WXC Integrated Services Module

Installation and Configuration Guide

Release 9.4

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Part Number: 530-027670-01, Revision 1

WXC Integrated Services Module Installation and Configuration Guide
Release 9.4

Revision History
August 2008—Revision 1

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

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. The JUNOS software has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

SOFTWARE LICENSE

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions. Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details. For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

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 présentés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattaché, soient redigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Table of Contents

About This Guide

This preface provides the following guidelines for using the *WXC Integrated Services Module Installation and Configuration Guide*:

Objectives

This guide contains instructions for installing and completing the initial configuration of a WXC Integrated Services Module (also known as WXC ISM 200) in a J-series Services Router running JUNOS software.

NOTE: This manual documents Release 9.4 of JUNOS software. For additional information—either corrections to or information that might have been omitted from this manual—see the *JUNOS Software Release Notes* at http://www.juniper.net.

Router operations are controlled by JUNOS software. You direct the software through either a Web browser or a command-line interface (CLI) to perform the tasks shown in Table 1 on page x.

You use the JUNOS CLI or the J-Web interface to perform the initial configuration of the WXC Integrated Services Module.

For an annotated list of documentation, see "List of Technical Publications" on page xiv. All documents are available at http://www.juniper.net/techpubs/.

Table 1: Capabilities of J-series User Interfaces

User Interface	WXC Integrated Services Module Tasks
J-Web graphical browser interface	■ Initial configuration. ■ Launching the WXOS Web interface. Select **Configuration > Quick Configuration > WAN Acceleration > Manage**.
JUNOS CLI	■ Initial configuration. ■ Basic monitoring.
WXOS Web interface	Configuring WAN acceleration features. The WXOS Web interface is part of the J-Web interface, launched in a separate browser window for configuring WAN acceleration.
WXOS CLI	Configuring advanced settings unavailable in the Web interface.

Audience

This manual is designed for anyone who installs, sets up, configures, monitors, or administers a J-series Services Router or an SRX-series services gateway running JUNOS software. The manual is intended for the following audiences:

- Customers with technical knowledge of and experience with networks and network security, the Internet, and Internet routing protocols
- Network administrators who install, configure, and manage Internet routers

Supported Routing Platforms

This manual describes features supported on J-series Services Routers and SRX-series services gateways running JUNOS software.

How to Use This Manual

This manual and the other manuals in this set explain how to install, configure, and manage:

- JUNOS software for J-series Services Routers
- JUNOS software for SRX-series services gateways

Table 2 on page xi identifies the tasks required to configure and manage these devices and shows where to find task information and instructions.

For an annotated list of the documentation referred to in Table 2 on page xi, see “List of Technical Publications” on page xiv. All documents are available at http://www.juniper.net/techpubs/.

Table 2: Tasks and Related Documentation

Task	Related Documentation
Basic Device Installation and Setup	
■ Reviewing safety warnings and compliance statements ■ Installing hardware and establishing basic connectivity ■ Initially setting up a device	J-series Services Routers: ■ *J-series Services Routers Quick Start* ■ *J-series Services Routers Hardware Guide* ■ *JUNOS Software Release Notes* SRX-series services gateways: the appropriate *Services Gateway Getting Started Guide*
Migration from ScreenOS or JUNOS Software (Legacy Services) to JUNOS Software (if necessary)	
■ Migrating from JUNOS software (legacy services) Release 8.3 or later to JUNOS software ■ Migrating from ScreenOS Release 5.4 or later to JUNOS software.	*JUNOS Software Migration Guide* (J-series Services Routers only)
Context—Changing to Secure Context or Router Context	
Changing the device from one context to another and understanding the factory default settings	*JUNOS Software Administration Guide*
Interface Configuration	
Configuring device interfaces	■ *JUNOS Software Interfaces and Routing Configuration Guide* ■ *JUNOS Software CLI Reference*
Deployment Planning and Configuration	
■ Understanding and gathering information required to design network firewalls and IPsec VPNs ■ Implementing a JUNOS software firewall from a sample scenario ■ Implementing a policy-based IPsec VPN from a sample scenario	*JUNOS Software Design and Implementation Guide* (J-series Services Routers only)
Security Configuration	
Configuring and managing the following security services: ■ Stateful firewall policies ■ Zones and their interfaces and address books ■ IPsec VPNs ■ Firewall screens ■ Interface modes: Network Address Translation (NAT) mode and Router mode ■ Public Key Cryptography (PKI) ■ Application Layer Gateways (ALGs) ■ Chassis clusters ■ Intrusion Detection and Prevention (IDP)	■ *JUNOS Software Security Configuration Guide* ■ *JUNOS Software CLI Reference*
Routing Protocols and Services Configuration	

Table 2: Tasks and Related Documentation *(continued)*

Task	Related Documentation
■ Configuring routing protocols, including static routes and the dynamic routing protocols RIP, OSPF, BGP, and IS-IS ■ Configuring class-of-service (CoS) features, including traffic shaping and policing ■ Configuring packet-based stateless firewall filters (access control lists) to control access and limit traffic rates ■ Configuring MPLS to control network traffic patterns	■ *JUNOS Software Interfaces and Routing Configuration Guide* ■ *JUNOS Software CLI Reference*
WAN Acceleration Module Installation (Optional)	
Installing and initially configuring a WXC Integrated Services Module (ISM 200)	*WXC Integrated Services Module Installation and Configuration Guide* (J-series Services Routers only)
User and System Administration	
■ Administering user authentication and access ■ Monitoring the device, routing protocols, and routing operations ■ Configuring and monitoring system alarms and events, real-time performance (RPM) probes, and performance ■ Monitoring the firewall and other security-related services ■ Managing system log files ■ Upgrading software ■ Diagnosing common problems	*JUNOS Software Administration Guide*
User Interfaces	
■ Understanding and using the J-Web interface ■ Understanding and using the CLI configuration editor	■ *J-series Services Routers Quick Start* (J-series Services Routers only) ■ *JUNOS Software Administration Guide*

Document Conventions

Table 3 on page xiii defines the notice icons used in this guide.

Table 3: 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 4 on page xiii defines the text and syntax conventions used in this guide.

Table 4: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** 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`
Italic text like this	■ Introduces important new terms. ■ Identifies book names. ■ Identifies RFC and Internet draft titles.	■ A policy *term* is a named structure that defines match conditions and actions. ■ *JUNOS System Basics Configuration Guide* ■ RFC 1997, *BGP Communities Attribute*
Italic text like this	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** *domain-name*
Plain text like this	Represents names of configuration statements, commands, files, and directories; IP addresses; configuration hierarchy levels; or labels on routing platform components.	■ To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. ■ The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub <default-metric** *metric***>;**

Table 4: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
| (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 (*string1* | *string2* | *string3*)
# (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 [*community-ids*]

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  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.	■ 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**.

