Juniper Networks

Application Acceleration Administration Guide

Release

6.1

Published: 2010-06-14

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

Application Acceleration Administration Guide

Revision History
June 2010—Revision 01

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 OS 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 website 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 xv

Objectives xv
Audience xv
Document Conventions xv
List of Technical Publications xvi
Requesting Technical Support xvii
Self-Help Online Tools and Resources xvii
Opening a Case with JTAC xvii

Part 1 Management of WXC Series Gateways

Chapter 1 **Introduction 3**

Application Acceleration Overview 3
Application Acceleration Technologies 3
WXC Features and Benefits 4
New Features in JWOS Release 6.1 4
Sample Deployments for WXC Series Gateways 5
Inline Deployment 5
Off-Path Deployment 6
Deployment with VPN Devices 6

Chapter 2 **Installing WXC Series Gateways 9**

Installation Overview for WXC Series Gateways 9
Preinstallation Tasks 9
Field-Replaceable Components 10
Interface Speeds and Modes 11
Installation Procedure 11
Inline and Off-Path WXC Installations 11
Installing a WXC590 Gateway 11
Installing a WXC2600 Gateway 15
Installing a WXC3400 Gateway 18
Running Quick Setup for a WXC Series Gateway 21
Postinstallation Tasks for a WXC Series Gateway 22

Chapter 3 **Configuring Setup Policies on WXC Series Gateways 23**

Using the JWOS Web Interface 23
Logging In 23
Understanding the JWOS Web Interface 24

Naming WXC Series Gateways and Other Objects 24
Configuring Basic WXC Setup Policies 25
Configuring the Name of a WXC Series Gateway 25
Configuring Bridge Interfaces for WXC Series Gateways 25
Configuring the Management Interface for WXC Series Gateways 27
Configuring the Domain Name for WXC Series Gateways 28
Configuring the Time for WXC Series Gateways 28
Obtaining a Permanent License for WXC Series Gateways 29
Configuring the Community for WXC Series Gateways 30
Configuring AAA for WXC Series Gateways 30
Defining Local User Accounts for WXC Series Gateways 30
Securing Front Panel Access for WXC Series Gateways 31
Configuring ARP for WXC Series Gateways 31
Configuring SNMP Support for WXC Series Gateways 32
Configuring Syslog Reporting for WXC Series Gateways 32
Configuring Packet Interception for WXC Series Gateways 33

Chapter 4 Configuring Acceleration Policies on WXC Series Gateways 35

Types of Application Acceleration 35
Overview of TCP Acceleration 35
Overview of Microsoft CIFS Acceleration 36
Configuring Application Policies for WXC Series Gateways 36
Configuring Application Definitions for WXC Series Gateways 37
Configuring SMB Signing for CIFS Acceleration 44

Chapter 5 Viewing Reports on WXC Series Gateways 47

Viewing and Printing WXC Reports 47
Executive Report on WXC Series Gateways 47
WAN Accelerated Throughput Report 49
WAN Application Summary Report on WXC Series Gateways 50
Compression Statistics 51
Compression Throughput Report on WXC Series Gateways 52
Compression Report on WXC Series Gateways 53
Compression by Endpoint Report on WXC Series Gateways 55
Compression Application Summary Report on WXC Series Gateways 56
Passthrough Report on WXC Series Gateways 58
TCP Connections Report on WXC Series Gateways 59

Chapter 6 Configuring Junos Pulse on WXC Series Gateways 61

Junos Pulse Client Hardware and Software Requirements 61
Installing the Junos Pulse Client 62
Downloading the Junos Pulse Client from a WXC Series Gateway 62
Downloading the Junos Pulse Client from a SA Series Gateway 63
Uninstalling the Junos Pulse Client 63
Managing Junos Pulse Client Software, Configurations, and Policies 63
Enabling Pulse Client Downloads from WXC Series Gateways 64
Enabling Pulse Client Adjacencies on WXC Series Gateways 64
Configuring Pulse Client Policies on WXC Series Gateways 64
Viewing the Status of Pulse Clients on WXC Series Gateways 65
Defining the Pulse Client Configuration on WXC Series Gateways 65

Viewing the Pulse Client Configuration on WXC Series Gateways 66
Uploading Pulse Client Software to WXC Series Gateways 66
Distributing the Pulse Client from WXC Series Gateways 67
Distributing the Pulse Client Through a SA Series Gateway 67
Distributing the Pulse Client Through SMS 68

Chapter 7 **Maintaining WXC Series Gateways 69**

Maintaining WXC Configurations and Software 69
Saving the WXC Configuration 69
Viewing the Configuration of WXC Series Gateways 70
Loading a Configuration File on WXC Series Gateways 70
Loading a Software Package on WXC Series Gateways 72
Clearing Monitoring Statistics on WXC Series Gateways 73
Restoring the Factory Default Configuration on WXC Series Gateways 73
Rebooting the WXC Gateway 74
Using Maintenance Tools 74
Using the Ping Utility on WXC Series Gateways 75
Using the Traceroute Utility on WXC Series Gateways 75
Using the Packet Capture Utility on WXC Series Gateways 76
Viewing and Saving System Logs on WXC Series Gateways 77
Viewing and Saving Access Control Logs on WXC Series Gateways 77
Exporting Performance Data on WXC Series Gateways 77
Creating a Diagnostic File on WXC Series Gateways 78
Viewing Flow Diagnostics on WXC Series Gateways 78
Troubleshooting Passthrough Mode on WXC Series Gateways 80
Detecting Passthrough Mode 80
Using the WXC Web Interface to Recover from Passthrough Mode 81
Using the WXC Console to Recover from Passthrough Mode 81

Part 2 Specifications

Appendix A **Specifications for WXC Series Gateways 85**

WXC Platform Specifications 85
General Specifications for All WXC Series Gateways 85
Specifications for WXC590, WXC2600, and WXC3400 87
DB9 Console Port Pinouts on WXC Series Gateways 88

Appendix B **SNMP Traps and Syslog Messages on WXC Series Gateways 91**

System Events and SNMP Traps for WXC Series Gateways 91
Syslog Message Format for WXC Series Gateways 93

Appendix C **Data Exported from WXC Series Gateways 95**

Performance Statistics Exported from WXC Series Gateways 95
General Device Information 95
Data Section Information 96
System Session Statistics 96
Compression Statistics 97
WAN Performance Statistics 98
TCP Flow Statistics 98
Flow Diagnostics Exported from WXC Series Gateways 99

Appendix D **Certifications for WXC Series Gateway 105**

Certifications for WXC Series Gateways 105
Product Reclamation and Recycling Program 106

Appendix E **Copyrights 109**

Traceroute Copyright License 109
OpenSSL Copyright License 110
GNU GENERAL PUBLIC LICENSE 112

Part 3 Index

Index 121

List of Figures

Part 1 Management of WXC Series Gateways

Chapter 1 **Introduction 3**

Figure 1: Typical Inline Deployment of WXC Series Gateways 6
Figure 2: Off-Path Deployment of WXC Series Gateways 6
Figure 3: WXC Series Gateways in a VPN Configuration 7

Chapter 2 **Installing WXC Series Gateways 9**

Figure 4: WXC590 Front Panel 12
Figure 5: Link and Speed LEDs on the WXC590 14
Figure 6: WXC2600 Front Panel 15
Figure 7: Link and Speed LEDs on the WXC2600 17
Figure 8: WXC3400 Front Panel 18
Figure 9: Link and Speed LEDs on the WXC3400 20

Chapter 3 **Configuring Setup Policies on WXC Series Gateways 23**

Figure 10: JWOS Web Interface 24

Chapter 5 **Viewing Reports on WXC Series Gateways 47**

Figure 11: Executive Report 48
Figure 12: WAN Accelerated Throughput Report 50
Figure 13: WAN Application Summary 51
Figure 14: Compression Throughput Report 52
Figure 15: Compression Report 54
Figure 16: Compression by Endpoint Report 56
Figure 17: Compression Application Summary 57
Figure 18: Passthrough Report 58
Figure 19: TCP Connections Report 60

List of Tables

About This Guide xv

Table 1: Notice icons xvi
Table 2: Text Conventions xvi
Table 3: GUI Conventions xvi

Part 1 Management of WXC Series Gateways

Chapter 3 Configuring Setup Policies on WXC Series Gateways 23

Table 4: WXC Interface Names 26

Chapter 4 Configuring Acceleration Policies on WXC Series Gateways 35

Table 5: Default Application Definitions 41
Table 6: ToS and DSCP Values 43

Chapter 7 Maintaining WXC Series Gateways 69

Table 7: Passthrough Error Messages 80

Part 2 Specifications

Appendix A Specifications for WXC Series Gateways 85

Table 8: General Specifications for All WXC Platforms 85
Table 9: WXC Family Specifications 87
Table 10: Pinouts for DB9-to-DB9 Cable 88
Table 11: Pinouts for DB9-to-DB25 Cable 89

Appendix B SNMP Traps and Syslog Messages on WXC Series Gateways 91

Table 12: System Events and SNMP Traps 91

Appendix C Data Exported from WXC Series Gateways 95

Table 13: General Device Information 95
Table 14: Data Section Information 96
Table 15: System Session Statistics 96
Table 16: Compression Session Statistics 97
Table 17: WAN Performance Statistics 98
Table 18: TCP Flow Statistics 98
Table 19: Flow Diagnostics 99

Appendix D Certifications for WXC Series Gateway 105

Table 20: Certifications for WXC Series Gateways 105

About This Guide

- Objectives on page xv
- Audience on page xv
- Document Conventions on page xv
- List of Technical Publications on page xvi
- Requesting Technical Support on page xvii

Objectives

This guide describes how to use the JWOS Web interface to configure, monitor, and manage the Juniper Networks WXC Application Acceleration gateways and their remote Junos Pulse clients.

To manage WXC Series gateways through the JWOS command-line interface (CLI), see the *JWOS Command Reference Guide*.

Audience

This guide is intended for administrators who configure and manage WXC Series gateways. Be sure you are familiar with your network architecture and devices and that you can perform basic network configuration procedures.

Document Conventions

Table 1 on page xvi defines notice icons used in this guide, Table 2 on page xvi defines text conventions used throughout the book, and Table 3 on page xvi defines the GUI conventions.

Table 1: Notice icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates that you may risk losing data or damaging your hardware.
	Warning	Alerts you to the risk of personal injury.

Table 2: Text Conventions

Convention	Description
Sans serif type	Filenames and directory names.
Italics	• Terms defined in text. • Variable elements for which you supply values. • Book titles.
+ (plus sign)	Key names linked with a plus sign indicate that you must press two or more keys simultaneously.

Table 3: GUI Conventions

Convention	Description
> (right angle bracket)	Navigation paths through the UI.
Bold type	User interface elements that you select in a procedure, such as tabs, buttons, and menu options.
Italics	Variables for which you supply values.

List of Technical Publications

The following additional documents are available at http://www.juniper.net/techpubs:

- *JWOS Command Reference Guide*—Describes how to use the CLI interface to configure the WXC Series gateways.
- *Junos Pulse Administration Guide*—Describes how to configure and distribute the Junos Pulse client from a Juniper Networks Infranet Controller or Juniper Networks SA Series SSL VPN Appliance. Online help provided with the Junos Pulse client describes how to use the features available to the end user, such as viewing the client status.

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/us/en/local/pdf/resource-guides/7100059-en.pdf .
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/ .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

PART 1

Management of WXC Series Gateways

- Introduction on page 3
- Installing WXC Series Gateways on page 9
- Configuring Setup Policies on WXC Series Gateways on page 23
- Configuring Acceleration Policies on WXC Series Gateways on page 35
- Viewing Reports on WXC Series Gateways on page 47
- Configuring Junos Pulse on WXC Series Gateways on page 61
- Maintaining WXC Series Gateways on page 69

CHAPTER 1

Introduction

This chapter introduces the WXC Series application acceleration gateways, and describes the new features in this release.

- Application Acceleration Overview on page 3
- Sample Deployments for WXC Series Gateways on page 5

Application Acceleration Overview

Application traffic can be accelerated between Juniper Networks WXC Series gateways (typically installed in a data center), and remote Windows computers that have the Junos Pulse client installed.

The WXC Series gateway must be a WXC3400, WXC2600, or a WXC590 running JWOS 6.1 or higher. The Junos Pulse client must be installed on computers running Windows 7, Windows Vista, or Windows XP.

- Application Acceleration Technologies on page 3
- WXC Features and Benefits on page 4
- New Features in JWOS Release 6.1 on page 4

Application Acceleration Technologies

The following technologies are used to compress and accelerate application traffic:

- **LZ compression**—A memory-based compression algorithm that locates repeated data patterns at the byte level, in real time, across all IP application sessions. Repeated patterns are sent as symbols, which the remote endpoint decompresses (restores) from a shared dictionary. The reduction in traffic effectively increases the WAN bandwidth, reduces network congestion, and improves overall data flow.
- **TCP acceleration**—While compression effectively increases available bandwidth, TCP acceleration improves TCP application performance where the use of available bandwidth is constrained by network latency, such as on low-speed remote-access connections.
- **CIFS acceleration**—An application-level acceleration method that accelerates Microsoft Common Internet File System (CIFS) traffic.

