.</p>
Advance Options	<p>You can configure the following:</p> <ul style="list-style-type: none"> ■ Keep routes—Specifies whether routes learned from a BGP peer must be retained in the routing table even if they contain an AS number that was exported from the local AS. ■ TCP MSS—Configures the maximum segment size (MSS) for the TCP connection for BGP neighbors. ■ MTU Discovery—Select to configure MTU discovery. ■ Remove Private ASN—Select to have the local system strip private AS numbers from the AS path when advertising AS paths to remote systems. ■ Graceful Restart—Specifies the time period when the restart is expected to be complete. Specify the maximum time that stale routes are kept during restart. ■ Multihop—Configures the maximum time-to-live (TTL) value for the TTL in the IP header of BGP packets. ■ Authentication Type—Select the authentication algorithm: None, MD5, Simple. 	<p>Select All or None to configure Keep Routes.</p> <p>Enter a value in the TCP MSS box.</p> <p>Click to enable MTU Discovery.</p> <p>Click to enable Remove Private ASN.</p> <p>Enter the time period for a graceful restart and the maximum time that stale routes must be kept.</p> <p>To configure Multihop, select NextHop Change to allow unconnected third-party next hops. Enter a TTL value.</p> <p>Select the authentication algorithm. If you select MD5, specify an MD5 authentication key (password).</p>
Policies tab		

Table 4: BGP Global Settings (continued)

Field	Function	Your Action
Import Policy	Specifies one or more routing policies to routes being imported into the routing table from BGP.	Click Add to add an import policy Click Move up or Move down to move the selected policy up or down the list of policies. Click Remove to remove an import policy.
Export Policy	Specifies one or more policies to routes being exported from the routing table into BGP.	Click Add to add an export policy Click Move up or Move down to move the selected policy up or down the list of policies. Click Remove to remove an export policy.
Trace Options tab		
File Name	Specifies the name of the file to receive the output of the tracing operation.	Type or select and edit the name.
Number of Files	Specifies the maximum number of trace files.	Type or select and edit the value.
File Size	Specifies the maximum size for each trace file.	Type or select and edit the value.
World Readable	Specifies whether the trace file can be read by any user or not.	Select True to allow any user to read the file. Select False to disallow all users being able to read the file.
Flags	Specifies the tracing operation to perform.	Select a value from the list.

Related Topics ■ [Monitoring BGP Routing Information on page 20](#)

■

Configuring an OSPF Network (J-Web Procedure)

J-Web Configuration allows you to create multi-area OSPF networks.

You can use the J-Web interface to configure a single-area OSPF network:

1. Select **Configure > Routing > OSPF**.
2. Click one:
 - **Add**—Adds an OSPF area. Enter information into the configuration page, as described in Table 5 on page 11.
 - **Edit**—Modifies an existing OSPF area. Enter information into the configuration page, as described in Table 5 on page 11.
 - **Delete**—Deletes an existing OSPF area.

3. To modify OSPF global settings, click **Edit**. Enter information as described in Table 6 on page 12.
4. To disable OSPF, click **Disable**.

Table 5: OSPF Routing Configuration Summary

Field	Function	Your Action
General tab		
Area Id	Uniquely identifies the area within its AS.	Type a 32-bit numeric identifier for the area. Type an integer or select and edit the value. If you enter an integer, the value is converted to a 32-bit equivalent. For example, if you enter 3, the value assigned to the area is 0.0.0.3.
Area Ranges	Specifies a range of IP addresses for an area when sending summary link advertisements (within an area).	To add a range: <ol style="list-style-type: none"> 1. Click Add. 2. Type the area range. 3. Specify the subnet mask. 4. To override the metric for the IP address range, type a specific metric value. 5. If you do not want to display the routes that are contained within a summary, select Restrict advertisements of this area range. 6. If you want a summary of a route to be advertised only when an exact match is made with the configured summary range, select Enforce exact match for advertisement of this area range. 7. Click OK. To modify an existing area range select the area range, and click Edit and edit the value. Click OK . To delete an area range, select the area range and click Delete .
Area Type	Designates the type of OSPF area. <ul style="list-style-type: none"> ■ regular—A regular OSPF area, including the backbone area ■ stub—A stub area ■ nssa—A not-so-stubby area (NSSA) 	Select the type of OSPF area you are creating from the list. If you select stub : <ol style="list-style-type: none"> 1. Enter the default metric. 2. To flood summary LSAs into the stub area, select the check box. If you select nssa : <ol style="list-style-type: none"> 1. Specify the metric type. 2. Enter the default metric. 3. To flood summary LSAs into the nssa area, select the check box. 4. To flood Type-7 LSAs into the nssa area, select the check box.
Interfaces tab		