List of Technical Publications

The following sections list hardware and software guides and release notes for J-series Services Routers running JUNOS software with enhanced services.

All documents are available at http://www.juniper.net/techpubs/.

Hardware Guides

- *J-series Services Routers Quick Start*—Explains how to quickly set up a J-series Services Router. This document contains router declarations of conformity.
- *J-series Services Routers Hardware Guide*—Provides an overview, basic instructions, and specifications for J-series Services Routers. This guide explains how to prepare a site, unpack and install the router, replace router hardware, and establish basic router connectivity. This guide contains hardware descriptions and specifications.

Software Guides

- *JUNOS Software Interfaces and Routing Configuration Guide*—Explains how to configure SRX-series and J-series interfaces for basic IP routing with standard routing protocols, ISDN service, firewall filters (access control lists), and class-of-service (CoS) traffic classification.
- *JUNOS Software Security Configuration Guide*—Explains how to configure and manage SRX-series and J-series security services such as stateful firewall policies, IPsec VPNs, firewall screens, Network Address Translation (NAT), Public Key Cryptography, chassis clusters, Application Layer Gateways (ALGs), and Intrusion Detection and Prevention (IDP).
- *JUNOS Software Administration Guide*—Shows how to monitor SRX-series and J-series devices and routing operations, firewall and security services, system alarms and events, and network performance. This guide also shows how to administer user authentication and access, upgrade software, and diagnose common problems.
- *JUNOS Software CLI Reference*—Provides the complete configuration hierarchy available on SRX-series and J-series devices. This guide also describes the configuration statements and operational mode commands unique to these devices.
- *JUNOS Network Management Configuration Guide*—Describes enterprise-specific MIBs for JUNOS software. The information in this guide is applicable to M-series, T-series, EX-series, SRX-series, and J-series devices.
- *JUNOS System Log Messages Reference*—Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message. The information in this guide is applicable to M-series, T-series, EX-series, SRX-series, and J-series devices.
- *JUNOS Software Design and Implementation Guide*—Provides guidelines and examples for designing and implementing IPsec VPNs, firewalls, and routing on J-series Services Routers running JUNOS software with enhanced services.
- *JUNOS Software Migration Guide*—Provides instructions for migrating an SSG device running ScreenOS software or a J-series Services Router running the JUNOS software to JUNOS software with enhanced services.
- *WXC Integrated Services Module Installation and Configuration Guide*—Explains how to install and initially configure a WXC Integrated Services Module in a J-series Services Router for application acceleration.

Release Notes

- *JUNOS Software Release Notes*—Summarize new features and known problems for a particular release of JUNOS software, including JUNOS software for J-series and SRX-series devices.The release notes also contain corrections and updates to the manuals and software upgrade and downgrade instructions for JUNOS software.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at

https://www.juniper.net/beta/junos/docbug/. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version

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/710059.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

Part 1

Installing and Configuring a WXC Integrated Services Module

Chapter 1

WXC Integrated Services Module Overview

The WXC Integrated Services Module (WXC ISM 200) provides WAN acceleration on a J-series Services Router running JUNOS software. The integration of application acceleration with branch routing platforms provides a consolidated solution for the branch office. The WXC ISM 200 is a LAN-based network device that enhances the throughput of WAN circuits by addressing the three constraints on WAN performance—bandwidth, latency, and application contention—and provides reporting and visibility into WAN traffic and throughput.

The WXC ISM 200 is installed in a J-series chassis like a Physical Interface Module (PIM), but unlike a PIM, it does not provide any physical interfaces. The module is controlled by the WX operating system (WXOS) software rather than the JUNOS software.

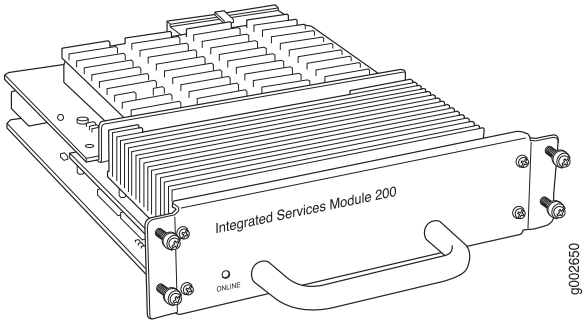
A WXC ISM 200 or WX/WXC device must be installed on each side of a WAN circuit.

This chapter contains the following topics:

Hardware Overview

Figure 1 on page 4 shows the WXC ISM 200.

Figure 1: WXC Integrated Services Module (WXC ISM 200)



An ONLINE LED is located on the left side of the WXC ISM 200. Table 5 on page 4 describes the LED states.

Table 5: WXC Integrated Services Module ONLINE LED

Color	State	Description
Green	On steadily	Module is functioning correctly.
Yellow	Blinking	Module is receiving power but has lost contact with the Routing Engine. No traffic is being forwarded to the module.
Amber	Blinking	Module has detected a problem with the disk drive.
Unlit	Off	Module is not receiving power.

The WXC ISM 200 occupies two slots in the J-series chassis. You can install only one WXC ISM 200 in a J-series Services Router chassis.

You can install Physical Interface Modules (PIMs) in the remaining slots to provide physical connections to a LAN or a WAN. PIMs receive incoming packets from the network and transmit outgoing packets to the network. Each PIM is equipped with a dedicated network processor that forwards incoming data packets to the Routing Engine, and receives outgoing data packets from the Routing Engine.

NOTE: The exact combination of PIMs that you can install in a J-series Services Router is affected by power and thermal constraints. For more information, see the *J-series Services Routers Hardware Guide*.

For information about network interfaces, and for instructions on configuring network interfaces, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

Supported Hardware and Software

You can install the WXC ISM 200 in any J2320, J2350, J4350, or J6350 Services Router running JUNOS software.

The WXC ISM 200 is supported on the following software releases:

- JUNOS Release 9.0 or later running on the J-series Services Router
- WXOS Release 5.4.6j or later running on the WXC ISM 200

Hardware Capacity

The WXC ISM 200 provides the following:

- Up to 4 Mbps of throughput
- Up to 10 connections to other WX/WXC platforms or modules
- Up to 256 application definitions
- Up to 8000 routes
- 120 GB of disk space

WXC Integrated Services Module Terms

To understand the WXC ISM 200, become familiar with the terms defined in Table 6 on page 5.