WXC Features and Benefits

WXC Series gateways and Junos Pulse clients enable networks to achieve maximum capacity over WAN links. The primary features and benefits include:

- **Substantial throughput gain**—Greatly improves WAN capacity, accelerates TCP applications in high-latency environments, and reduces the load on other network devices.
- **Immediate impact with autodiscovery**—Gains are realized immediately. The WXC Series gateways and Junos Pulse clients discover each other automatically, and dynamically form an *adjacency* to accelerate the traffic between them.
- **Transparent**—Operates transparently to existing network equipment, topologies, and WAN interfaces (such as Frame Relay, MPLS, and ATM). No network or application modifications are required.
- **Application independent**—Works on any TCP-based application (such as email, database, Web, ERP, and so on). Uses open standard protocols.
- **QoS interoperable**—Preserves QoS priority levels within your network.
- **Fail-safe nonstop operation**—Traffic is passed through on any hardware or software disruption, including power loss.
- **Easily managed**—Provides administrative access through an intuitive Web user interface (SSL) and a CLI using SSH. You can also monitor performance through an SNMP-based management system.
- **VPN and firewall friendly**—Installs on the LAN side of encryption devices to work seamlessly with virtual private networks (VPNs) and firewalls.
- **Secure**—Provides confidentiality and message integrity for WAN traffic.

New Features in JWOS Release 6.1

JWOS Release 6.1 includes the following new features:

- **Scalability enhancements**—The JWOS-compatible WXC Series gateways now support up to 1000 Junos Pulse clients (see the following table), and the user interface is enhanced so that long lists are easier to view and navigate.

WXC Series Gateway	Junos Pulse Clients
WXC3400	1000
WXC2600	250
WXC590	100

- **Junos Pulse Client**—The WX Client has been replaced by the integrated Junos Pulse client for Application Acceleration services. The Junos Pulse client also includes secure network access services, and can be downloaded from a WXC Series gateway, an IC

Series gateway, or an SA Series gateway. The Pulse client includes the following enhancements:

- Support for Windows 7, Windows Vista, and Windows XP (Windows 2000 is no longer supported)
- Changes to acceleration policies on the WXC Series gateway are propagated to the Junos Pulse clients when a new connection (adjacency) is established.
- Nonadministrative users can install Junos Pulse if the Juniper Installation Service (JIS) is installed on their Windows system (available from IC Series and SA Series gateways).

Junos Pulse is NOT a feature-for-feature replacement for the WX Client. Please refer to the *Junos Pulse Client Migration Guide* for feature comparisons between Junos Pulse and the legacy WX Client. For more information about Junos Pulse 1.0, see the *Junos Pulse Release Notes* and the *Junos Pulse Administration Guide*.

- **LZ compression**—Memory-based Lev-Zempel (LZ) compression provides first pass performance improvements through reduced bandwidth utilization - critical for mobile users.
- **Compatibility with previous releases**— Any WXC590, WXC2600, or WXC3400 that has WXOS 5.6.5 or higher can be upgraded to JWOS 6.1. However, traffic can be accelerated only between Junos Pulse clients and a WXC Series gateway running JWOS 6.1 or higher. Junos Pulse clients cannot form adjacencies with WXC Series gateways that are running JWOS 6.0 or any version of WXOS.

  To upgrade from JWOS 6.0 to JWOS 6.1, you must first downgrade to WXOS (see the *JWOS 6.1 Release Notes*).

Related Topics
- WXC Platform Specifications on page 85

Sample Deployments for WXC Series Gateways

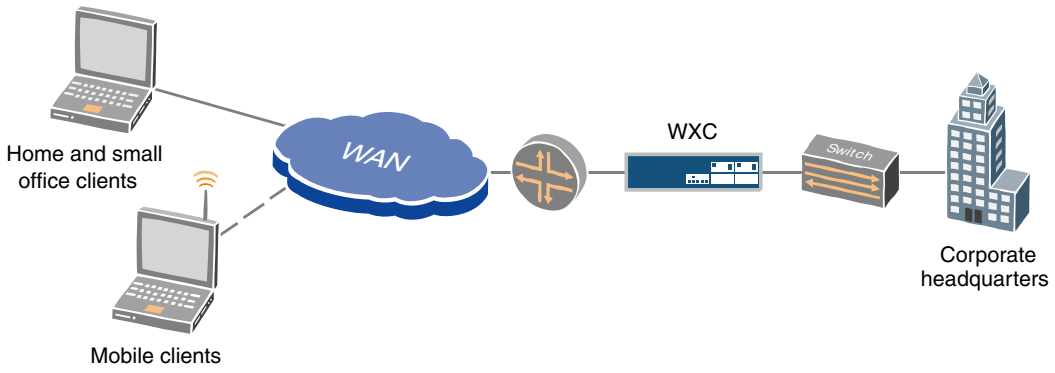
The following topics provide sample deployment topologies for WXC Series gateways:

- Inline Deployment on page 5
- Off-Path Deployment on page 6
- Deployment with VPN Devices on page 6

Inline Deployment

When the Junos Pulse client is installed on Windows workstations, WAN traffic can be accelerated from the Pulse clients to a remote WXC Series gateway installed on the other side of the WAN. Typically, WXC Series gateways are deployed in the data path between a LAN switch and an edge router (see Figure 1 on page 6).

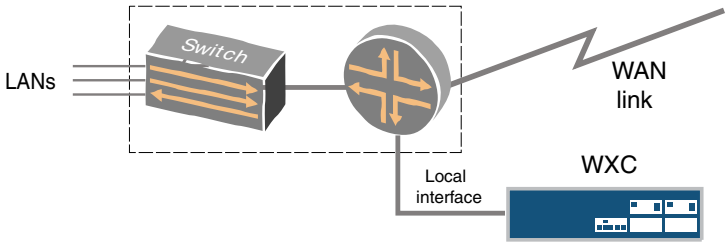
Figure 1: Typical Inline Deployment of WXC Series Gateways



Off-Path Deployment

WXC Series gateways are usually deployed in the physical data path between a LAN switch and a WAN edge router, with no changes to Layer 3 routing. When interrupting the data path is not practical, such as in collapsed backbone environments where the switch and the router are the same physical device, you can deploy the WXC gateway off path (see Figure 2 on page 6). In this case, the Local interface is connected to the switch or the router, and the Remote interface is not used. (We recommend connecting the Local interface directly to the router.)

Figure 2: Off-Path Deployment of WXC Series Gateways

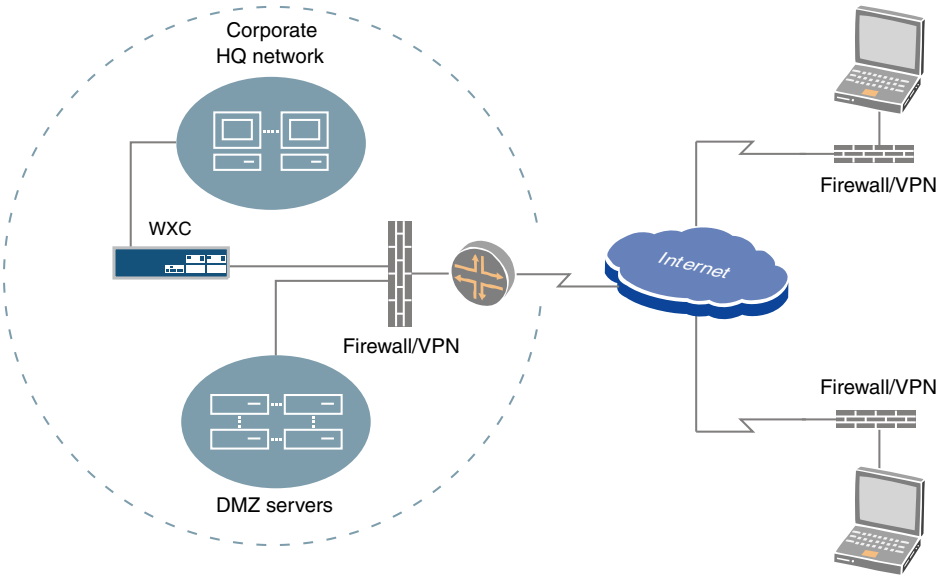


Deployment with VPN Devices

WXC Series gateways operate transparently relative to existing network equipment, including firewalls and VPN devices (see Figure 3 on page 7). By compressing data before it enters the VPN tunnel, the WXC Series gateways and Pulse clients reduce the workload for the VPN devices. The same bandwidth multiplication effect is achieved for VPN encapsulated traffic as for unencapsulated traffic.

NOTE: The WXC Series gateways do not support Network Address Translation (NAT). If NAT is enabled on the local firewall, all traffic is passed through without any processing.

Figure 3: WXC Series Gateways in a VPN Configuration



CHAPTER 2

Installing WXC Series Gateways

- Installation Overview for WXC Series Gateways on page 9
- Installing a WXC590 Gateway on page 11
- Installing a WXC2600 Gateway on page 15
- Installing a WXC3400 Gateway on page 18
- Running Quick Setup for a WXC Series Gateway on page 21
- Postinstallation Tasks for a WXC Series Gateway on page 22

Installation Overview for WXC Series Gateways

- Preinstallation Tasks on page 9
- Field-Replaceable Components on page 10
- Interface Speeds and Modes on page 11
- Installation Procedure on page 11
- Inline and Off-Path WXC Installations on page 11

Preinstallation Tasks

Before you begin, complete the following preinstallation tasks:

- Ensure that sufficient power is available and that power supply circuits are protected by a 15A or 20A circuit breaker.
- Ensure there is ample space and lighting. You need enough space to connect one or two CAT-5 UTP Ethernet data cables and one or two power cords to the back of the chassis, as well as enough lighting to see the LEDs on the data ports.
- Provide a minimum of 6 inches of clearance in the front and back of the chassis. For a WXC590, provide 3 inches of clearance on both sides of the chassis to allow cooling air to be drawn through the side panels. Do not install one WXC Series gateway directly behind another, which can cause warm or hot air to be recirculated. There are no ventilation requirements above or below the gateway.
- Ensure that paper materials or heavy equipment are not stacked on top of a WXC Series gateway.
- For rack-mount installations, reserve sufficient space for each form factor, as follows:

  - 1 U — WXC2600
  - 2 U — WXC590 and WXC3400
- Identify a 10/100 or 10/100/1000 Ethernet LAN port where you can connect the WXC Series gateway. This port is typically on an aggregation switch or another LAN device that is connected directly to the WAN router.
- Log in to the router that will be on the WAN side of the WXC Series gateway and note the interface speed and duplex mode.
- On all firewall and antivirus software between the WXC Series gateways and Pulse clients, note the following:
  - TCP/UDP ports 3577 and 3578 and UDP port 3579 must be open. For example, if Kaspersky software is installed on a Pulse client, it must be configured to allow traffic on UDP port 3578.
  - If the WXC Series gateway is installed in the DMZ, and you plan to upgrade the JWOS software using FTP, you must open an FTP port in the firewall between the DMZ and the intranet.
  - Network Address Translation (NAT) is not supported. If NAT is enabled on the local firewall, all traffic is passed through without any optimization.
  - TCP options must NOT be stripped from SYN or SYN-ACK packets. TCP options are required to form adjacencies between the WXC Series gateway and the Pulse clients.
- Reserve an IP address for the WXC Series gateway and identify the default gateway. The default gateway is the next hop on the WAN side of the WXC Series gateway.

CAUTION: Special packaging material is provided to protect the WXC systems during shipping. Retain the packing material in case the unit needs to be shipped again for any reason. Shipping the unit without the original packaging material voids the warranty.

WARNING: WXC Series gateways have no user-serviceable parts. Opening the chassis voids the warranty. As a safety caution, note that opening the chassis exposes a lithium battery. If you attempt to remove or replace the lithium cell, do not use a conductive instrument because a short-circuit can cause the cell to explode. A replacement cell must be of the same type (CR2032). Dispose of a spent cell promptly. Do not recharge, disassemble, or incinerate spent cells. Keep cells away from children.
For additional general safety recommendations and warnings, see the *Security Products Safety Guide*.

Field-Replaceable Components

The fans, disk drives, and power supplies can be replaced on WXC590, WXC2600, and WXC3400 gateways. Do not remove a disk drive while the power is on. Doing so disables the drive. If a drive is removed while the system is running, reboot the system to reactivate the drive.

After you replace a failed drive, enter the following CLI command to activate the drive:

```
config set disk activate
```

For more information about replacing the disk drives, see *WXC590 Field-Replaceable Units Removal and Installation* and *WXC2600 and WXC3400 Field-Replaceable Units Removal and Installation*.

Interface Speeds and Modes

Interface speed and duplex settings should be the same across all devices: the switch, the WXC Local and Remote interfaces, and the router. This ensures connectivity through the WXC Series gateway in case of a power loss or a condition that causes a hardware bypass.