Table 5: OSPF Routing Configuration Summary (continued)

Field	Function	Your Action
Interfaces	Specifies the interfaces to be associated with the OSPF configuration	To associate an interface with the configuration, select the interface from the list, select Associate and click OK . To edit an interface's configuration: <ol style="list-style-type: none"> 1. Select the interface from the list and click Edit. 2. Specify the cost of an OSPF interface. 3. Specify the traffic engineering metric. 4. Specify how often the router sends hello packets from the interface. 5. Specify how long the router waits to receive a link-state acknowledgment packet before retransmitting link-state advertisements to an interface's neighbors. 6. To enable OSPF on the interface, select the check box. 7. To inform other protocols about neighbor down events, select the check box. 8. To treat the interface as a secondary interface, select the check box. 9. To only advertise OSPF, select the check box. 10. Click OK.
Policies tab		
Import Policy	Specifies one or more policies to control which routes learned from an area are used to generate summary link-state advertisements (LSAs) into other areas.	Click Add to add an import policy Click Move up or Move down to move the selected policy up or down the list of policies. Click Remove to remove an import policy.
Export Policy	Specifies one or more policies to control which summary LSAs are flooded into an area.	Click Add to add an export policy Click Move up or Move down to move the selected policy up or down the list of policies. Click Remove to remove an export policy.

Table 6: Edit OSPF Global Settings

Field	Function	Your Action
General tab		
Router Id	Specifies the ID for the routing device.	Type or select and edit the value.
RIB Group	Installs the routes learned from OSPF routing instances into routing tables in the OSPF routing table group.	Select a value.
Internal Route Preference	Specifies the route preference for internal groups.	Type or select and edit the value.

Table 6: Edit OSPF Global Settings (continued)

Field	Function	Your Action
External Route Preference	Specifies the route preference for external groups.	Type or select and edit the value.
Graceful Restart	Configures graceful restart for OSPF.	To configure graceful restart: <ol style="list-style-type: none"> 1. Specify the estimated time to send out purged grace LSAs over all the interfaces. 2. Specified the estimated time to reacquire a full OSPF neighbor from each area. 3. To disable No Strict LSA Checking, select the check box. 4. To disable graceful restart helper capability, select the check box. Helper mode is enabled by default. 5. Click OK.
SPF Options	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 hold-down interval after the SPF algorithm runs the maximum number of times.	To configure SPF: <ol style="list-style-type: none"> 1. Specify the time interval between the detection of a topology change and when the SPF algorithm runs. 2. Specify the time interval to hold down, or wait before a subsequent SPF algorithm runs after the SPF algorithm has run the configured maximum number of times in succession. 3. Specify the maximum number of times the SPF algorithm can run in succession. After the maximum is reached, the holddown interval begins.
Policies tab		
Import Policy	Specifies one or more policies to control which routes learned from an area are used to generate summary link-state advertisements (LSAs) into other areas.	Click Add to add an import policy Click Move up or Move down to move the selected policy up or down the list of policies. Click Remove to remove an import policy.
Export Policy	Specifies one or more policies to control which summary LSAs are flooded into an area.	Click Add to add an export policy Click Move up or Move down to move the selected policy up or down the list of policies. Click Remove to remove an export policy.
Trace Options tab		
File Name	Specifies the name of the file to receive the output of the tracing operation.	Type or select and edit the name.
Number of Files	Specifies the maximum number of trace files.	Type or select and edit the name.
File Size	Specifies the maximum size for each trace file.	Type or select and edit the name.