Table 6: WXC Integrated Services Module Terms

Term	Definition
JUNOS software	Operating system that combines the security features from ScreenOS with the routing features from the JUNOS software.
J-Web	Graphical user interface used to configure, monitor, and manage individual Juniper Networks routing platforms.
NSM	NetScreen-Security Manager (NSM). A central management tool for J-series Services Routers, including device configuration, network settings, and security policy.
WX **WXC**	Juniper Networks application acceleration platforms and modules. WX stands for *WAN acceleration*. The WXC ISM 200 is inserted in a J-series Services Router. All other models are standalone platforms. The WXC platforms and modules use disk-based compression and generally achieve higher compression rates than the non-disk-based WX platforms.
WX CMS	The WX Central Management System software. A central management tool for managing, monitoring, and configuring up to 2000 Juniper Networks WX and WXC application acceleration platforms, including WXC Integrated Services Modules.
WXOS Web interface	Graphical user interface used to configure WAN acceleration features. To open the WXOS Web interface for the WXC ISM 200, select **Configuration > Quick Configuration > WAN Acceleration > Manage** in the J-Web interface.

Sample Deployment Topologies

Figure 2 on page 6, Figure 3 on page 6, and Figure 4 on page 7 show three sample deployment topologies for J-series routers that have the WXC ISM 200 installed.

NOTE: The WXC ISM 200 supports only route-based IPSec VPNs. Policy-based IPSec VPNs are not supported.

Figure 2: Sample Private WAN Deployment

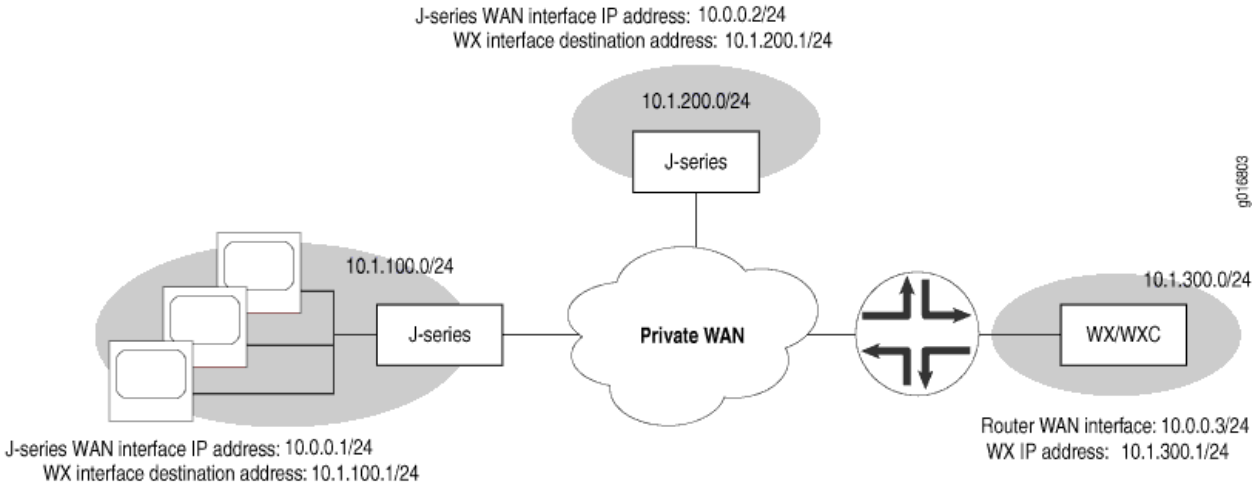


Figure 3: Sample IPSec VPN Deployment

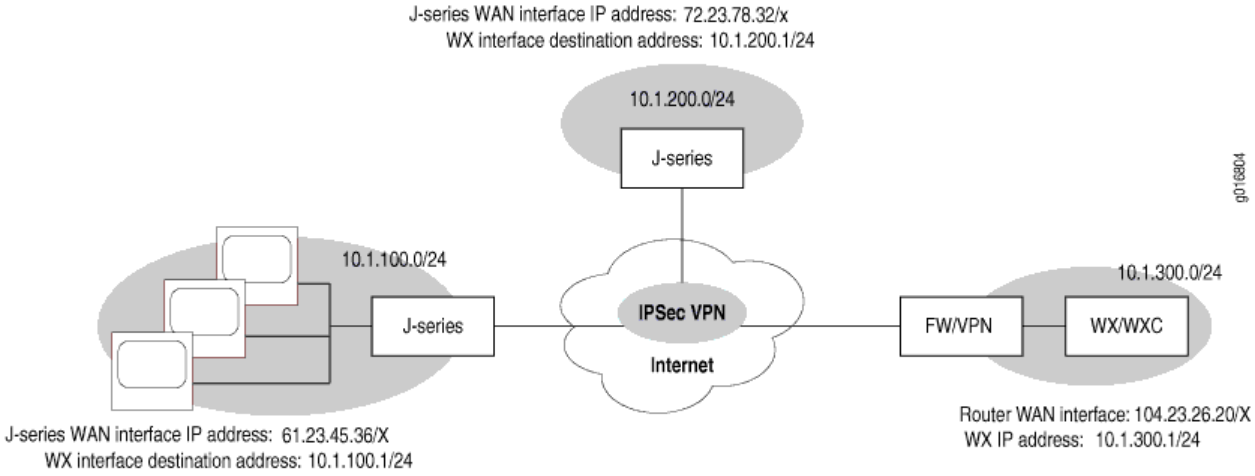
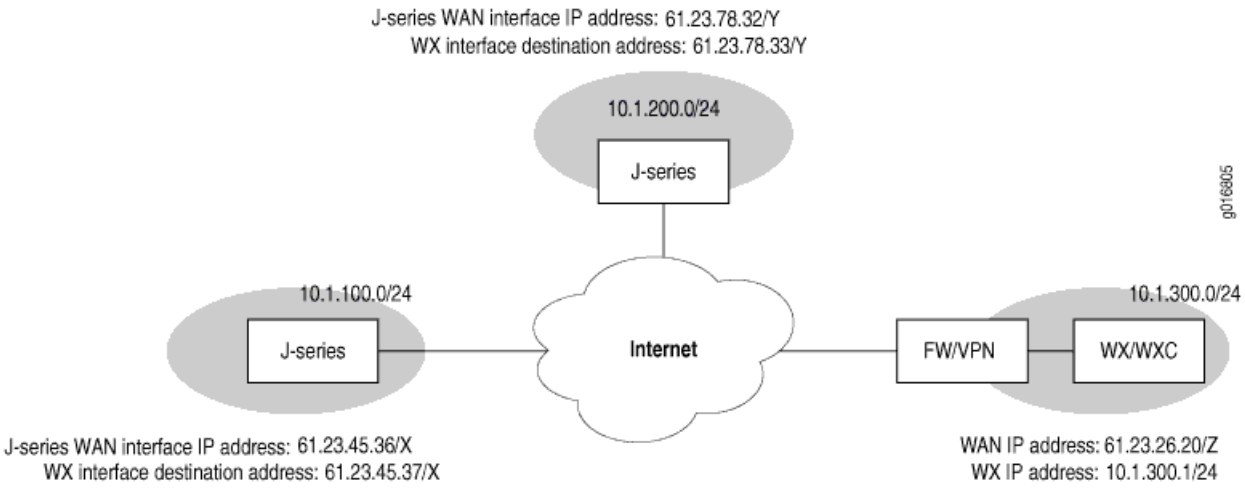