Installation Procedure

Installation of a WXC Series gateway consists of the following steps:

1. Install the hardware, apply power, and configure the network settings, such as the IP address.
2. Run Quick Setup to define the required configuration settings (see "Running Quick Setup for a WXC Series Gateway" on page 21).
3. Perform postinstallation tasks for optional configuration settings (see "Postinstallation Tasks for a WXC Series Gateway" on page 22).

Inline and Off-Path WXC Installations

WXC Series gateways are usually installed in the data path (inline) between a LAN switch (or other aggregation device) and the WAN edge router. If interrupting the data path is not practical, such as in collapsed-backbone environments, you can deploy the gateway off path.

The installation instructions describe how to install a WXC Series gateway in the data path. To install a WXC gateway off path, note the following:

- Do not disconnect any cables. Simply connect the Local interface of the WXC Series gateway to the switch or the router. We recommend connecting directly to the router. Set the Local interface to full-duplex mode (half-duplex mode can cause excessive collisions).
- Do not connect the Remote interface to the router. The Remote interface is not used, so you can apply power without first verifying connectivity between the LAN and the router.
- After you run Quick Setup, configure packet interception to route traffic to the off-path WXC Series gateway (see "Configuring Packet Interception for WXC Series Gateways" on page 33).

Installing a WXC590 Gateway

To install a WXC590 in your network:

1. Set up the chassis in one of the following ways:

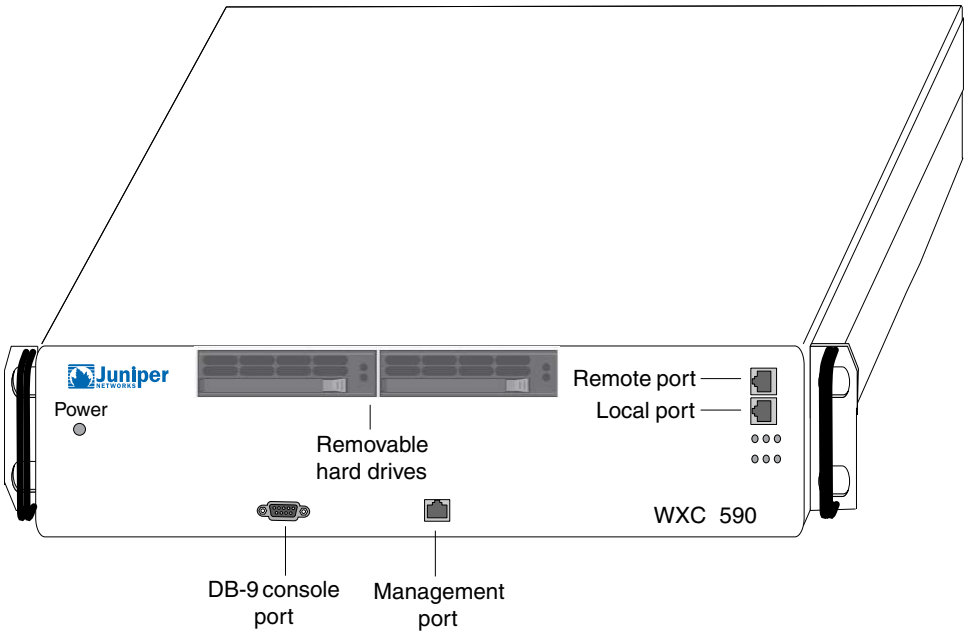
   - To install the WXC590 in a 19-inch rack, first install the supplied brackets (front panel forward) to the sides of the chassis with the countersunk screws provided, and then install the chassis in your network rack.
   - To install the WXC590 on a desktop, place the chassis upside down on a smooth, flat surface, and install the supplied rubber feet on the bottom of the chassis. Place the chassis on a desktop or on top of another device so that all four rubber feet are secure on the flat surface.

NOTE: Do not connect the power until Step 4.

2. Connect the network cables and verify connectivity.

   The standard WXC590 has two 10/100/1000 autosensing Ethernet interfaces (see Figure 4 on page 12).

Figure 4: WXC590 Front Panel



To connect the network cables to the WXC590:

a. Locate the cable that connects the switch (or other aggregating device) to the router.

b. Disconnect this cable from the router port and connect it to the Local port on the WXC590.

c. Connect a crossover cable (not provided) from the router port to the Remote port on the WXC590.

d. (Optional) Connect a straight-through cable from the MGT port on the WXC590 to your management network.

3. Use one of the following methods to verify connectivity across the WXC590 when the power is off. This step ensures that the correct cables are used and that traffic is passed through the WXC590 during a power loss.
   - Ping a host on the remote side of the WXC590 from a host on the local side of the WXC590.
   - Observe the link status LEDs (if available) on the interfaces of the adjacent network devices (switch and router).
4. Connect the supplied power cords to the dual power supplies on the back of the chassis, and then connect the power cords to the local power source.

   The maximum power usage for a WXC590 is 300 W or 1025 BTU/hour.

WARNING: The appliance is designed to work with IT power systems. Because the appliance has more than one power supply connection, you must remove all connections completely to remove power from the unit.

5. Connect an ANSI-compatible terminal to the serial console port on the front of the WXC590 (see Figure 4 on page 12).

NOTE: The serial console port is of type RS-232 (AT-compatible) with a male DB-9 connector. You should use a female/female DB-9 crossover cable (such as a null-modem cable) when connecting directly to a PC serial port. The pinouts for the console port are shown in “DB9 Console Port Pinouts on WXC Series Gateways” on page 88.

6. Verify the following serial port settings:
   - Baud rate: 9600 bps
   - Data bits: 8
   - Parity: none
   - Stop bits: 1
   - Flow control: none
7. Start a terminal emulation program (such as HyperTerminal), and connect through the serial port.
8. Type **admin** for the username and **juniper** for the password.
9. Press Enter and enter the following network information at the prompts:
   a. Type an IP address for the WXC590, and then press Enter.
   b. Type the subnet mask for the network, and then press Enter.
   c. Type the default gateway address, and then press Enter.

The default gateway is typically the next hop on the Remote side of the WXC590.

d. Press Enter to confirm the network settings.

10. By default, the Local and Remote interfaces are set to autonegotiate the speed and duplex mode. However, to avoid problems when the switch or router speed and duplex mode are set manually, we strongly recommend that you manually configure the Local and Remote interface settings.

    To manually configure the interface settings:

    a. At the prompt to configure the interface settings, type **y** and press Enter.

    b. Enter a number (0 to 5) for the speed and mode of the Local interface.

    0 - 10-full
    1 - 10-half
    2 - 100-full
    3 - 100-half
    4 - 1000-full
    5 - auto

    Press Enter to confirm the setting, and then repeat for the Remote interface.

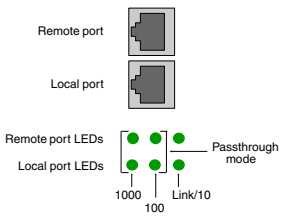
11. Continue with the Quick Setup, or press Enter at each prompt and run Quick Setup from the Web interface. Note that the last prompt is to save the configuration as **startup.cfg**, which is used when you reboot the gateway.

12. Observe the LEDs below the Ethernet ports (see Figure 5 on page 14). Note the following:

    - The link LEDs indicate the port is connected properly.
    - The 100 and 1000 LEDs indicate the interface speed in Mbps. If the 100 and 1000 LEDs are off, the port is running at 10 Mbps.
    - If all four 100 and 1000 LEDs are on, the system is in passthrough mode. This occurs during a restart or system failure (the default).

      In high-availability environments, you can disable hardware passthrough by entering the **config set system no-bypass-capability** command (see the *JWOS Command Reference Guide*). This command blocks traffic through the WXC during a restart or a system failure so that the traffic can be routed to an alternate device.

Figure 5: Link and Speed LEDs on the WXC590



NOTE: The LEDs on the hard drives do not light up during operation.

The installation is complete. You can now run Quick Setup as described in “Running Quick Setup for a WXC Series Gateway” on page 21.

Installing a WXC2600 Gateway

To install the WXC2600 in your network:

1. Set up the chassis in one of the following ways:
   - To install the WXC2600 in a 19-inch rack, first install the supplied brackets (front panel forward) to the sides of the chassis with the countersunk screws provided, and then install the chassis in your network rack.
   - To install the WXC2600 on a desktop, place the chassis on a desktop or on top of another device.

NOTE: Do not connect power until Step 4.

2. Connect the network cables.

   The WXC2600 has two 10/100/1000 Ethernet interfaces on the front panel labeled Local and Remote (see Figure 6 on page 15), plus a management port (MGT). A high-availability port and USB port are provided for future use (not currently supported).

   To connect the network cables:

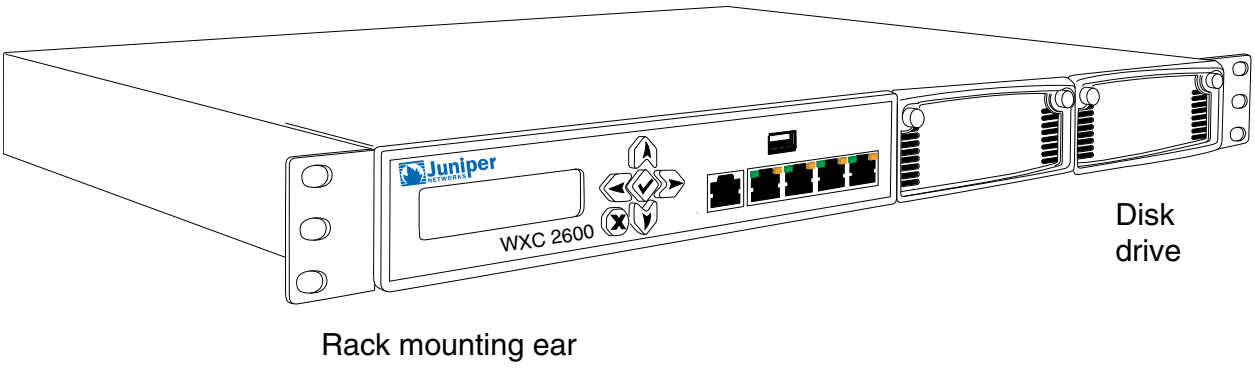
   a. Locate the cable that connects the switch (or other aggregating device) to the router.

   b. Disconnect this cable from the router and connect it to the Local port on the WXC2600.

   c. Connect the crossover cable from the router port to the Remote port on the WXC2600.

   d. (Optional) Connect a straight-through cable from the MGT port on the WXC2600 to your management network.

Figure 6: WXC2600 Front Panel



3. Use one of the following methods to verify connectivity across the WXC2600 when the power is off. This step ensures that the correct cables are used and that traffic is passed through during a power loss.
   - Ping a host on the remote side of the WXC2600 from a host on the local side of the WXC2600.
   - Observe the link status LEDs (if available) on the interfaces of the adjacent network devices (switch and router).
4. Connect the power supply to the back of the chassis, and then connect the power cord to the local power source.

NOTE: The maximum power usage is 300 W or 1025 BTU/hour.

5. Use the front-panel keypad and LCD to configure the network settings:
   a. Press the Enter button (center button).
   b. Press Enter at the **Select Setup Network** prompt in the LCD.
   c. Use the front-panel keypad to assign an IP address, subnet mask, and default gateway:
      - Use the Up and Down Arrow buttons to display a number (between 0-9). Use the Left and Right Arrow buttons to move to the previous or next character.
      - Press Enter after each of the three settings. To discard all changes and start over, press the X button.
      - After you enter the gateway address, use the Left Arrow button to select **Save & Reboot**, and press Enter.

NOTE: The default gateway is typically the next hop on the Remote side of the gateway.

6. After the reboot, specify the speed and mode of each interface. By default, the Local and Remote interfaces are set to autonegotiate. However, to avoid problems when the switch or router speed and duplex mode are set manually, we strongly recommend that you manually configure the Local and Remote interface settings.

   To configure the interfaces from the front panel:
   a. Press Enter to display the **Setup Network_** prompt in the LCD.
   b. Use the Down Arrow button to show the Local If Settings menu option, and press Enter.
   c. Use the Left Arrow button to select **y**, and press Enter.

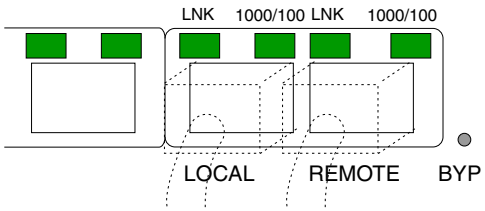
d. Use the Down Arrow button to show the desired speed and duplex setting, and press Enter. The options are 10/Half, 10/Full, 100/Half, 100/Full, 1000/Full, Auto-Negotiate.

e. Use the Left Arrow button to select **Commit&Save**, and press Enter. Repeat this process for the Remote interface.

NOTE: After installation, you can change the interface settings from the Web interface or the CLI.

7. Observe the LEDs above the Local and Remote ports (see Figure 7 on page 17). Note the following:
   - The link LEDs indicate the port is connected properly.
   - The 1000/100 LEDs indicate the interface speed: yellow for 1000 Mbps, green for 100 Mbps, or off for 10 Mbps.