Table 6: Edit OSPF Global Settings (continued)

Field	Function	Your Action
World Readable	Specifies whether the trace file can be read by any user or not.	Select True to allow any user to read the file. Select False to disallow all users being able to read the file.
Flags	Specifies the tracing operation to perform.	Select a value from the list.

Related Topics ■ Monitoring OSPF Routing Information on page 22

■

Configuring a RIP Network (J-Web Procedure)

You can use the J-Web interface to create RIP networks.

To configure a RIP network:

1. Select **Configure > Routing > RIP**.
2. Click one:
 - **Add**—Configures a RIP instance. Enter information into the configuration page for RIP, as described in Table 7 on page 14.
 - **Edit**—Modifies an existing RIP instance. Enter information into the configuration page for RIP, as described in Table 7 on page 14.
 - **Delete**—Deletes an existing RIP instance.
4. To modify RIP global settings, click **Edit**. Enter information in the configuration as described in Table 8 on page 15.

Table 7: RIP Routing Configuration Summary

Field	Function	Your Action
General tab		
Routing instance name	Specifies a name for the routing instance.	Type or select and edit the name.
Preference	Specifies the preference of external routes learned by RIP as compared to those learned from other routing protocols.	Type or select and edit the value.
Metric Out	Specifies the metric value to add to routes transmitted to the neighbor.	Type or select and edit the value.
Update interval	Specifies an update time interval to periodically send out routes learned by RIP to neighbors.	Type or select and edit the value.
Route timeout	Specifies the route timeout interval for RIP.	Type or select and edit the value.

Table 7: RIP Routing Configuration Summary (continued)

Field	Function	Your Action
Policies tab		
Import Policy	Applies one or more policies to routes being imported into the local router from the neighbors.	Click Add to add an import policy Click Move up or Move down to move the selected policy up or down the list of policies. Click Remove to remove an import policy.
Export Policy	Applies a policy to routes being exported to the neighbors.	Click Add to add an export policy Click Move up or Move down to move the selected policy up or down the list of policies. Click Remove to remove an export policy.
Neighbors tab		
RIP-Enabled Interfaces	Selects the interfaces to be associated with the RIP instance.	To enable RIP on an interface, click the checkbox next to the interface name. Click Edit if you want to modify an interface's settings.

Table 8: Edit RIP Global Settings

Field	Function	Your Action
General tab		
Send	Specifies RIP send options.	Select a value.
Receive	Configure RIP receive options.	Select a value.
Route timeout (sec)	Specifies the route timeout interval for RIP.	Type a value.
Update interval (sec)	Specifies the update time interval to periodically send out routes learned by RIP to neighbors.	Type or select and edit the value.
Hold timeout (sec)	Specifies the time period the expired route is retained in the routing table before being removed.	Type or select and edit the value.
Metric in	Specifies the metric to add to incoming routes when advertising into RIP routes that were learned from other protocols.	Type or select and edit the value.
RIB Group	Specifies a routing table group to install RIP routes into multiple routing tables.	Select and edit the name of the routing table group.
Message size	Specifies the number of route entries to be included in every RIP update message.	Type or select and edit the value.

Table 8: Edit RIP Global Settings (continued)