Figure 4: Sample NAT Deployment



NOTE: On the WXC ISM 200, the interface destination address must be a public IP address.

Chapter 2

Installing a WXC Integrated Services Module

A single WXC ISM 200 can be installed in any J2320, J2350, J4350, or J6350 Services Router running the JUNOS software.

This chapter contains the following topics:

Before You Begin

Before you begin installing a WXC ISM 200 in a J-series Services Router, complete the following tasks:

- If you have not already done so, install and configure the J-series Services Router as described in the *J-series Services Routers Hardware Guide*.
- If you do not already have the JUNOS software, load the latest version from a console connected to the router. (For release information, see "Supported Hardware and Software" on page 4. For loading instructions, see the *JUNOS Software Administration Guide*.)
- Configure the WAN interfaces on the J-series Services Router, as described in the *JUNOS Software Interfaces and Routing Configuration Guide*.
- Verify that the WXC ISM 200 you are installing and the PIMs already installed in the router do not exceed the limitations of the chassis. For more information, see the power management section in the *J-series Services Routers Hardware Guide*.

CAUTION: Do not install a combination of modules in a single chassis that exceeds the maximum power and heat capacity of the chassis. If J-series power management is enabled, modules that exceed the maximum power and heat capacity remain offline when the chassis is powered on.

- Gather the following tools and parts:

- WXC ISM 200 (For release information, see “Supported Hardware and Software” on page 4.)
- Electrostatic bag or antistatic mat
- Electrostatic discharge (ESD) grounding wrist strap
- Phillips (+) screwdriver, number 2

Installing and Removing a WXC ISM 200

WXC Integrated Services Modules are field-replaceable. You must power off the router before installing or removing modules. This section contains the following topics:

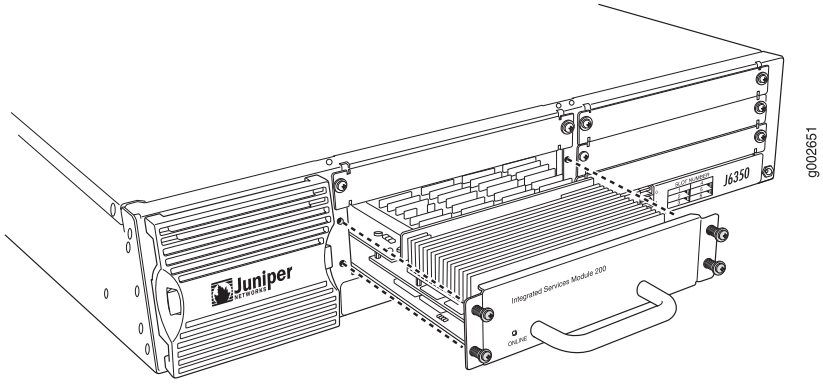
Installing a WXC ISM 200

You can install a single WXC ISM 200 in either regular or high-speed slots of a J2320, J2350, J4350, or J6350 Services Router. The module occupies two slots, and the extra connector on high-speed slots is detected and configured automatically. If you insert a second WXC ISM 200, the module in the higher slot numbers will not power on.

CAUTION: Do not hot-swap WXC Integrated Services Modules or PIMs. Failure to power off the router before removing or installing a module might result in damage to the hardware.

To install a WXC ISM 200 (see Figure 5 on page 10):

Figure 5: Installing a WXC Integrated Services Module



1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to the ESD point on the chassis, or to an outside ESD point if the Services Router is disconnected from earth ground. For more information about ESD, see the *J-series Services Routers Hardware Guide*.
2. Back up the current router configuration.
3. To power off the router, use the CLI command request system power-off (recommended), or hold down the power button for at least 2 seconds. Verify that the POWER LED blinks and then turns off.
4. Remove the faceplates from two of the slots.
5. Align the notches in the connector at the rear of the WXC ISM 200 with the notches in the Services Router slot, and slide the module in until it lodges firmly in the router.

CAUTION: Slide the WXC ISM 200 straight into the slot to avoid damaging the components on the module.

6. Tighten the screws on each side of the module faceplate.
7. Press and release the power button to power on the router. Verify that the POWER LED for the J-series Services Router lights steadily after you press the power button.
8. Verify that the ONLINE LED on the module lights steadily green.

   You can also verify the module is online by issuing the show chassis fpc pic-status command:

```
user@host> show chassis fpc pic-status

Slot 0 Online FPC
  PIC 0 Online 4x GE Base PIC
Slot 2 Online FPC
  PIC 0 Online Integrated Services Module
```

NOTE: In show chassis fpc-pic-status output, the higher of the two slot numbers occupied by the WXC ISM 200 is reported as an FPC number, and the PIC number is always zero.

   For more information about show chassis fpc pic-status, see the *JUNOS System Basics and Services Command Reference*.

9. Complete the initial configuration of the WXC ISM 200, as described in "Configuring a WXC Integrated Services Module" on page 13.

Removing the WXC ISM 200

The WXC ISM 200 is installed in the front of the Services Router.

CAUTION: Do not hot-swap WXC Integrated Services Modules or PIMs. Failure to power off the router before removing or installing a module might result in damage to the hardware.

To remove the WXC ISM 200:

1. Place an electrostatic bag or antistatic mat on a flat, stable surface to receive the WXC ISM 200.
2. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to the ESD point on the chassis, or to an outside ESD point if the Services Router is disconnected from earth ground. For more information about ESD, see the *J-series Services Routers Hardware Guide*.
3. To power off the router, use the CLI command request system power-off (recommended), or hold down the power button for at least 2 seconds. Verify that the POWER LED blinks and then turns off.
4. Loosen the screws on each side of the WXC ISM 200 faceplate.
5. Grasp the handle on the WXC ISM 200 faceplate, and slide the module out of the router. Place it in the electrostatic bag or on the antistatic mat.
6. If you are not reinstalling a PIM or WXC ISM 200 in the emptied slots, install blank PIM panels over the slots to maintain proper airflow.