Figure 7: Link and Speed LEDs on the WXC2600



8. View the other LEDs on the front panel.

Front Panel LED	Description
POWER	Indicates that power is on.
BYP	Indicates whether traffic is being processed, passed through, or blocked. • **Green**. Traffic is being processed (normal operation). • **Orange**. All traffic is passing through without any processing (hardware passthrough). This occurs during a restart or system failure when the bypass capability is enabled (the default). • **Off**. All traffic through the gateway is blocked. This occurs during a restart or system failure when the bypass capability (hardware passthrough) is disabled. In high-availability environments, you can disable hardware passthrough by entering the **config set system no-bypass-capability** command (see the *JWOS Command Reference Guide*). This command blocks traffic during a restart or system failure so that the traffic can be routed to an alternate device.

The installation is complete. You can now run Quick Setup, as described in “Running Quick Setup for a WXC Series Gateway” on page 21.

Installing a WXC3400 Gateway

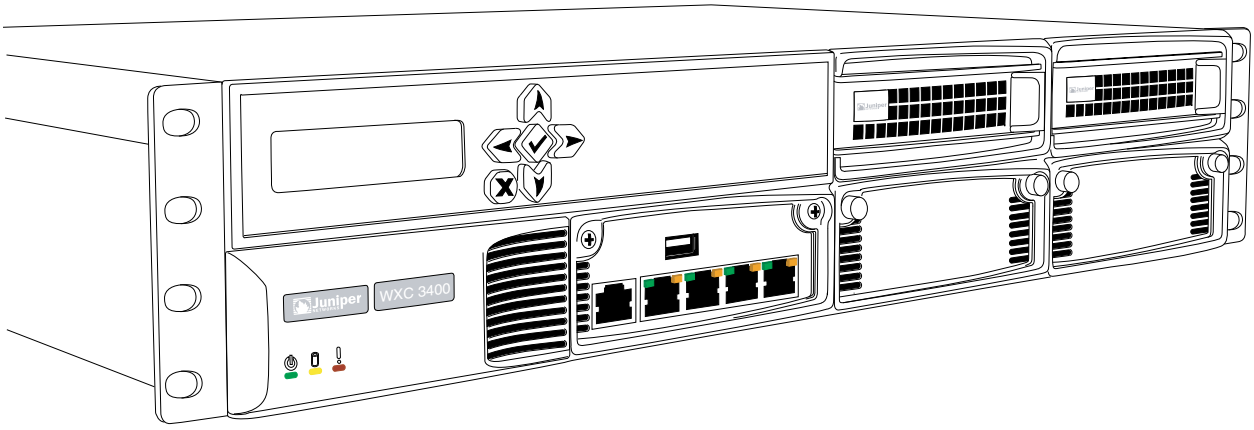
To install the WXC3400 in your network:

1. Set up the chassis in one of the following ways:
   - To install the WXC3400 in a 19-inch rack, first install the supplied brackets (front panel forward) to the sides of the chassis with the countersunk screws provided, and then install the chassis in the network rack.
   - To install the WXC3400 on a desktop, place the chassis on a desktop or on top of another device.
2. Connect the network cables.

NOTE: Do not connect power until Step 4.

The WXC3400 has two 10/100/1000 Ethernet interfaces on the front panel labeled Remote and Local (see Figure 8 on page 18), plus a management port (MGT). A high-availability port and USB port are provided for future use (not currently supported).

Figure 8: WXC3400 Front Panel



Rack mounting ear

To connect the network cables:

a. Locate the cable that connects the switch (or other aggregating device) to the router.

b. Disconnect this cable from the router and connect it to the Local port on the WXC3400.

c. Connect the crossover cable from the router port to the Remote port on the WXC3400.

d. (Optional) Connect a straight-through cable from the MGT port on the WXC3400 to your management network.

3. Use one of the following methods to verify connectivity across the WXC3400 when the power is off. This step ensures that the correct cables are used and that traffic passes through the gateway during a power loss.

   - Ping a host on the remote side of the WXC3400 from a host on the local side of the WXC3400.
   - Observe the link status LEDs (if available) on the interfaces of the adjacent network devices (switch and router).

   Connect the power cables to the two power supplies on the back of the chassis (a second power supply is optional), and then connect the cables to the local power source.

   If you have two power supplies and one of them fails, the other one can provide full power indefinitely. You can replace the failed power supply while the system is running.

   The WXC3400 maximum power usage is 400 W or 1370 BTU/hour.

WARNING: The appliance is designed to work with IT power systems. Because the appliance has more than one power supply connection, you must remove all connections completely to remove power from the unit.

4. Use the front-panel keypad and LCD to configure the network settings:

   a. Press the Enter button (center button).

   b. Press Enter at the **Select Setup Network** prompt in the LCD.

   c. Use the front-panel keypad to assign an IP address, subnet mask, and default gateway:

      - Use the Up and Down Arrow buttons to display a number (between 0-9). Use the Left and Right Arrow buttons to move to the previous or next character.
      - Press Enter after each of the three settings. To discard all changes and start over, press the X button.
      - After you enter the gateway address, use the Left Arrow button to select **Save & Reboot**, and press Enter.

NOTE: The default gateway is typically the next hop on the Remote side of the gateway.

5. After the reboot, specify the speed and mode of each interface. By default, the Local and Remote interfaces are set to autonegotiate. However, to avoid problems when

the switch or router speed and duplex mode are set manually, we strongly recommend that you manually configure the Local and Remote interface settings.

To configure the interfaces from the front panel:

a. Press Enter to display the **Setup Network_** prompt in the LCD.

b. Use the Down Arrow to show the Local If Settings menu option, and press Enter.

c. Use the Left Arrow to select **y**, and press Enter.

d. Use the Down Arrow to show the desired speed and duplex setting, and press Enter. The options are 10/Half, 10/Full, 100/Half, 100/Full, 1000/Full, Auto-Negotiate.

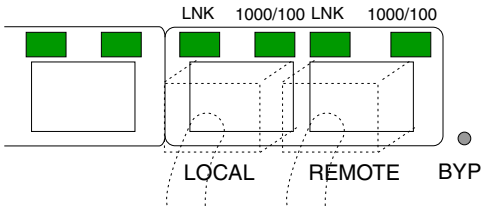
e. Use the Left Arrow to select **Commit&Save**, and press Enter. Repeat this process for the Remote interface.

NOTE: After installation, you can change the interface settings from the Web interface or CLI.

6. Observe the LEDs above the Local and Remote ports (see Figure 9 on page 20). Note the following:

   - The link LEDs indicate the port is connected properly.
   - The 1000/100 LEDs indicate the interface speed: yellow for 1000 Mbps, green for 100 Mbps, or off for 10 Mbps.

Figure 9: Link and Speed LEDs on the WXC3400



7. Observe the other LEDs on the front panel.

Front Panel LED	Description
POWER	Indicates that power is on.
DISK	Indicates disk drive activity.
FAULT	Indicates a system failure.

Front Panel LED	Description
BYP	Indicates whether traffic is being processed, passed through, or blocked: • **Green**. Traffic is being processed (normal operation). • **Orange**. All traffic is passing through without any processing (hardware passthrough). This occurs during a restart or system failure when the bypass capability is enabled (the default). • **Off**. All traffic through the gateway is blocked. This occurs during a restart or system failure when the bypass capability (hardware passthrough) is disabled. In high-availability environments, you can disable hardware passthrough by entering the **config set system no-bypass-capability** CLI command (see the *JWOS Command Reference Guide*). This command blocks traffic through the WXC gateway during a restart or system failure so that traffic can be routed to an alternate device.

The installation is complete. You can now run Quick Setup, as described in "Running Quick Setup for a WXC Series Gateway" on page 21.

Running Quick Setup for a WXC Series Gateway

After you start a WXC Series gateway and configure network settings, you can run the Quick Setup program. The first time you log in to the Web interface, the Quick Setup program starts automatically and guides you through the required configuration steps. All settings made during Quick Setup can be changed later.

You can log in to the JWOS Web interface from any computer in your network. Data is securely transmitted through HTTPS. The JWOS Web interface has the following requirements:

- Microsoft Internet Explorer version 7.0 or 8.0, or Mozilla Firefox 3.0, 3.5, or 3.6.
- Monitor display settings of 1024 x 768 or higher.

To run Quick Setup from the Web interface:

1. Verify that the browser accepts cookies (required to log in) and that the server is always checked for the latest configuration information. Privacy and security settings should be medium or lower.
2. In the browser's Address field, enter the URL for the WXC gateway's IP address in the following format:

   https://*IP address of the WXC gateway*
3. If the Security Alert dialog box appears, click **Yes** to proceed.
4. On the Login page, type **admin** for the username and **juniper** for the password, and click **Login**.
5. Click **Next** to open the Bridge Interfaces page.

6. If necessary, change the IP address, subnet mask, or default gateway address that were entered for the **br-0/0** bridge interface during the initial setup. You can also change the speed and mode of the Local and Remote interfaces.
7. Click **Finish**.

The initial configuration is complete. For a list of key configuration tasks, see "Postinstallation Tasks for a WXC Series Gateway" on page 22.

Postinstallation Tasks for a WXC Series Gateway

After you run Quick Setup, you can continue configuring the WXC Series gateway through the Web interface or through the CLI.

- To use the Web interface, see "Using the JWOS Web Interface" on page 23.
- To use the CLI, see the *JWOS Command Reference Guide*.

Be sure to review the following key configuration tasks:

- Set the time manually, or specify an NTP server, as described in "Configuring the Time for WXC Series Gateways" on page 28.
- Change the default password for the **admin** account, as described in "Defining Local User Accounts for WXC Series Gateways" on page 30.
- Review the application definitions provided and add any new ones needed for your network, as described in "Configuring Application Definitions for WXC Series Gateways" on page 37.
- Configure acceleration for the appropriate applications, as described in "Configuring Application Policies for WXC Series Gateways" on page 36.
- Install the Junos Pulse client on the appropriate Windows workstations, as described in "Installing the Junos Pulse Client" on page 62.

CHAPTER 3

Configuring Setup Policies on WXC Series Gateways

This chapter describes how to use the Web interface to perform the basic WXC setup procedures. To configure a WXC Series gateway using the CLI, see the *JWOS Command Reference Guide*.

- Using the JWOS Web Interface on page 23
- Configuring Basic WXC Setup Policies on page 25
- Configuring AAA for WXC Series Gateways on page 30
- Configuring ARP for WXC Series Gateways on page 31
- Configuring SNMP Support for WXC Series Gateways on page 32
- Configuring Syslog Reporting for WXC Series Gateways on page 32
- Configuring Packet Interception for WXC Series Gateways on page 33

Using the JWOS Web Interface

The JWOS Web interface lets you securely access management and performance information for WXC Series gateways from anywhere in your network.

The JWOS Web interface supports the Microsoft Internet Explorer, version 7.0 or 8.0, or Mozilla Firefox 3.0, 3.5, or 3.6. Be sure to configure the browser privacy settings to accept cookies. The Web interface is designed to be viewed at 1024 x 768 pixels. To ensure secure transmission of configuration and management data, the Web interface uses the Secure Sockets Layer protocol (SSL/HTTPS).

- Logging In on page 23
- Understanding the JWOS Web Interface on page 24
- Naming WXC Series Gateways and Other Objects on page 24

Logging In

To log in to a WXC Series gateway through the Web interface:

1. Using a supported Web browser, enter the IP address of a WXC Series gateway:

   https://*IP address of a WXC gateway*

2. If a Security Alert dialog box appears, click **Yes** to proceed.
3. In the Enter Network Password dialog box, enter your username and password.

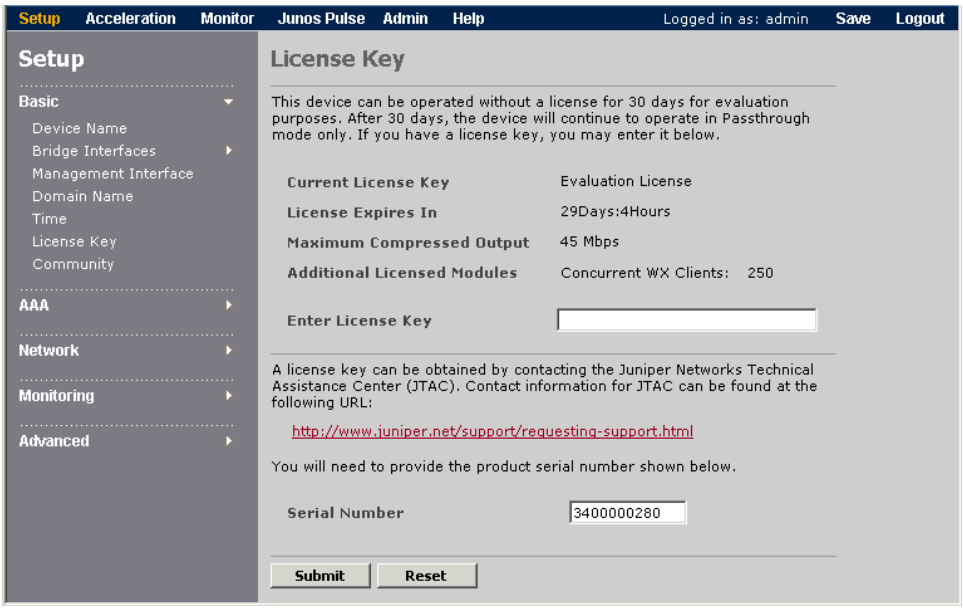
   When you access a new WXC Series gateway for the first time, use **admin** and **juniper** for the username and password, and then run Quick Setup (see "Running Quick Setup for a WXC Series Gateway" on page 21).