Field	Function	Your Action
Check Zero	<p>Specifies whether the reserved fields in a RIP packet are zero. Options are:</p> <ul style="list-style-type: none"> ■ check-zero—Discard version 1 packets that have nonzero values in the reserved fields and version 2 packets that have nonzero values in the fields that must be zero. This default behavior implements the RIP version 1 and version 2 specifications. ■ no-check-zero—Receive RIP version 1 packets with nonzero values in the reserved fields or RIP version 2 packets with nonzero values in the fields that must be zero. This is in spite of the fact that they are being sent in violation of the specifications in RFC 1058 and RFC 2453. 	Select a value.
Graceful switchover	Configures graceful switchover for OSPF.	<p>To disable graceful restart, select Disable.</p> <p>Type or select and edit the estimated time for the restart to finish, in seconds.</p>
Authentication Type	<p>Specifies the type of authentication for RIP route queries received on an interface. Options are:</p> <ul style="list-style-type: none"> ■ None ■ MD5 ■ Simple 	<p>Select the authentication type.</p> <p>Enter the authentication key for MD5.</p>
Policies tab		
Import Policy	Applies one or more policies to routes being imported into the local router from the neighbors.	<p>Click Add to add an import policy</p> <p>Click Move up or Move down to move the selected policy up or down the list of policies.</p> <p>Click Remove to remove an import policy.</p>
Export Policy	Applies a policy to routes being exported to the neighbors.	<p>Click Add to add an export policy</p> <p>Click Move up or Move down to move the selected policy up or down the list of policies.</p> <p>Click Remove to remove an export policy.</p>
Trace Options tab		
File Name	Specifies the name of the file to receive the output of the tracing operation.	Type or select and edit the name.
Number of Files	Specifies the maximum number of trace files.	Type or select and edit the name.
File Size	Specifies the maximum size for each trace file.	Type or select and edit the name.

Table 8: Edit RIP Global Settings (continued)

Field	Function	Your Action
World Readable	Specifies whether the trace file can be read by any user or not.	Select True to allow any user to read the file. Select False to disallow all users being able to read the file.
Flags	Specifies the tracing operation to perform.	Select a value from the list.

- Related Topics**
- Monitoring RIP Routing Information on page 25
 -

Configuring Static Routing (CLI Procedure)

Static routes are routes that are manually configured and entered into the routing table. Dynamic routes, in contrast, are learned by the EX Series switch and added to the routing table using a protocol such as OSPF or RIP.

The switch uses static routes:

- When the switch does not have a route to a destination that has a better (lower) *preference* value. The preference is an arbitrary value in the range from 0 through 255 that the software uses to rank routes received from different protocols, interfaces, or remote systems. The routing protocol process generally determines the active route by selecting the route with the lowest preference value. In the given range, 0 is the lowest and 255 is the highest.
- When the switch cannot determine the route to a destination.
- When the switch is forwarding unroutable packets.

To configure basic static route options using the CLI:

- To configure the switch's default gateway:

```
[edit]
user@switch# set routing-options static route 0.0.0.0/0 next-hop 10.0.1.1
```

- To configure a static route and specify the next address to be used when routing traffic to the static route:

```
[edit]
user@switch# set routing-options static route 20.0.0.0/24 next-hop
10.0.0.2.1
```

- To always keep the static route in the forwarding table:

```
[edit]
user@switch# set routing-options static route 20.0.0.0/24 retain
```

- To prevent the static route from being readvertised:

```
[edit]
user@switch# set routing-options static route 20.0.0.0/24 no-readvertise
```

- To remove inactive routes from the forwarding table:

```
[edit]
user@switch# set routing-options static route 20.0.0.0/24 active
```

- Related Topics**
- Configuring Static Routing (J-Web Procedure) on page 19
 - Monitoring Routing Information on page 26

Configuring Static Routing (J-Web Procedure)

You can use the J-Web interface to configure static routes.

To configure static routes:

1. Select **Configure > Routing > Static Routing**. The Static Routing page displays details of the configured routes.
2. Click one:
 - **Add**—To configure a route. Enter information into the routing page, as described in Table 9 on page 19.
 - **Edit**—To modify an existing route. Enter information into the routing page, as described in Table 9 on page 19.
 - **Delete**—To delete an existing route.