Chapter 3

Configuring a WXC Integrated Services Module

You can use the J-Web interface or the JUNOS CLI to perform the initial configuration of the WXC ISM 200.

This chapter contains the following topics:

Before You Begin

Before you begin configuring the WXC ISM 200, install the module in the chassis, as described in “Installing a WXC ISM 200” on page 10.

When installation is complete and the router is powered on, the operating system automatically creates two interfaces:

- wx-*slot*/0/0—You must configure an IP address for this internal interface.
- pc-*slot*/0/0—This internally configured interface is used by the system as a control path between the WXC ISM 200 and the Routing Engine (RE).

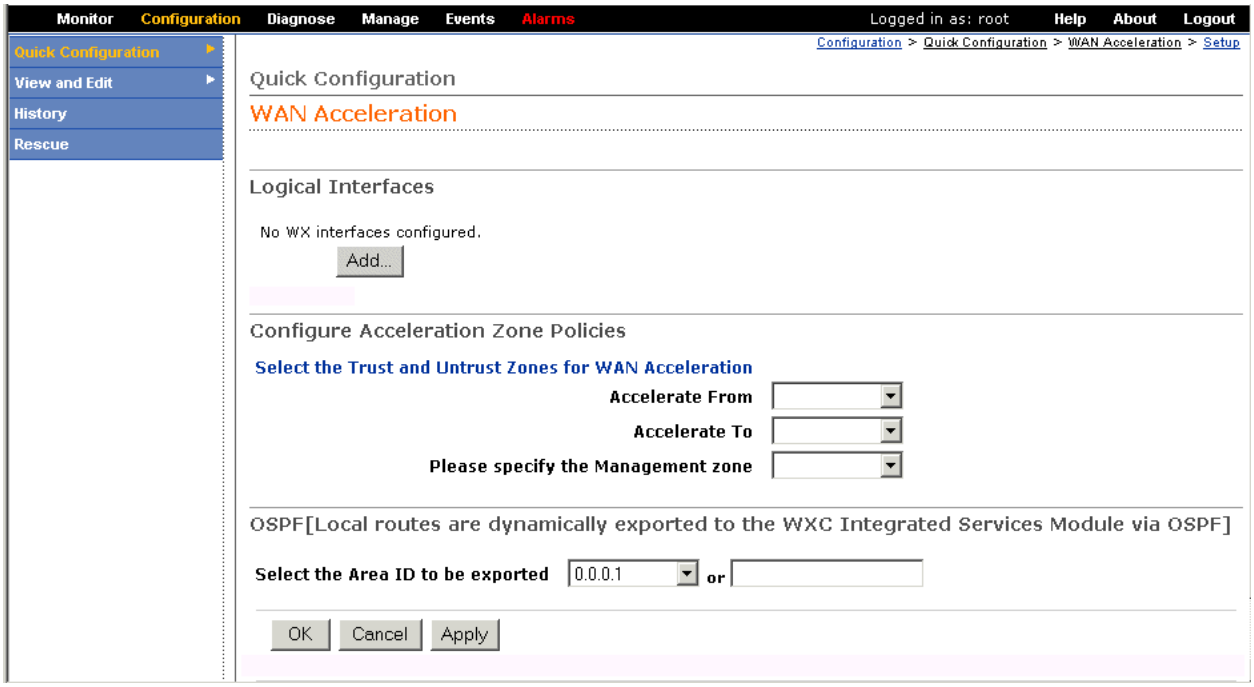
In both interface names, *slot* is the higher number of the two slots in which the WXC ISM 200 is installed. For example, for a module installed in slots 5 and 6, the interface names are wx-6/0/0 and pc-6/0/0. If you later move the module to another pair of slots, the interface names are changed, and you must configure an IP address for the new wx- interface.

Configuring the WXC ISM 200 Using J-Web Quick Configuration

You can use the WAN Acceleration Quick Configuration page to perform the initial configuration of a WXC ISM 200, as shown in Figure 6 on page 14. If the J-series

Services Router is operating in a router context (that is, all interfaces are in the same zone), the acceleration zone policies are replaced by local and remote LAN addresses.

Figure 6: WAN Acceleration Quick Configuration Page



To perform the initial WXC ISM 200 configuration with Quick Configuration:

1. In the J-Web interface, select **Configuration > Quick Configuration > WAN Acceleration > Setup**.
2. Enter information into the WAN Acceleration Quick Configuration page as described in Table 7 on page 14.
3. Click one of the following buttons:
   - To apply the configuration and stay in the Quick Configuration page, click **Apply**.
   - To apply the configuration and return to the previous Quick Configuration page, click **OK**.
   - To cancel your entries and return to the previous Quick Configuration page, click **Cancel**.
4. To check the configuration, go on to "Verifying the Initial WXC ISM 200 Configuration" on page 19.

Table 7: WAN Acceleration Quick Configuration Summary

Field	Function	Your Action
Logical Interfaces		

Table 7: WAN Acceleration Quick Configuration Summary *(continued)*

Field	Function	Your Action
Add logical interface	Specifies IP addresses for the wx-*slot*/0/0.0 interface that is created automatically when you install the WXC ISM 200. The *slot* indicates the higher of the two slot numbers occupied by the WXC ISM 200.	Click **Add** to configure the interface for the first time, or select the interface name to change the interface description or IP addresses.
Logical Interface Description	(Optional) Describes the logical interface.	Type a text description of the logical interface to more clearly identify it in monitoring displays.
IPv4 Address and Prefix	Specifies the IPv4 address and prefix for the primary interface.	Type an IPv4 address and prefix. The address can be any value, but the prefix must be /32. For example: 2.2.2.2/32
Destination Address	Specifies the primary IP address, which is used to manage the WXC ISM 200, and as the source and destination address of optimized traffic sent across the WAN.	Type an IP address on the LAN that is in the same subnet as the Services Router. If NAT is used, the destination address must be a public WAN IP address.
Configure Multipath	If a WXC ISM 200 has two possible WAN paths to a remote WX endpoint, you can configure a secondary address and next-hop gateway to route selected application traffic to a designated secondary path.	Click Configure Multipath to configure a secondary address. For more configuration options, see "Configuring Multi-Path Routing Policies" on page 23.
IPv4 Address and Prefix	Specifies the IPv4 address and prefix for the secondary interface.	Type an IPv4 address and prefix. The address can be any value, but the prefix must be /32.
Destination Address	Specifies the secondary IP address of the WXC ISM 200, which is used as the source address of optimized traffic to be routed to the secondary path.	Type an IP address on the LAN that is in the same subnet as the Services Router.
Secondary WAN Link Nexthop Destination Address	Specifies the IP address of the WAN link for the secondary path.	Type the IP address of the secondary WAN link.
Configure Acceleration Zone Policies (Security Context Only)		
Accelerate From Accelerate To	Identifies the source and destination zones of the traffic that is redirected to the WXC ISM 200 for acceleration.	Select the From and To zones of the traffic to be accelerated, such as **trust** and **untrust**. The From and To zones must be for LAN and WAN interfaces, respectively. If the appropriate zones are not listed, select **Configuration > Quick Configuration > Zones** to create the zones.