To log out of the JWOS Web interface, click **Logout** in the taskbar of any page. Users are logged out automatically if their sessions are inactive for the session timeout time (default is 30 minutes).

Understanding the JWOS Web Interface

The JWOS Web interface contains a taskbar at the top of the page, a left-hand navigation pane, and a data pane for configuring and viewing policies and performance data. Note that the **Save** function is in the upper right corner of the taskbar.

Figure 10: JWOS Web Interface



From the taskbar, select **Help > About** to view hardware and software information for the gateway, such as the IP address, the software and hardware versions, and the license key. Select **Help > Site Map** to view a list of the options available under each taskbar selection. Select **Help > Online Documentation** to access the documentation website.

Naming WXC Series Gateways and Other Objects

Use only letters (A-Z, a-z), numbers (0-9), dashes (-), underscores (_), and periods (.) when you assign names to WXC Series gateways, applications, and other objects.

Configuring Basic WXC Setup Policies

- Configuring the Name of a WXC Series Gateway on page 25
- Configuring Bridge Interfaces for WXC Series Gateways on page 25
- Configuring the Management Interface for WXC Series Gateways on page 27
- Configuring the Domain Name for WXC Series Gateways on page 28
- Configuring the Time for WXC Series Gateways on page 28
- Obtaining a Permanent License for WXC Series Gateways on page 29
- Configuring the Community for WXC Series Gateways on page 30

Configuring the Name of a WXC Series Gateway

You can change the name of the WXC Series gateway displayed in the Web interface banner and CLI prompts, as well as specify the gateway's physical location and the contact information for the system administrator.

To configure the gateway name and contact information:

1. Select **Setup > Basic > Device Name**.
2. Specify the following information:

Device Name	Enter the WXC Series gateway name (up to 30 characters) displayed in the banner of the Web interface and in CLI prompts (default is the IP address). Use only letters, numbers, dashes, underscores, and periods. A name change is propagated to the other WXC Series gateways in the community.
Device Location	Enter a description of the gateway's physical location.
Contact Information	Enter the contact information (up to 64 characters) for the system administrator.

3. Click **Submit** to activate the changes, or click **Reset** to discard them.
4. Click **Save** in the taskbar to retain your changes after the next reboot.

Configuring Bridge Interfaces for WXC Series Gateways

A bridge interface connects a pair of Local and Remote ports on the WXC gateway. When either port receives traffic that is not processed by the WXC gateway, such as broadcast or passthrough traffic, the traffic is sent out the other port. The two ports, called a *port-pair*, share the IP address of the bridge interface.

Table 4 on page 26 describes how interface names are assigned automatically.

Table 4: WXC Interface Names

Interface	Name	Description
Bridge	**br-*slot/pair***	Every WXC Series gateway has a bridge interface named **br-0/0**.
Local	**fe-*slot/pair*/0** or ge-slot/pair/0	The **fe** or **ge** indicates the interface speed (Fast Ethernet or Gigabit Ethernet). The slot and pair numbers are the same as the associated bridge interface. The **/0** indicates the Local interface.
Remote	**fe-*slot/pair*/1** or ge-slot/pair/1	Same as the Local interface name, except the **/1** indicates the Remote interface.

From the Web interface, you can:

- View the status, media access control (MAC) address, and speed and mode for the Local and Remote interfaces on each bridge interface.
- Change the IP address, subnet mask, and default gateway of a bridge interface.
- Enable link-failure propagation so that when a failure is detected on one interface, the other interface turns off for 15 seconds.
- Add static routes to a bridge interface.

To configure the bridge interfaces:

1. Select **Setup > Basic > Bridge Interfaces**, and then select the name of the bridge interface to be configured.
2. To change the interface settings, specify the following information and click **Submit**:

IP address	Enter the IP address of the bridge interface. If you change the IP address or subnet mask, you must reboot the gateway (see “Rebooting the WXC Gateway” on page 74).
Subnet mask	Specify the network portion of the IP address. For example, **255.255.255.0** indicates that the first 24 bits of the IP address are used for the network portion of the address.
Default gateway	Enter the IP address of the default router, which must be on the same subnet as the bridge IP address.
Speed/Duplex	Select the speed and mode for the Local or Remote interface (such as **1000 full-duplex**). By default, the Local and Remote interfaces are set to negotiate the speed and mode automatically. Note that a passive test runs periodically and displays a message above the taskbar if a speed or mode mismatch is detected. The passive test can detect a mismatch only when data is sent and received at the same time.

Link Failure	In high-availability environments, you can enable the following options so that when a failure is detected on one interface, the other interface turns off for 15 seconds. This allows the switch or router to detect the failure, and ensures that the routing mechanisms work as expected. • **Propagate to Remote**—If the switch fails, the Remote interface is disabled so that the router detects the loss of connectivity with the switch. • **Propagate to Local**—If the router fails, the Local interface is disabled so that the switch detects a loss of connectivity with the router. You can also disable the hardware passthrough feature so that the router detects the loss of traffic if the WXC Series gateway fails (see the **config set system bypass-capability** command in the *JWOS Command Reference Guide*).

3. To add static routes to the bridge interface:
   a. On the Bridge Interfaces page, select the Local Routes tab.
   b. Enter the IP address, subnet mask, and the IP address of the gateway for a subnet.
   c. Click **Submit** to add the route to the list of local routes. Note that ICMP redirect routes take precedence over static routes.
   d. Click **DELETE** next to any route that you want to remove.
4. Click **Save** in the taskbar to retain your changes after the next reboot.

Configuring the Management Interface for WXC Series Gateways

You can connect the management port to your management network, and then configure an IP address, subnet mask, and default gateway for the port. The name of the management interface is **fxp0**.

To configure the management interface:

1. Select **Setup > Basic > Management Interface**.
2. Select the **Enable management interface** check box, and specify the following information:

IP Address	Enter the IP address of the management interface. If you change the IP address or subnet mask, you must reboot the gateway (see “Rebooting the WXC Gateway” on page 74).
Subnet Mask	Specify the network portion of the IP address. For example, **255.255.255.0** indicates that the first 24 bits of the IP address are used for the network portion of the address.
Default Gateway	Enter the IP address of the default router, which must be on the same subnet as the interface IP address.
Speed	Select **Auto** to allow the interface speed and mode to be negotiated. To set the interface speed and mode manually, select **Manual**, and then select a speed and mode setting from the list (such as **1000 full-duplex**).

3. Click **Submit** to activate the changes, or click **Reset** to discard them.
4. Click **Save** in the taskbar to retain your changes after the next reboot.

Configuring the Domain Name for WXC Series Gateways

You can specify the local DNS domain name of the WXC Series gateway, and up to three DNS servers for use in resolving IP addresses on the Flow Diagnostics page (see "Viewing Flow Diagnostics on WXC Series Gateways" on page 78).

To configure the domain name:

1. Select **Setup > Basic > Domain Name**.
2. Specify the following information:

Domain Name	Enter the local DNS domain name (up to 256 characters). The domain name must include at least one period, but not as the first or last character. When an IP address in the local domain is resolved by one of the specified DNS servers, the local domain name is prepended to the host name shown on the Flow Diagnostics page. If the domain is blank, only the host names are shown for resolved IP addresses in the local domain. Resolved addresses outside the local domain include the domain name returned by the DNS server.
DNS Servers	Enter the IP addresses of up to three DNS servers (one per line).

3. Click **Submit** to activate the changes, or click **Reset** to discard them.
4. Click **Save** in the taskbar to retain your changes after the next reboot.

Configuring the Time for WXC Series Gateways

If your network uses the Network Time Protocol (NTP), you can specify a primary and secondary NTP server to maintain the current time. You can also set the time manually. Each entry in the system log files includes the current time.

To configure the time settings:

1. Select **Setup > Basic > Time**.
2. Select the time format (**AM/PM** or **24 Hour**).
3. Do one of the following:
   - If you have an NTP server in your network, select **Use NTP Server** and enter the IP address of the NTP server in the Primary box. A secondary NTP server is optional.
   - If you do not have an NTP server, select **Enter Local Time** and enter the current time and date.
4. Select a time zone, GMT offset, or geographical location from the Time Zone list. Optionally, select the check box to automatically adjust the time for daylight savings time.

5. Click **Submit** to activate the changes, or click **Reset** to discard them.
6. Click **Save** in the taskbar to retain your changes after the next reboot.

Obtaining a Permanent License for WXC Series Gateways

Each WXC Series gateway requires a permanent license key for operation. The license key registers the product and determines the gateway's licensed modules and throughput. Initially, a 30-day license provides access to all features. When the temporary license expires, all traffic is passed through without any processing.

To obtain a permanent license key, gather the following information:

- Device serial number displayed in the License Key page (also displayed in the About box and on the back of the gateway).
- Authorization Code Certificate that was e-mailed to you in PDF format (if you purchased license upgrades).
- User ID and password to access the License Key server at:

  http://www.juniper.net/generate_license

  If you lose the license key, you can use the License Key server to retrieve your current license key.

If you have any problems with the licensing process, open a case with the Juniper Case Manager at **http://www.juniper.net/cm**. To call from the United States, Canada, or Mexico, dial +1-888-314-JTAC. To call from other locations, check the list of local support centers at **http://www.juniper.net/support/requesting-support.html** or dial +1-408-745-9500.

To install a permanent license key:

1. Select **Setup > Basic > License Key**.

   The License Key page displays the status of the current license, including the licensed modules and the compressed output for the gateway.
2. Enter your registered license key in the Enter License Key box. To obtain a registered license key:
   a. Go to **http://www.juniper.net/generate_license**, register to create an account, and then log in.
   b. Select **Application Acceleration Products** from the menu, and click **Go**.
   c. Enter your gateway serial number and authorization code, and click **Generate**.
   d. Copy the displayed license key into the Enter License Key box in the WXC Web interface.
3. Click **Submit** to activate the changes, or click **Reset** to discard them.

Configuring the Community for WXC Series Gateways

A WXC Series gateway and Junos Pulse client can form an adjacency and accelerate the traffic between them only if they belong to the same community. Initially, all WXC Series gateways are in the **default** community. In large deployments you may want to define separate communities.

By default, Windows clients are in the same community as the WXC Series gateway from which the Junos Pulse client is downloaded (see "Installing the Junos Pulse Client" on page 62).

To configure the community:

1. Select **Setup > Basic > Community**.
2. Enter the community name (up to 64 characters). If you do not specify a community name, the gateway remains in the **default** community. Note that changing the community name disables all adjacencies with the Pulse clients in the old community.
3. Click **Submit** to activate the changes, or click **Reset** to discard them.
4. Click **Save** in the taskbar to retain your changes after the next reboot.

Configuring AAA for WXC Series Gateways

The following topics describe how to configure the JWOS security features:

- Defining Local User Accounts for WXC Series Gateways on page 30
- Securing Front Panel Access for WXC Series Gateways on page 31

Defining Local User Accounts for WXC Series Gateways

You can define up to 25 users for local authentication. The user class assigned to each account determines the user's access privileges. The predefined **admin** account has full access, and a default password of **juniper**. To ensure secure access, you should change the passwords periodically.

To define local user accounts:

1. Select **Setup > AAA > Local Users**.

   From the Local Users page, you can:

   - Add a new user account, as described in Step 2.
   - Change a user account. Click the username, make any needed changes, and click **Submit**.
   - Delete user accounts. Select the check box next to the accounts you want to delete, and click **Submit**.

2. Click **New User** to add a new account, and specify the following information:

User Name	Enter the account name (up to 32 characters).

User Class	Select a user class to specify the user's privileges: • **Superuser**. Full read/write privileges, including management of user accounts. • **Operator**. Read/write configuration privileges, but no packet capture or user management privileges. • **Read Only Plus**. Read-only privileges and packet capture capability. • **Read Only**. Read-only privileges.
Idle Timeout	Enter the number of minutes that elapse before an idle user is logged out (the default is 30).
Password	Enter the password twice (from 4 to 64 characters).

3. Click **Submit** to activate the changes.
4. Click **Save** in the taskbar to retain your changes after the next reboot.

Securing Front Panel Access for WXC Series Gateways

On WXC Series gateways that have a keypad on the front panel, you can lock the keypad to prevent anyone from rebooting the gateway or making configuration changes through the front panel keypad.

To lock the front panel keypad:

1. Select **Setup > AAA > Front Panel Access**.
2. Select **Locked** to lock the front panel keypad.
3. Click **Submit** to activate the changes, or click **Reset** to discard them.
4. Click **Save** in the taskbar to retain your changes after the next reboot.