Table 9: Static Routing Configuration Summary

Field	Function	Your Action
Default Route		
Default Route	Specifies the default gateway for the switch.	<p>To specify an IPv4 address:</p> <ol style="list-style-type: none"> 1. Select IPv4. 2. Type an IP address—for example, 10.10.10.10. 3. Enter the subnet mask or address prefix. For example, 24 bits represents 255.255.255.0. <p>To specify an IPv6 address:</p> <ol style="list-style-type: none"> 1. Select IPv6. 2. Type an IP address—for example, 2001:ab8:85a3::8a2e:370:7334. 3. Enter the subnet mask or address prefix.
Static Routes		

Table 9: Static Routing Configuration Summary (continued)

Field	Function	Your Action
Nexthop	Specifies the next-hop address or addresses to be used when routing traffic to the static route.	<p>To add an address:</p> <ol style="list-style-type: none"> 1. Click Add. 2. In the IP address dialog, enter the IP address. <p>NOTE: If a route has multiple next-hop addresses, traffic is routed across each address in round-robin fashion.</p> <ol style="list-style-type: none"> 3. Click OK. <p>To delete a next hop address, select it from the list and click Delete.</p>

- Related Topics**
- Configuring Static Routing (CLI Procedure) on page 18
 - Monitoring Routing Information on page 26
 -

Verifying Layer 3 Protocols Configuration

- Monitoring BGP Routing Information on page 20
- Monitoring OSPF Routing Information on page 22
- Monitoring RIP Routing Information on page 25
- Monitoring Routing Information on page 26

Monitoring BGP Routing Information

Purpose Use the monitoring functionality to monitor BGP routing information on the routing device.

Action To view BGP routing information in the J-Web interface, select **Monitor > Routing > BGP Information**.

To view BGP routing information in the CLI, enter the following commands:

- show bgp summary
- show bgp neighbor

Meaning Table 10 on page 21 summarizes key output fields in the BGP routing display in the J-Web interface.

Table 10: Summary of Key BGP Routing Output Fields

Field	Values	Additional Information
BGP Peer Summary		
Total Groups	Number of BGP groups.	
Total Peers	Number of BGP peers.	
Down Peers	Number of unavailable BGP peers.	
Unconfigured Peers	Address of each BGP peer.	
RIB Summary tab		
RIB Name	Name of the RIB group.	
Total Prefixes	Total number of prefixes from the peer, both active and inactive, that are in the routing table.	
Active Prefixes	Number of prefixes received from the EBGp peers that are active in the routing table.	
Suppressed Prefixes	Number of routes received from EBGp peers currently inactive because of damping or other reasons.	
History Prefixes	History of the routes received or suppressed.	
Dumped Prefixes	Number of routes currently inactive because of damping or other reasons. These routes do not appear in the forwarding table and are not exported by routing protocols.	
Pending Prefixes	Number of pending routes.	
State	Status of the graceful restart process for this routing table: BGP restart is complete, BGP restart in progress, VPN restart in progress, or VPN restart is complete.	
BGP Neighbors		
Details	Click this button to view the selected BGP neighbor details.	
Peer Address	Address of the BGP neighbor.	
Autonomous System	AS number of the peer.	

Table 10: Summary of Key BGP Routing Output Fields (continued)

Field	Values	Additional Information
Peer State	Current state of the BGP session: <ul style="list-style-type: none"> ■ Active—BGP is initiating a TCP connection in an attempt to connect to a peer. If the connection is successful, BGP sends an open message. ■ Connect—BGP is waiting for the TCP connection to become complete. ■ Established—The BGP session has been established, and the peers are exchanging BGP update messages. ■ Idle—This is the first stage of a connection. BGP is waiting for a Start event. ■ OpenConfirm—BGP has acknowledged receipt of an open message from the peer and is waiting to receive a keepalive or notification message. ■ OpenSent—BGP has sent an open message and is waiting to receive an open message from the peer. 	Generally, the most common states are Active , which indicates a problem establishing the BGP connection, and Established , which indicates a successful session setup. The other states are transition states, and BGP sessions normally do not stay in those states for extended periods of time.
Elapsed Time	Elapsed time since the peering session was last reset.	
Description	Description of the BGP session.	