Table 7: WAN Acceleration Quick Configuration Summary *(continued)*

Field	Function	Your Action
Management Zone	Identifies the zone from which the WXC ISM 200 is managed.	Select the source zone of the management traffic (the **untrust** zone is the default).
Configure the Local and Remote LAN Network Address (Router Context Only)		
Local LAN Network Address	Specifies the local LAN network addresses for which traffic is redirected to the WXC ISM 200.	Type the local network address and prefix.
Remote LAN Network Address	Specifies the remote LAN network addresses for which traffic is redirected to the WXC ISM 200.	Type a remote network address and prefix, and click **Add**. You can add any number of remote addresses.
OSPF [Local routes are dynamically exported...]		
Select the Area ID to be exported	Identifies the OSPF area ID of the routes to be exported to the WXC ISM 200.	Select the Area ID or type in the Area ID number.

Configuring the WXC ISM 200 Using the CLI

This section describes how to perform the initial configuration of a WXC ISM 200 using the JUNOS CLI. The WXC ISM 200 in this sample procedure is installed in slots 5 and 6 of the J-series Services Router.

To initially configure the WXC ISM 200:

1. Assign IP addresses to the wx-6/0/0 interface:

   ```
   user@host# set interfaces wx-6/0/0 unit 0 family inet address 2.2.2.2/32
     destination 10.8.51.2
   ```

   The internal IP prefix and netmask 2.2.2.2/32 can be any IP address, but the netmask /32 is required. The primary (destination) IP address 10.8.51.2 can be any real address on the LAN in the same subnet as the router. To use the WXC ISM 200 with NAT, the destination address must be a public WAN IP address.

2. Assign the wx-6/0/0 interface to OSPF area 0.0.0.1; import static routes, direct routes, RIP routes, OSPF routes, and IS-IS routes from the routing table; and create a policy to accept the routes:

   ```
   user@host# set protocols ospf export wx-export
   user@host# set protocols ospf area 0.0.0.1 interface wx-6/0/0.0
   user@host# set policy-options policy-statement wx-export from instance master
     protocol [ static direct rip ospf isis ]
   user@host# set policy-options policy-statement wx-export then accept
   ```

3. If the J-series Services Router is operating in a security context, create the following zones and policies. If the router is operating in a router context (one zone), go to Step 4.

   a. Configure a trust security zone and an untrust security zone and assign them to LAN and WAN interfaces, respectively. The router cannot be accessed remotely until you assign at least one interface to the trust zone.

      user@host# **set security zones security-zone trust interfaces ge-0/0/0.0 host-inbound-traffic system-services all**
      user@host# **set security zones security-zone untrust interfaces ge-0/0/1.0 host-inbound-traffic system-services all**

   b. Create the internal zone wx-zone that includes only the wx-6/0/0.0 interface to which all accelerated traffic is to be directed:

      user@host# **set security zones security-zone wx-zone interfaces wx-6/0/0.0 host-inbound-traffic system-services all**
      user@host# **set security zones security-zone wx-zone interfaces wx-6/0/0.0 host-inbound-traffic protocols all**

   c. Create the acceleration zone security policy trust–to-untrust to redirect traffic sent from the trust zone to the untrust zone. In the following example, all traffic from the trust to untrust zone is redirected to the WXC ISM 200:

      user@host# **set security policies from-zone trust to-zone untrust policy trust–to-untrust match source-address any**
      user@host# **set security policies from-zone trust to-zone untrust policy trust–to-untrust match destination-address any**
      user@host# **set security policies from-zone trust to-zone untrust policy trust–to-untrust match application any**
      user@host# **set security policies from-zone trust to-zone untrust policy trust–to-untrust then permit application-services redirect-wx**

      Packets sent from the LAN to the WAN are redirected to the WXC ISM 200 by the application service redirect-wx.

   d. Similarly, specify an untrust–to-trust policy that redirects traffic from the untrust zone to the trust zone:

      user@host# **set security policies from-zone untrust to-zone trust policy untrust–to-trust match source-address any**
      user@host# **set security policies from-zone untrust to-zone trust policy untrust–to-trust match destination-address any**
      user@host# **set security policies from-zone untrust to-zone trust policy untrust–to-trust match application any**
      user@host# **set security policies from-zone untrust to-zone trust policy untrust–to-trust then permit application-services reverse-redirect-wx**

      Packets sent from the WAN to the LAN are redirected to the WXC ISM 200 by the application service reverse-redirect-wx.

   e. Create security policies wx–to–untrust and untrust-to-wx to allow traffic between the internal zone wx-zone and the untrust zone:

```
user@host# set security policies from-zone wx-zone to-zone untrust policy
  wx–to–untrust match source-address any
user@host# set security policies from-zone wx-zone to-zone untrust policy
  wx–to–untrust match destination-address any
user@host# set security policies from-zone wx-zone to-zone untrust policy
  wx–to–untrust match application any
user@host# set security policies from-zone wx-zone to-zone untrust policy
  wx–to–untrust then permit

user@host# set security policies from-zone untrust to-zone wx-zone policy
  untrust-to-wx match source-address any
user@host# set security policies from-zone untrust to-zone wx-zone policy
  untrust-to-wx match destination-address any
user@host# set security policies from-zone untrust to-zone wx-zone policy
  untrust-to-wx match application any
user@host# set security policies from-zone untrust to-zone wx-zone policy
  untrust-to-wx then permit
```

f. Create a wx–to–wx policy to allow the WXC ISM 200 to send pings and registration server traffic:

```
user@host# set security policies from-zone wx-zone to-zone wx-zone policy
  wx–to–wx match source-address any
user@host# set security policies from-zone wx-zone to-zone wx-zone policy
  wx–to–wx match destination-address any
user@host# set security policies from-zone wx-zone to-zone wx-zone policy
  wx–to–wx match application any
user@host# set security policies from-zone wx-zone to-zone wx-zone policy
  wx–to–wx then permit
```