Configuring ARP for WXC Series Gateways

The Address Resolution Protocol (ARP) determines whether the gateway for a route is on the Local or Remote interface and discovers the hardware (MAC) addresses of devices that are directly addressable on the Local and Remote interfaces.

For devices that do not respond to ARP requests, you can add static ARP entries that map their IP addresses to their MAC addresses. You can also clear the dynamic ARP entries if you suspect some entries are out of date.

To configure the ARP table:

1. Select **Setup > Network > ARP**.
2. Click **Flush** to delete all dynamic ARP entries. This forces new ARP requests to be issued as needed.
3. Click **DELETE** next to any static ARP entry that you want to remove.
4. Click **Add** to add one or more static ARP entries. For each entry, enter the IP address and its associated MAC address, and then select the Local or Remote interface. You

can add up to five entries at one time. The format of the MAC address is: **xx:xx:xx:xx:xx:xx**.

Click **Submit** to activate the new entries, or click **Cancel** to discard them.

5. Click **Save** in the taskbar to retain your changes after the next reboot.

Configuring SNMP Support for WXC Series Gateways

The following support is provided for SNMP:

- SNMP version 2
- Enterprise management information base (MIB)
- MIB II, Interface Group public objects

NOTE: SNMPv2-compatible utilities are needed to query the 64-bit counters in the Enterprise MIB.

You can use the Enterprise MIB to view performance statistics from a network management system (NMS). In addition, you can enable SNMP traps to be sent to an NMS and other network devices. For a description of the SNMP traps, see "System Events and SNMP Traps for WXC Series Gateways" on page 91.

To configure support for SNMP:

1. Select **Setup > Monitoring > SNMP**.
2. Select the **SNMP Enabled** check box to enable support for SNMP, and then enter the read and write community strings used by the NMS to access SNMP data on the gateway. The default community strings are **public** and **private**.
3. Select the **Trap Enabled** check box to generate SNMP traps (version 2 traps only). To add trap destinations (up to 10), enter the IP address and community string (up to 30 characters), and click **Add**. To delete a trap destination, click **Delete** next to the destination.
4. Select the **Authentication Trap Enabled** check box to generate traps for incorrect logins and unauthorized user access attempts.
5. Click **Submit** to activate the changes, or click **Reset** to discard them.
6. Click **Save** in the taskbar to retain your changes after the next reboot.

Configuring Syslog Reporting for WXC Series Gateways

Syslog messages can be sent to up to five syslog servers. A syslog server allows you to centrally log and analyze configuration events and system error messages such as interface status, security alerts, and environmental conditions. For a description of the syslog messages, see "System Events and SNMP Traps for WXC Series Gateways" on page 91.

To enable syslog reporting:

1. Select **Setup > Monitoring > Syslog Server**.
2. Enter the IP addresses of up to five syslog servers (one per line).
3. Select a facility from the Facility list to send the syslog messages to a specific facility (**local1** through **local7**). The default is **local0**.
4. Select the lowest severity level of the messages sent to the syslog servers. Select **Any** to include all severity levels, including debug messages.
   - **Emergency**—Critical error messages about system failures.
   - **Alert**—Critical error messages that need immediate action.
   - **Critical**—Critical error messages that need prompt action.
   - **Error**—Noncritical error messages, such as license expired.
   - **Warning**—Informational messages about minor events that are not errors.
   - **Notice**—Informational messages about normal, but significant events.
   - **Info**—Informational messages, such as reload requests.
5. Click **Submit** to activate the changes, or click **Reset** to discard them. Click **Save** in the taskbar to retain your changes after the next reboot.

Configuring Packet Interception for WXC Series Gateways

Typically, WXC Series gateways are deployed in the data path between a LAN switch and a WAN edge router. When interrupting the data path is not practical, you can deploy the WXC gateway off path, where the Local interface is connected to the switch or router, and the Remote interface is not used (we recommend connecting the Local interface directly to the router).

After a WXC Series gateway is installed off path, you must configure packet interception to redirect the appropriate traffic to the WXC gateway for acceleration.

To configure packet interception:

1. Select **Setup > Advanced > Packet Interception**.
2. Select **Use external policy-based router commands**.

CAUTION: Enabling packet interception disables the Remote interface for all bridge interfaces. If the gateway is installed in the data path, all data transmission through the gateway will stop.

3. Click **Submit** to activate the changes.
4. Click **Save** in the taskbar to retain your changes after the next reboot.

5. Configure a policy on the local router or Layer 3 switch to redirect traffic to the WXC Series gateway.

   If the off-path gateway is connected to a dedicated port on a router, apply the policy to the inbound interface from the LAN switch. In the following example, any incoming packet on interface **FastEthernet 0/0** that matches **access-list 120** is routed to the WXC Series gateway at IP address 192.168.10.10. The access list shown here redirects all packets, but you can specify additional filtering criteria.

   ```
   interface FastEthernet 0/0
   ip address 192.168.9.1 255.255.255.0
   ip policy route-map Juniper
   access-list 120 permit ip any any
   route-map Juniper permit 50
   match ip address 120
   set ip next-hop 192.168.10.10
   ```

   If the off-path gateway is connected to a dedicated VLAN on a Layer 3 switch, the commands are almost the same, except that you apply the policy to the inbound interface from the LAN:

   ```
   interface Vlan200
     ip address 192.168.9.1 255.255.255.0
     ip policy route-map Juniper
   ```

NOTE: Use the set ip next-hop command to redirect packets to the IP address of the bridge interface on the WXC Series gateway. Do not use the set interface command to redirect traffic to the interface where the WXC gateway is connected.

CHAPTER 4

Configuring Acceleration Policies on WXC Series Gateways

- Types of Application Acceleration on page 35
- Configuring Application Policies for WXC Series Gateways on page 36
- Configuring Application Definitions for WXC Series Gateways on page 37
- Configuring SMB Signing for CIFS Acceleration on page 44

Types of Application Acceleration

- Overview of TCP Acceleration on page 35
- Overview of Microsoft CIFS Acceleration on page 36

Overview of TCP Acceleration

In WAN environments, TCP may restrict the transmission of data because long wait times for acknowledgments (ACKs) are interpreted as signs of network congestion. TCP acceleration solves this problem by terminating each TCP session locally. The result is three independent TCP sessions—between the TCP source and the Junos Pulse client, between the client and the WXC endpoint, and between the WXC endpoint and the destination. Because each TCP acknowledgement (ACK) is sent locally, more data can be put "in flight" at once.

NOTE: TCP acceleration is required for both LZ compression and Microsoft CIFS acceleration.

TCP acceleration is most effective for applications that transfer large amounts of data. In general, TCP acceleration improves performance if the maximum window size (the effective bandwidth multiplied by the latency) exceeds the TCP window size. The typical TCP window size is 64 KB for Windows 2000 and later, and 16 KB for Windows 98.

For example, on a T1 link (1.5 Mbps) where the latency is 200 ms, and a 50 percent data compression doubles the effective bandwidth, the maximum window size is:

(3,088,000 bps * 0.200 seconds)/8 = 77,200 bytes

In this case, TCP acceleration improves performance if the host's TCP window size is 64 KB or less.

NOTE: As with high bandwidth and latency, high compression rates also increase the maximum window size, which in turn increases the benefit of TCP acceleration.

Overview of Microsoft CIFS Acceleration

If TCP acceleration is enabled, you can enable acceleration for Microsoft CIFS traffic. Microsoft CIFS transfers files by sending one block of data at a time, and then waiting for an acknowledgment before sending the next block. The serial transmission of small data blocks is a major contributor to slow performance over the WAN.

When CIFS acceleration is enabled, each block of traffic sent during bulk read/write operations is acknowledged locally. This allows many data blocks to be in flight at the same time, which speeds up the data transfer. Acceleration benefits begin at relatively low latencies (about 20-ms round-trip time).

Note the following:

- CIFS acceleration is supported between Junos Pulse clients and most Windows servers and between Pulse clients and Samba version 3.0 and later. However, CIFS traffic flows between any combination of Windows 7, Windows Vista, and Windows Server 2008 platforms are not accelerated.
- When Server Message Block (SMB) signing is enabled, additional processing is required to accelerate the traffic flow (see "Configuring SMB Signing for CIFS Acceleration" on page 44). CIFS traffic flows are not accelerated when SMB2 signing is enabled.
- You can accelerate all CIFS traffic, or you can create application definitions that let you accelerate traffic to specific servers.

Configuring Application Policies for WXC Series Gateways

For each defined application, you can enable or disable compression and acceleration services, as well as monitoring for reports. The application policies are applied to the traffic sent to all adjacent Junos Pulse clients, provided that you enabled the appropriate services for each client (see "Configuring Pulse Client Policies on WXC Series Gateways" on page 64).

To add or change an application definition, see "Configuring Application Definitions for WXC Series Gateways" on page 37.

To configure application policies:

1. Select **Acceleration > Policies > Applications**.
2. Select the check box at the top of the list for each service that you want to enable, and then select the check boxes for the appropriate applications. To enable or disable

a service for all applications, select or clear the **Select All/Clear** check box below the list.

Service	Description
TCP Acceleration	Indicates whether to apply TCP acceleration to application's traffic (see "Overview of TCP Acceleration" on page 35). TCP acceleration is intended for applications that transfer large amounts of data (such as FTP and CIFS) over high-latency links (such as satellite connections) and long-haul, high-bandwidth links (such as E3 and T3). TCP acceleration is required for LZ compression and CIFS acceleration.
LZ Compression	Indicates whether to use LZ compression for data compression. You can select only applications that are enabled for TCP acceleration. To conserve system processing capacity, disable compression for applications whose traffic is encrypted or already compressed.
CIFS Acceleration	Indicates whether CIFS traffic is accelerated. You can select only CIFS applications that are enabled for TCP acceleration. To accelerate transactions that use SMB signing, see "Configuring SMB Signing for CIFS Acceleration" on page 44.
Monitor	Indicates whether to include compression and acceleration statistics for the application on reports. You can monitor up to 100 applications. For more information about the reports, see "Viewing and Printing WXC Reports" on page 47. Application definitions are provided for applications with well-known port numbers. All other applications are grouped together as the **Undefined-Application**, which is monitored by default. To define additional applications, see "Configuring Application Definitions for WXC Series Gateways" on page 37.

3. Click **Submit** to activate the changes, or click **Reset** to discard them.
4. Click **Save** in the taskbar to retain your changes after the next reboot.

Configuring Application Definitions for WXC Series Gateways

Application definitions allow WXC Series gateways to identify the traffic of up to 256 applications. Definitions are provided for applications with well-known port numbers, and all other applications are grouped together as the **Undefined-Application**. For each additional application you define, you can:

- Enable or disable compression, acceleration, and monitoring for reports.
- View compression and acceleration statistics for each monitored application (see "Viewing and Printing WXC Reports" on page 47).

NOTE: Only TCP traffic can be compressed and accelerated. Non-TCP traffic can only be monitored.

Each application definition can have up to ten rules, and each rule can specify a protocol, source and destination port numbers (or range of port numbers), source and destination IP addresses or subnets, and a ToS/DSCP value.

A packet matches an application definition if a match occurs on any of its rules. All the values defined in the same rule must be true for a match to occur on that rule. A packet is classified under the first application for which a rule match is found. Packets are compared against the definitions according to the order number (definitions with the lowest-order numbers are checked first). The comparison stops on the first match, so if two definitions are similar, the more specific definition must have a lower-order number.

To add or change the application definitions:

1. Select **Acceleration > Applications > Definitions**.

   From the Application Definitions page, you can:

   - Review the current list of application definitions. In the default definitions (see Table 5 on page 41), each definition has rules to match any traffic that has the specified port numbers as the source or destination. The UDP definition acts as a default (no port numbers defined).
   - Add a new application definition, as described in Step 2.
   - Change an application definition. Click the application name, make any needed changes, and click **Submit**.
   - Change a definition's order number. Enter a new value in the Order box, and click **Submit** to renumber the definitions. The new value cannot exceed the highest value in the current range. The definitions are compared against the traffic in ascending order.
   - Delete application definitions. Select the check box for each application you want to delete, and click **Submit**.