- Related Topics**
- Configuring BGP Sessions (J-Web Procedure) on page 6
 - Layer 3 Protocols Supported on EX Series Switches on page 3

Monitoring OSPF Routing Information

Purpose Use the monitoring functionality to monitor OSPF routing information.

Action To view OSPF routing information in the J-Web interface, select **Monitor > Routing > OSPF Information**.

To view OSPF routing information in the CLI, enter the following CLI commands:

- `show ospf neighbor`
- `show ospf interface`
- `show ospf statistics`

Meaning Table 11 on page 23 summarizes key output fields in the OSPF routing display in the J-Web interface.

Table 11: Summary of Key OSPF Routing Output Fields

Field	Values	Additional Information
OSPF Interfaces		
Interface	Name of the interface running OSPF.	
State	State of the interface: BDR, Down, DR, DROther, Loop, PtToPt, or Waiting.	The Down state, indicating that the interface is not functioning, and PtToPt state, indicating that a point-to-point connection has been established, are the most common states.
Area	Number of the area that the interface is in.	
DR ID	Address of the area's designated device.	
BDR ID	Address of the area's backup designated device.	
Neighbors	Number of neighbors on this interface.	
Adjacency Count	Number of devices in the area using the same area identifier.	
Stub Type	The areas into which OSPF does not flood AS external advertisements	
Passive Mode	In this mode the interface is present on the network but does not transmit or receive packets.	
Authentication Type	The authentication scheme for the backbone or area.	
Interface Address	The IP address of the interface.	
Address Mask	The subnet mask or address prefix.	
MTU	The maximum transmission unit size.	
Interface Cost	The path cost used to calculate the root path cost from any given LAN segment is determined by the total cost of each link in the path.	
Hello Interval	How often the routing device sends hello packets out of the interface.	
Dead Interval	The interval during which the routing device receives no hello packets from the neighbor.	
Retransmit Interval	The interval for which the routing device waits to receive a link-state acknowledgment packet before retransmitting link-state advertisements to an interface's neighbors.	
OSPF Statistics		
Packets tab		

Table 11: Summary of Key OSPF Routing Output Fields (continued)

Field	Values	Additional Information
Sent	Displays the total number of packets sent.	
Received	Displays the total number of packets received.	
Details tab		
Flood Queue Depth	Number of entries in the extended queue.	
Total Retransmits	Number of retransmission entries enqueued.	
Total Database Summaries	Total number of database description packets.	
OSPF Neighbors		
Address	Address of the neighbor.	
Interface	Interface through which the neighbor is reachable.	
State	State of the neighbor: Attempt , Down , Exchange , ExStart , Full , Init , Loading , or 2way .	Generally, only the Down state, indicating a failed OSPF adjacency, and the Full state, indicating a functional adjacency, are maintained for more than a few seconds. The other states are transitional states that a neighbor is in only briefly while an OSPF adjacency is being established.
ID	ID of the neighbor.	
Priority	Priority of the neighbor to become the designated router.	
Activity Time	The activity time.	
Area	Area that the neighbor is in.	
Options	Option bits received in the hello packets from the neighbor.	
DR Address	Address of the designated router.	
BDR Address	Address of the backup designated router.	
Uptime	Length of time since the neighbor came up.	
Adjacency	Length of time since the adjacency with the neighbor was established.	

Related Topics ■ [Configuring an OSPF Network \(J-Web Procedure\) on page 10](#)

- Layer 3 Protocols Supported on EX Series Switches on page 3

Monitoring RIP Routing Information

Purpose Use the monitoring functionality to monitor RIP routing.

Action To view RIP routing information in the J-Web interface, select **Monitor > Routing > RIP Information**.

To view RIP routing information in the CLI, enter the following CLI commands:

- show rip statistics
- show rip neighbor

Meaning Table 12 on page 25 summarizes key output fields in the RIP routing display in the J-Web interface.