4. If the router is operating in a router context, create one zone and the following policies:

   a. Configure a trust security zone for all interfaces that specifies the local and remote address ranges. For example:

```
user@host# set security zones security-zone trust interfaces all
user@host# set security zones security-zone trust host-inbound-traffic
  system-services all
user@host# set security zones security-zone trust host-inbound-traffic
  protocols all
user@host# set security zones security-zone trust address-book address
  local_lan_network 20.10.10.0/30
user@host# set security zones security-zone trust address-book address
  remote_lan_network 30.10.10.0/30
```

   b. Create a security policy redirect so that traffic sent from the local to the remote network is redirected to the WXC ISM 200:

```
user@host# set security policies from-zone trust to-zone trust policy redirect
  match source-address local_lan_network
user@host# set security policies from-zone trust to-zone trust policy redirect
  match destination-address remote_lan_network
user@host# set security policies from-zone trust to-zone trust policy redirect
  match application any
```

```
user@host# set security policies from-zone trust to-zone trust policy redirect
  then permit application-services redirect-wx
```

The application service redirect-wx redirects each packet to the WXC ISM 200.

c. Create a security policy reverse so that traffic sent from the remote to the local network is redirected to the WXC ISM 200:

```
user@host# set security policies from-zone trust to-zone trust policy reverse
  match source-address remote_lan_network
user@host# set security policies from-zone trust to-zone trust policy reverse
  match destination-address local_lan_network
user@host# set security policies from-zone trust to-zone trust policy reverse
  match application any
user@host# set security policies from-zone trust to-zone trust policy reverse
  then permit application-services reverse-redirect-wx
```

The application service reverse-redirect-wx redirects each packet to the WXC ISM 200.

d. Specify the following security flows:

```
user@host# set security flow allow-dns-reply
user@host# set security flow tcp-session no-syn-check
user@host# set security flow tcp-session no-syn-check-in-tunnel
user@host# set security flow tcp-session no-sequence-check
```

5. Commit the configuration to make it the operating configuration on the router:

```
user@host# commit
```

6. To check the configuration, go on to "Verifying the Initial WXC ISM 200 Configuration" on page 19.

Verifying the Initial WXC ISM 200 Configuration

To verify that the WXC ISM 200 is properly configured, perform the following task.

Verifying WAN Acceleration Status

Purpose Verify the status of the WXC ISM 200, and the compatibility of the router and WXOS software.

Action From configuration mode in the CLI, enter the show wan-acceleration status command.

```
user@host> show wan-acceleration status
  Redirection status: active, Interface: wx-2/0/0
  Primary address: 10.87.5.2, Secondary address: 0.0.0.0
  JUNOS version: 9.4R1 Enhanced Services
  WXOS version: 5.4.6.0j
  JUNOS/WXOS protocol: Version compatible
```

Meaning Verify that the status of the WXC ISM 200 interface is active, the correct IP address is assigned to the interface, and the router and WXOS software versions are compatible.

Related Topics For a complete description of show wan-acceleration status, see the *JUNOS Software CLI Reference*.

Monitoring the WAN Acceleration Interface

To view status information and traffic statistics for the WAN acceleration interface, select **Monitor > WAN Acceleration** in the J-Web interface, or select **Monitor > Interfaces** and select the interface name (wx-s*lot*/0/0). Alternatively, enter the following CLI command:

```
user@host> show interfaces wx-slot/0/0 detail
```

For a description of the interface properties and statistics, see the *JUNOS Software Administration Guide*.

Applying Screens to Security Zones

On the J-series Services Router, the **set security screen** command can be applied to the zone that contains the WAN interface, but it has no effect when applied to the zone that contains the WX interface (the wx-zone).

Chapter 4

Configuring WAN Acceleration Features

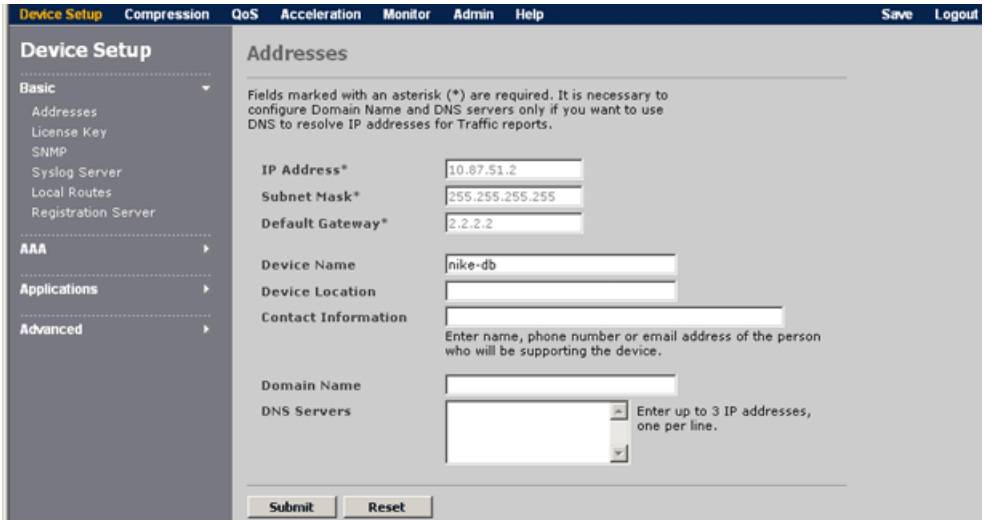
This chapter contains the following topics:

Enabling WAN Acceleration

After you perform the initial configuration of the WXC ISM 200, use the following procedure to enable WAN acceleration:

1. Select **Configuration > Quick Configuration > WAN Acceleration > Manage** in the J-Web interface to open the WXOS Web interface in a separate window (see Figure 7 on page 22).

Figure 7: Entry Page to the WXOS Web interface



If you have difficulty opening multiple WXOS Web interface windows using Microsoft Internet Explorer, version 6, go to **Tools > Internet Options > Temporary Internet Files > Settings** and select **Automatically**.

2. If you already have a WX registration server, do the following:

   a. Click **Device Setup > Registration Server**.

   b. Click **Transfer registration server**.

   c. Type the IP address of your current registration server, and click **Submit**.

   Alternatively, change your remote WX endpoints to use the WXC ISM 200 as the registration server. WAN acceleration can occur only between endpoints that use the same registration server and belong to the same WX community (the default).