2. To add a new application definition:

a. Click **New Application** and specify the following information:

Application Name	Enter a name for the application (up to 63 characters). Use only letters (A-Z, a-z), numbers (0-9), dashes (-), underscores (_), and periods(.).
Application Type	Select one of the following application types: • **Default**. No special processing. • **FTP**. Apply to the FTP application to allow FTP ports to be learned dynamically. Applies only to active FTP.
Services	Select or clear the check box next to each service to be enabled or disabled for the application. The services can also be configured on the Application Policies page (see "Configuring Application Policies for WXC Series Gateways" on page 36).
Specify up to 10 rules composed of one or more of the following values. A match occurs if any of the rules are true. All values defined in the same rule must be true for a match to occur on that rule. You can have a total of 512 rules for all applications.	
Source Address	Enter a source IP address or subnet. The general format is: **address/subnetmask** A blank or an asterisk (*) with no subnet mask indicates any source IP address.
Source Port	Enter a source port number, a series of comma-separated port numbers, or a range of port numbers separated by a hyphen (-). A blank indicates any port. For a list of common application ports, see: **http://www.iana.org/assignments/port-numbers**
Destination Address	Enter a destination IP address or subnet (same format as the source address). A blank or asterisk (*) indicates any destination IP address. Typically, source and destination addresses are specified in separate rules so that a match occurs on either one. A rule that specifies source and destination addresses will match only the traffic between those addresses.
Destination Port	Enter one or more destination port numbers (same format as the source port). A blank indicates any port. Typically, source and destination ports are specified in separate rules so that a match occurs on either one. A rule that specifies source and destination ports will match only the traffic between those ports.
Protocol	Select an application protocol or select **Any** to indicate that a match can occur on any TCP or non-TCP packet (the default). Also, if you do not specify any port numbers you can type in a protocol number (0 to 134). **NOTE:** Only TCP traffic can be compressed and accelerated. Non-TCP traffic can only be monitored. If the protocol is **Any**, all selected services are applied to the TCP traffic, but the monitoring statistics include the matching non-TCP traffic (if any).

b. Click **Advanced** next to a rule to include a type of service (ToS) value, and then specify the following:

ToS bits	Select the check box, and then select one of the following: **IP Precedence**. Select an IP precedence value (0 through 7). **DSCP**. Select a DSCP value (0 through 63) or name. Table 6 on page 43 lists the DSCP names and the equivalent DSCP and IP precedence values for the class selector (CSx) names. The assured forwarding (AFx) and expedited forwarding (EF) names are defined by RFCs 2597 and 3246.

c. Click **Continue** to return to the Application Definition page.

d. Click **Submit** to activate the definition, or click **Cancel** to discard it. To erase an entire rule, including the advanced settings, click **CLEAR** next to the rule.

3. Click **Save** in the taskbar to retain your changes after the next reboot.
4. Review the policy settings for the new application (see "Configuring Application Policies for WXC Series Gateways" on page 36).

   Each new application definition is assigned the next highest order number (the lowest precedence) and is enabled automatically for compression, TCP acceleration, and monitoring for reports. If the new application is encrypted or already compressed, disable compression.
5. Verify that traffic for the new application is shown on the reports (for example, see "WAN Application Summary Report on WXC Series Gateways" on page 50).

   If you do not see any traffic for the application, verify the accuracy of the definition and that the traffic is not being counted against an application with a more general definition and a higher precedence (lower-order number).

Table 5: Default Application Definitions

Application	Order	Port Numbers
AOL	37	5190-5193
ClearCase	24	371
CVS	34	2401
DNS	15	53
Exchange	20	135 **NOTE:** Port 135 is the startup port; other ports are learned dynamically. This definition applies only to Exchange traffic for Windows clients, not for Web clients.
Filenet	41	32768-32774

Table 5: Default Application Definitions *(continued)*

Application	Order	Port Numbers
FTP	1	20-21 **NOTE:** Nondefault FTP ports are learned dynamically.
Groupwise	30	1677
Hostname Resolution	21	42
HTTP	4	80, 8080
HTTPS	12	443
ICA (Citrix)	19	1494
ICMP	22	Protocol 1 (no ports specified)
Kerberos	17	88
LDAP	16	389
Lotus Notes	7	1352
Mail	3	25,110,143
Microsoft SQL Monitor	43	1434
Microsoft SQL Server	6	1433
MS Streaming	31	1755
MS Terminal Services	18	3389
NetApp SnapMirror	40	10566
NetBios	5	137, 138
NFS	33	2049
Novell NCP	28	524
Oracle	11	1525
Oracle SQL*Net	46	1529 TCP
Oracle SQL*Net v1	45	1525 TCP
Oracle SQL*Net v2	44	1521 TCP

Table 5: Default Application Definitions *(continued)*

Application	Order	Port Numbers
PCAnywhere	38	5631-5632
Printer	27	515
RADIUS	32	1812, 1813
RTSP	29	554
SAP	36	3200, 3300-3388, 3390-3399, 3600-3699
Shell	25	514 TCP
SNMP	19	161-162
SNTP	14	123
SSH	13	22
Sybase	10	1498
Symantec Anti-Virus	35	2967
Syslog	26	514 UDP
TACACS	23	49
Telnet	2	23
Traceroute	42	33434-33534 UDP
UniSQL	47	1978
UniSQL Java	48	1979 TCP
XWindows	39	6000-6063

Table 6: ToS and DSCP Values

Name	DSCP	IP Precedence
Default	0	0
CS1	8	1
CS2	16	2
CS3	24	3

Table 6: ToS and DSCP Values *(continued)*

Name	DSCP	IP Precedence
CS4	32	4
CS5	40	5
CS6	48	6
CS7	56	7
AF11	10	–
AF12	12	–
AF13	14	–
AF21	18	–
AF22	20	–
AF23	22	–
AF31	26	–
AF32	28	–
AF33	30	–
AF41	34	–
AF42	36	–
AF43	38	–
EF	46	–

Configuring SMB Signing for CIFS Acceleration

By default, CIFS transactions are not accelerated when SMB signing is used. For servers that have SMB signing enabled, but not required, the WXC can simply disable SMB signing. If a server requires SMB signing, you can configure the WXC to log in to the server to obtain the key needed to create an SMB signature.

To disable the SMB signing requirement on Windows 2000 or Windows 2003 domain controllers, see the Microsoft website:

http://support.microsoft.com/kb/887429

To configure SMB signing for CIFS acceleration:

1. Select **Acceleration > Protocol Acceleration > CIFS Acceleration**.
2. Select the following options:
   - **Disable SMB signing when not required by the server**. Allows CIFS transactions to be accelerated for servers that have SMB signing enabled, but not required. Note that CIFS traffic flows using SMB2 are not accelerated.
   - **Apply SMB signing across the WAN when required by the server**. Allows CIFS transactions to be accelerated for servers that require SMB signing. The SMB signature is based on a key derived from the login password. To allow the WXC Series gateway to log in to a server and create a signature, specify a valid username, password, and (optional) Windows domain that matches an account on the appropriate Windows servers. You must specify the domain if the WXC must log in to a Windows domain controller.

     Note the following:

     - A Windows domain user needs the minimal rights.
     - SMB signing occurs between the Junos Pulse client and the server.
     - CIFS traffic flows between any combination of Windows 7, Windows Vista, and Windows 2008 platforms are not accelerated.
3. Click **Submit** to activate the changes, or click **Reset** to discard them.
4. Click **Save** in the taskbar to retain your changes after the next reboot.

CHAPTER 5

Viewing Reports on WXC Series Gateways

This chapter describes how to view statistics for data compression, bandwidth utilization, application acceleration, and overall traffic statistics.

- Viewing and Printing WXC Reports on page 47
- Executive Report on WXC Series Gateways on page 47
- WAN Accelerated Throughput Report on page 49
- WAN Application Summary Report on WXC Series Gateways on page 50
- Compression Statistics on page 51
- TCP Connections Report on WXC Series Gateways on page 59

Viewing and Printing WXC Reports

Use the following methods to view and print WXC reports:

- To view a report for all remote endpoints, click **Monitor** in the taskbar, select a report from the Report list, and click **Submit**.
- To view a report for a specific remote endpoint, click the magnifier icon next to the Enter Endpoint list, and select the appropriate endpoint. To page through the list of endpoints, click the page numbers and arrow icons above the list.
- To view the numerical value associated with a point on a chart, move the cursor over the point on the chart.
- To print a report, select **Print** in the upper right corner of the report.

Executive Report on WXC Series Gateways

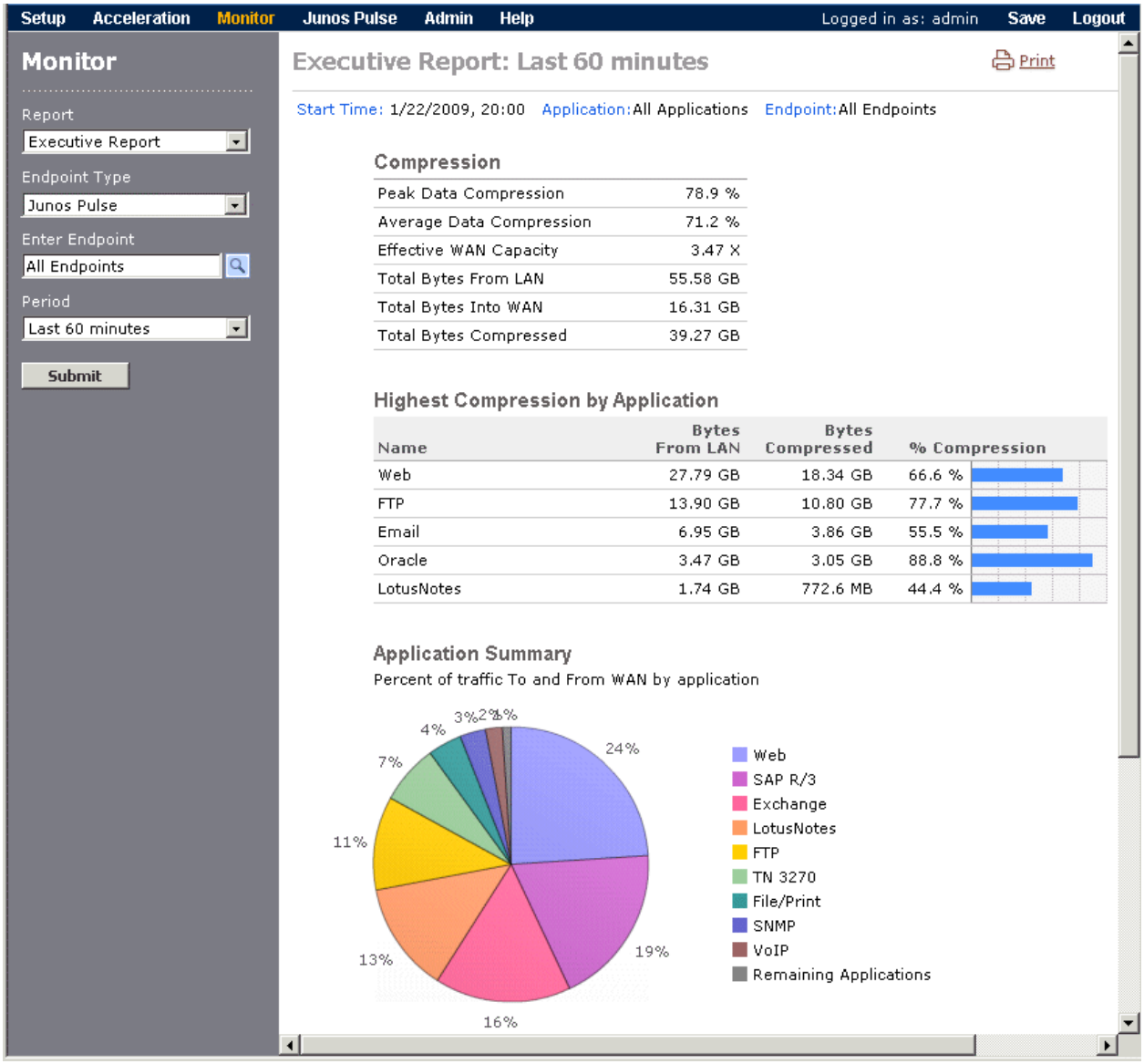
The Executive report summarizes the compression results and traffic volume by application for one or all remote Junos Pulse clients.

To view the Executive report:

1. Select **Monitor**, and select **Executive Report** from the Report list.
2. (Optional) Change the following report parameters as needed, and click **Submit**.

- Select a specific Pulse client from the Enter Endpoint list to view statistics only for traffic sent to the selected endpoint. The default is **All Endpoints**.
- Select a time period from the Period list. You can select the current or previous hour, day, or week. The default is **Last 60 minutes**.

Figure 11: Executive Report



3. Review the following information:
   - The Compression table shows the following:

  - **Peak Data Compression**. Highest percentage of data compression for the selected time period. Based on 5-second intervals for hourly reports, 1-minute intervals for daily reports, and 1-hour intervals for weekly and monthly reports.
  - **Average Data Compression**. Average percentage of data compression for the selected time period.
  - **Effective WAN Capacity**. Factor increase in WAN capacity resulting from the total data compression. For example, this value is 2.00 if total data compression is 50%.
  - **Total Bytes From LAN**. Number of bytes received from the LAN.
  - **Total Bytes Into WAN**. Number of bytes sent to the WAN.
  - **Total Bytes Compressed**. Number of bytes of traffic compressed.
- The Highest Compression by Application table has the following columns:
  - **Name**. Names of the top ten monitored applications with the highest compression percentage.
  - **Bytes from LAN**. Number of bytes received from the LAN for each application.
  - **Bytes Compressed**. Number of bytes compressed for each application.
  - **% Compression**. Percentage of data compression achieved for each application.
- The Application Summary pie chart shows up to nine monitored applications with the highest percentage of the total traffic sent to and from the WAN. The Remaining Applications category, when shown, indicates the traffic for all other applications (both defined and undefined).
- The Traffic Volume by Application graph shows the traffic volume over the selected time period for the top monitored applications.