Table 12: Summary of Key RIP Routing Output Fields

Field	Values	Additional Information
RIP Statistics		
Protocol Name	The RIP protocol name.	
Port number	The port on which RIP is enabled.	
Hold down time	The interval during which routes are neither advertised nor updated.	
Global routes learned	Number of RIP routes learned on the logical interface.	
Global routes held down	Number of RIP routes that are not advertised or updated during hold-down.	
Global request dropped	Number of requests dropped.	
Global responses dropped	Number of responses dropped.	
RIP Neighbors		
Neighbor	Name of the RIP neighbor.	This value is the name of the interface on which RIP is enabled. Click the name to see the details for this neighbor.
State	State of the RIP connection: Up or Dn (Down).	

Table 12: Summary of Key RIP Routing Output Fields (continued)

Field	Values	Additional Information
Source Address	Local source address.	This value is the configured address of the interface on which RIP is enabled.
Destination Address	Destination address.	This value is the configured address of the immediate RIP adjacency.
Send Mode	The mode of sending RIP messages.	
Receive Mode	The mode in which messages are received.	
In Metric	Value of the incoming metric configured for the RIP neighbor.	

- Related Topics**
- Configuring a RIP Network (J-Web Procedure) on page 14
 - Layer 3 Protocols Supported on EX Series Switches on page 3

Monitoring Routing Information

Purpose Use the monitoring functionality to view the inet.0 routing table.

Action To view the routing tables in the J-Web interface, select **Monitor > Routing > Route Information**. Apply a filter or a combination of filters to view messages. You can use filters to display relevant events.

To view the routing table in the CLI, enter the following commands in the CLI interface:

- show route terse
- show route detail

Table 13 on page 26 describes the different filters, their functions, and the associated actions.

Table 13: Filtering Route Messages

Field	Function	Your Action
Destination Address	Specifies the destination address of the route	Enter the destination address.
Protocol	Specifies the protocol from which the route was learned.	Enter the protocol name.
Next hop address	Specifies the network layer address of the directly reachable neighboring system (if applicable) and the interface used to reach it.	Enter the next hop address.

Table 13: Filtering Route Messages (continued)

Field	Function	Your Action
Receive protocol	Specifies the dynamic routing protocol using which the routing information was received through a particular neighbor .	Enter the routing protocol.
Best route	Specifies only the best route available.	Select the view details of the best route.
Inactive routes	Specifies the inactive routes.	Select the view details of inactive routes.
Exact route	Specifies the exact route.	Select the view details of the exact route.
Hidden routes	Specifies the hidden routes	Select the view details of hidden routes.
Search	Applies the specified filter and displays the matching messages.	To apply the filter and display messages, click Search .

Meaning Table 14 on page 27 summarizes key output fields in the routing information display.

Table 14: Summary of Key Routing Information Output Fields

Field	Values	Additional Information
Static Route Addresses	The list of static route addresses.	
Protocol/	Protocol from which the route was learned: Static , Direct , Local , or the name of a particular protocol.	
Preference	The preference is the individual preference value for the route.	The route preference is used as one of the route selection criteria.
Next-Hop	Network layer address of the directly reachable neighboring system (if applicable) and the interface used to reach it.	<p>If a next hop is listed as Discard, all traffic with that destination address is discarded rather than routed. This value generally means that the route is a static route for which the discard attribute has been set.</p> <p>If a next hop is listed as Reject, all traffic with that destination address is rejected. This value generally means that the address is unreachable. For example, if the address is a configured interface address and the interface is unavailable, traffic bound for that address is rejected.</p> <p>If a next hop is listed as Local, the destination is an address on the host (either the loopback address or Ethernet management port 0 address, for example).</p>
Age	How long the route has been active.	
State	Flags for this route.	There are many possible flags.

Table 14: Summary of Key Routing Information Output Fields *(continued)*

Field	Values	Additional Information
AS Path	AS path through which the route was learned. The letters of the AS path indicate the path origin: <ul style="list-style-type: none"> ■ I—IGP. ■ E—EGP. ■ ?—Incomplete. Typically, the AS path was aggregated. 	

- Related Topics**
- Configuring Static Routing (J-Web Procedure) on page 19
 - Configuring Static Routing (CLI Procedure) on page 18
 -