3. Log in to each remote WX endpoint where you want to establish a tunnel to the WXC ISM 200, and do the following:

   a. Click **Compression > Advanced > Tunnel Mode**, change the tunnel mode from IpComp (the default) to UDP, and click **Submit**. The tunnel mode on a WXC ISM 200 is always set to UDP, and cannot be changed.

CAUTION: Traffic to remote WX endpoints will be blocked unless the tunnel mode is set to UDP.

---

   b. Click **Compression > Endpoints** and verify that a tunnel to the WXC ISM 200 is enabled.

c. Click **Acceleration** to verify that TCP Acceleration to the WXC ISM 200 is enabled.

4. On the WXC ISM 200, click **Compression > Endpoints** to enable or disable tunnels to the appropriate endpoints. Click **Acceleration** to verify that TCP Acceleration is enabled. To accelerate traffic to a remote endpoint, compression and acceleration must be enabled in both directions.

5. Click **Compression > Compression Subnets**, select the local subnets that you want to advertise to remote endpoints for compression, and click **Submit**. Only the local subnet of the wx-*slot*/0/0 interface is advertised by default.

For more information about configuring WXC features, see the *WX/WXC Operator's Guide*, available at http://www.juniper.net/techpubs/hardware/wx/.

Configuring IPSec

The WXC ISM 200 module cannot establish encrypted tunnels with other WX endpoints. However, the WXC ISM 200 module supports route-based IPSec VPNs configured between J-series routers. Policy-based VPNs are not supported. To configure route-based IPSec VPNs, refer to the *JUNOS Software Security Configuration Guide*.

Configuring Multi-Path Routing Policies

If a WXC ISM 200 has two possible WAN paths to a remote WX endpoint, you can designate one path as the primary and the other as the secondary. You can then route application traffic to the primary or secondary path based on the performance requirements of the application and the performance of the path.

To configure the J-series Services Router to support Multi-Path:

1. Specify a secondary address for the wx-*slot*/0/0 interface:

```
user@host# set interfaces wx-6/0/0 unit 0 family inet filter input
   classify-secondary
user@host# set interfaces wx-6/0/0 unit 0 family inet address 2.2.2.2/32
   destination 10.8.51.3
```

   The secondary address (10.8.51.3) is displayed automatically in the WXOS Web interface.

2. Specify a firewall filter so that packets that have the secondary address as their source address are forwarded by the routing instance wx-multipath:

```
user@host# set interfaces wx-6/0/0 unit 0 family inet filter input
   classify-secondary
user@host# set firewall family inet filter classify-secondary term 1 from
   source-address 10.8.51.3
user@host# set firewall family inet filter classify-secondary term 1 then
   routing-instance wx–multipath
user@host# set firewall family inet filter classify-secondary term default then
   accept
```

3. Optionally, you can add an IP precedence or class-of-service DiffServ code point value to the firewall filter. For example, if the WXC ISM 200 is configured to mark packets for the secondary path with an IP precedence value of 2, use the following command to update the firewall filter:

   user@host# **set firewall family inet filter classify-secondary term 1 from precedence 2**

4. Define the routing instance wx-multipath to route the filtered packets to the appropriate WAN interface:

   user@host# **set routing-instances wx–multipath instance-type forwarding routing-options static route 0.0.0.0/32 next-hop 10.8.4.1 retain**

5. Import routes from default inet.0 routing table to the wx-multipath.inet routing table:

   user@host# **set routing-options interface-routes rib-group inet fb1**
   user@host# **set routing-options rib-groups fb1 import-rib [inet.0 wx-multipath.inet.0]**

6. On both the local WXC ISM 200 and the remote WX endpoint:

   a. Enable Multi-Path and configure an IP precedence or DSCP value as a supplemental marking method (optional).

   b. Define the appropriate traffic classes, and define Multi-Path templates that specify the preferred path (primary or secondary) for each traffic class.

   c. Apply a template to the remote WX endpoint, and specify the congestion and latency thresholds for each path.

   The router for the remote WX endpoint must also be configured to support Multi-Path. For more information about configuring Multi-Path, see the *WX/WXC Operator's Guide*.

Accessing the WXOS CLI

Use any of the following methods to access the WXOS CLI:

- From the JUNOS CLI, enter the following command, where *slot* is the higher number of the two slots occupied by the WXC ISM 200:

  user@host> **request wan-acceleration login fpc *slot***
  Copyright 2001-2007 Juniper Networks, Inc. All Rights Reserved.

  WXC-10.1.1.2#

  To view the slot number, enter the show chassis fpc pic-status command. Note that users require interface permission for read-only access, and interface-control and configure permission for read-write access.

- From the WXOS Web interface, select Admin>Tools>Command Line Interface. Some CLI commands cannot be entered from the Web interface (refer to the *WX/WXC Operator's Guide*).

Restarting WAN Acceleration and Enabling Trace Options

If you cannot access the WXC ISM 200, or the module is not responding, you can restart the WAN acceleration process (wxd) on the router:

```
user@host> restart wan-acceleration gracefully
```

If necessary, you can stop WAN acceleration temporarily by disabling the WAN acceleration process:

```
user@host# set system processes wan-acceleration disable
user@host# commit
```

To enable trace options for WAN acceleration:

```
user@host# set system processes wan-acceleration traceoptions flag <all |
   configuration | fpc-ipc | fpc-ipc-heartbeat | memory | ssam | wx-login>
user@host# commit
```

By default, the trace is saved in the /var/log/wxd file. Note that setting the all or fpc-ipc-heart-beat options will add a large volume of entries to the log file.

Upgrading the WXC ISM 200 Software

The procedure to upgrade the boot image on a WXC ISM 200 is the same as for upgrading a standalone WX device, Loading a boot image does not affect the configuration settings stored in the startup.cfg file. All configuration settings are preserved.

To load a new boot image on the WXC ISM 200:

1. Copy the new boot image to a local disk, an FTP server, or a TFTP server.
2. Select **Configuration > Quick Configuration > WAN Acceleration > Manage** in the J-Web interface to open the WXOS Web interface.
3. In the WXOS Web interface, select Admin>Load Boot Image.
4. On the Load Boot Image page, select the source of the boot image (Local Disk, TFTP server, or FTP server), specify the image location and filename, and click Load. Loading the boot image may take several minutes.
5. Select Reboot in the left-hand navigation frame, and click the Reboot button to activate the new system software.

Part 2
Index

Index

M

N

O

P

Q

R

S

T

U

V

W

Z