WAN Accelerated Throughput Report

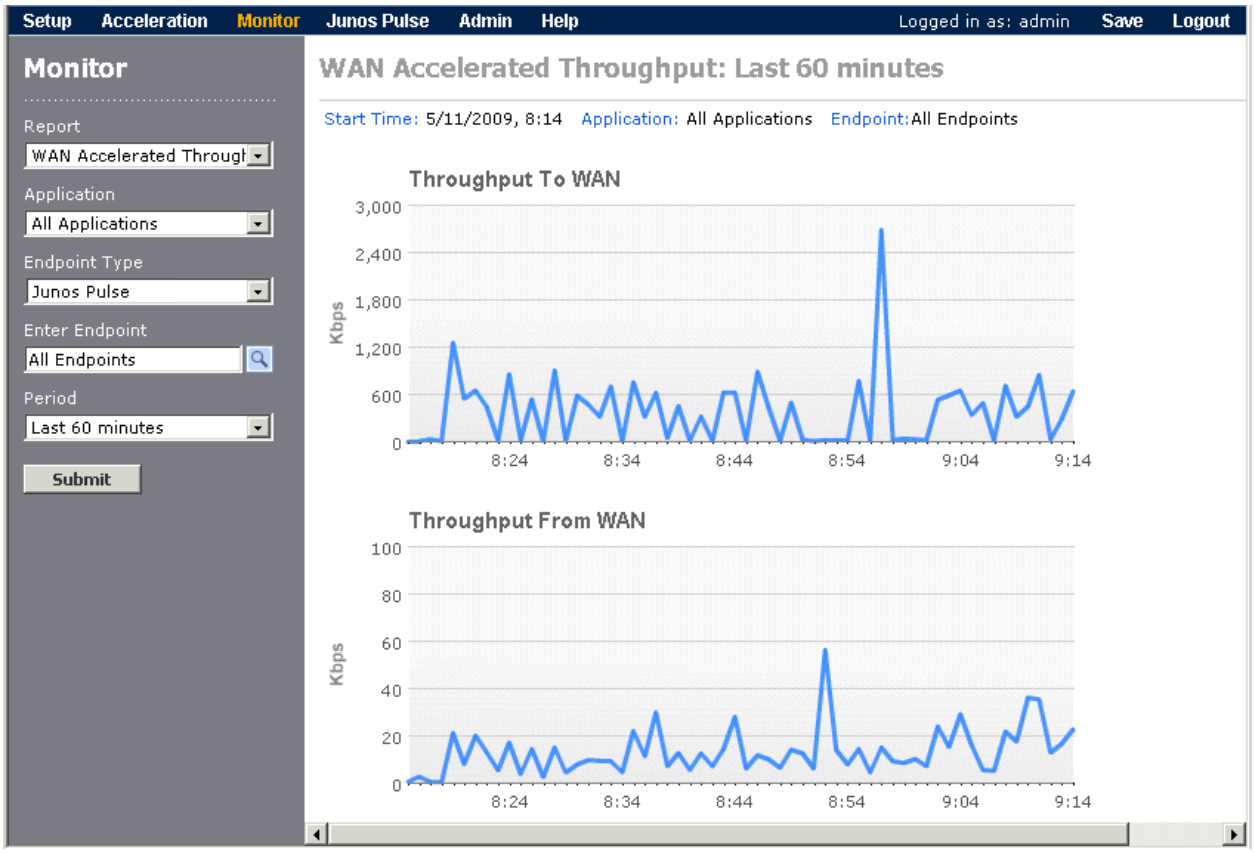
The WAN Accelerated Throughput report shows separate graphs of the throughput to and from the WAN for all remote endpoints, or for a specific endpoint. These statistics help you gauge the speed of all traffic to and from the WAN.

To view the WAN Accelerated Throughput report:

1. Select **Monitor**, and select **WAN Throughput** in the Report list.
2. (Optional) Change the following report parameters as needed, and click **Submit**.
   - Select a monitored application from the Application list. The default is **All Applications**. To specify the monitored applications, see “Configuring Application Policies for WXC Series Gateways” on page 36.
   - Select a specific Pulse client from the Enter Endpoint list to view statistics only for traffic sent to the selected endpoint. The default is **All Endpoints**.

- Select a time period from the Period list. You can select the current or previous hour, day, or week. The default is **Last 60 minutes**.

Figure 12: WAN Accelerated Throughput Report



3. Review the following information:

   - The Throughput To WAN graph shows the average throughput of data sent to the WAN.
   - The Throughput From WAN graph shows the average throughput of data received from the WAN.

WAN Application Summary Report on WXC Series Gateways

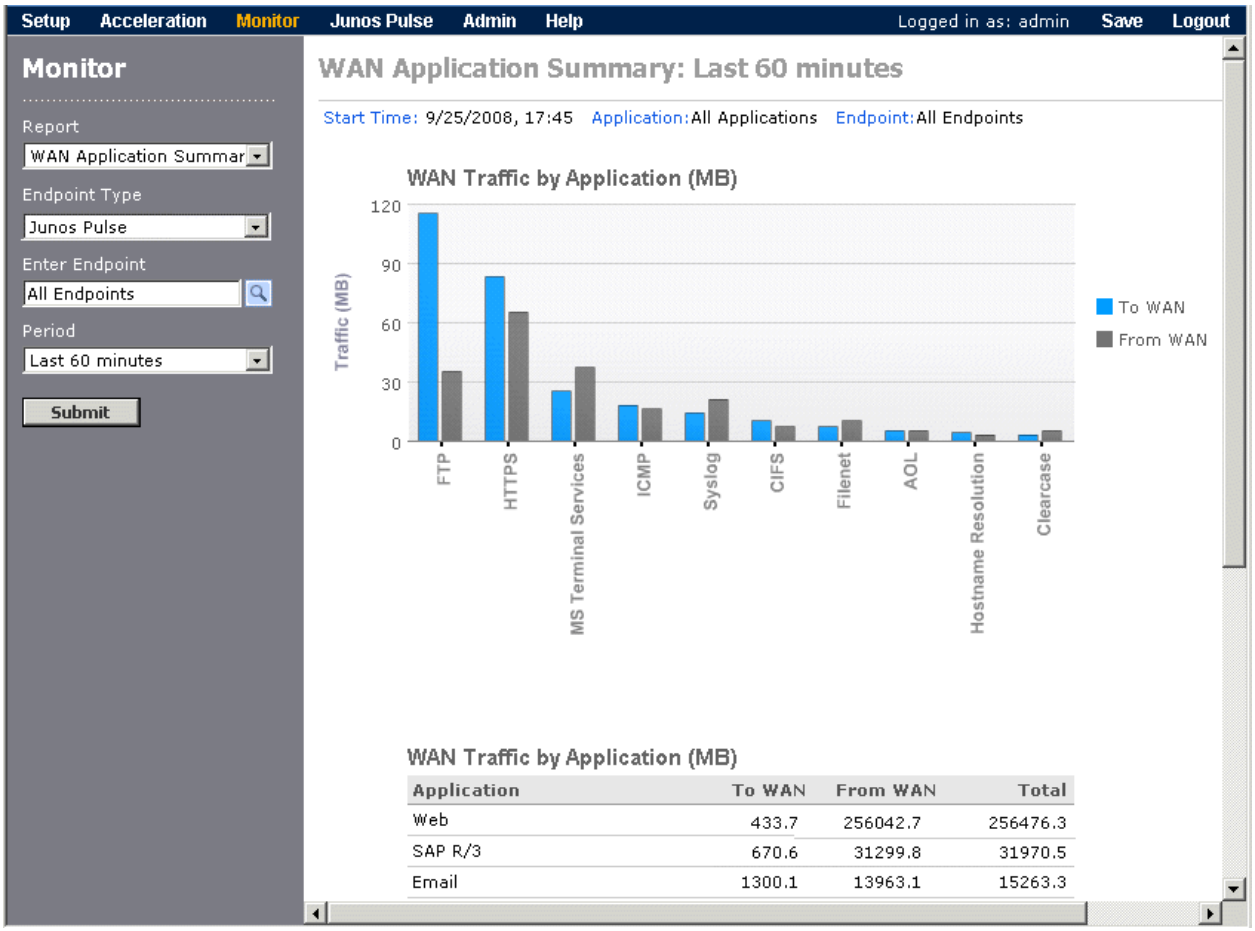
The WAN Application Summary shows the application traffic to and from the WAN for all remote endpoints, or for a specific endpoint. You can view the traffic to and from the WAN for up to 100 monitored applications. To specify the monitored applications, see “Configuring Application Policies for WXC Series Gateways” on page 36.

To view the WAN Application Summary:

1. Select **Monitor**, and select **WAN Application Summary** in the Report list.
2. (Optional) Change the following report parameters as needed, and click **Submit**.

- Select a specific Pulse client from the Enter Endpoint list to view statistics only for traffic sent to the selected endpoint. The default is **All Endpoints**.
- Select a time period from the Period list. You can select the current or previous hour, day, or week. The default is **Last 60 minutes**.

Figure 13: WAN Application Summary



3. Review the following information:
   - The bar chart shows the nine monitored applications that have the most traffic sent to and from the WAN.
   - The application table shows the traffic in megabytes sent to and from the WAN for each monitored application. The applications are sorted in descending order by total traffic.

Compression Statistics

- Compression Throughput Report on WXC Series Gateways on page 52
- Compression Report on WXC Series Gateways on page 53
- Compression by Endpoint Report on WXC Series Gateways on page 55

- Compression Application Summary Report on WXC Series Gateways on page 56
- Passthrough Report on WXC Series Gateways on page 58

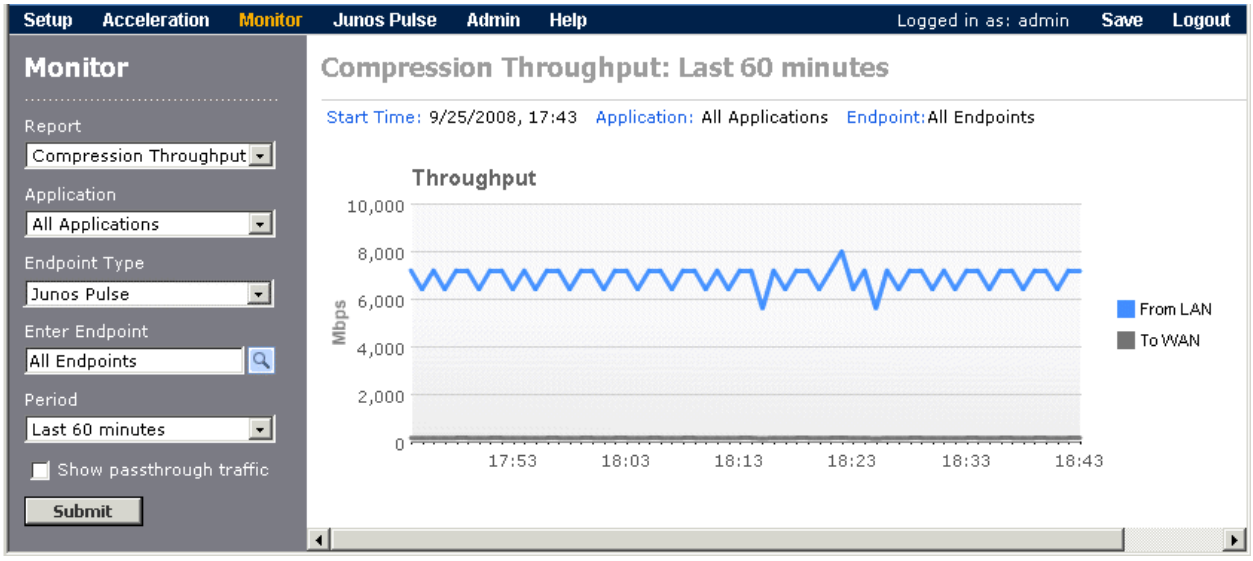
Compression Throughput Report on WXC Series Gateways

The Compression Throughput report compares the throughput of the traffic into the compression engine from the LAN with the throughput of the compressed traffic sent to the WAN.

To view the Compression Throughput report:

1. Select **Monitor**, and select **Compression Throughput** from the Report list.
2. (Optional) Change the following report parameters as needed, and click **Submit**.
   - Select a monitored application from the Application list. The default is **All Applications**. To specify the monitored applications, see "Configuring Application Policies for WXC Series Gateways" on page 36.
   - Select a specific Pulse client from the Enter Endpoint list to view statistics only for traffic sent to the selected endpoint. The default is **All Endpoints**.
   - Select a time period from the Period list. You can select the current or previous hour, day, or week. The default is **Last 60 minutes**.
   - Select the **Show passthrough traffic** check box to display the total traffic sent to the WAN without any processing.

Figure 14: Compression Throughput Report



3. Review the following information on the Throughput graph:
   - **From LAN**. Average data throughput into the compression engine.
   - **To WAN**. Average data throughput out of the compression engine.

Compression Report on WXC Series Gateways

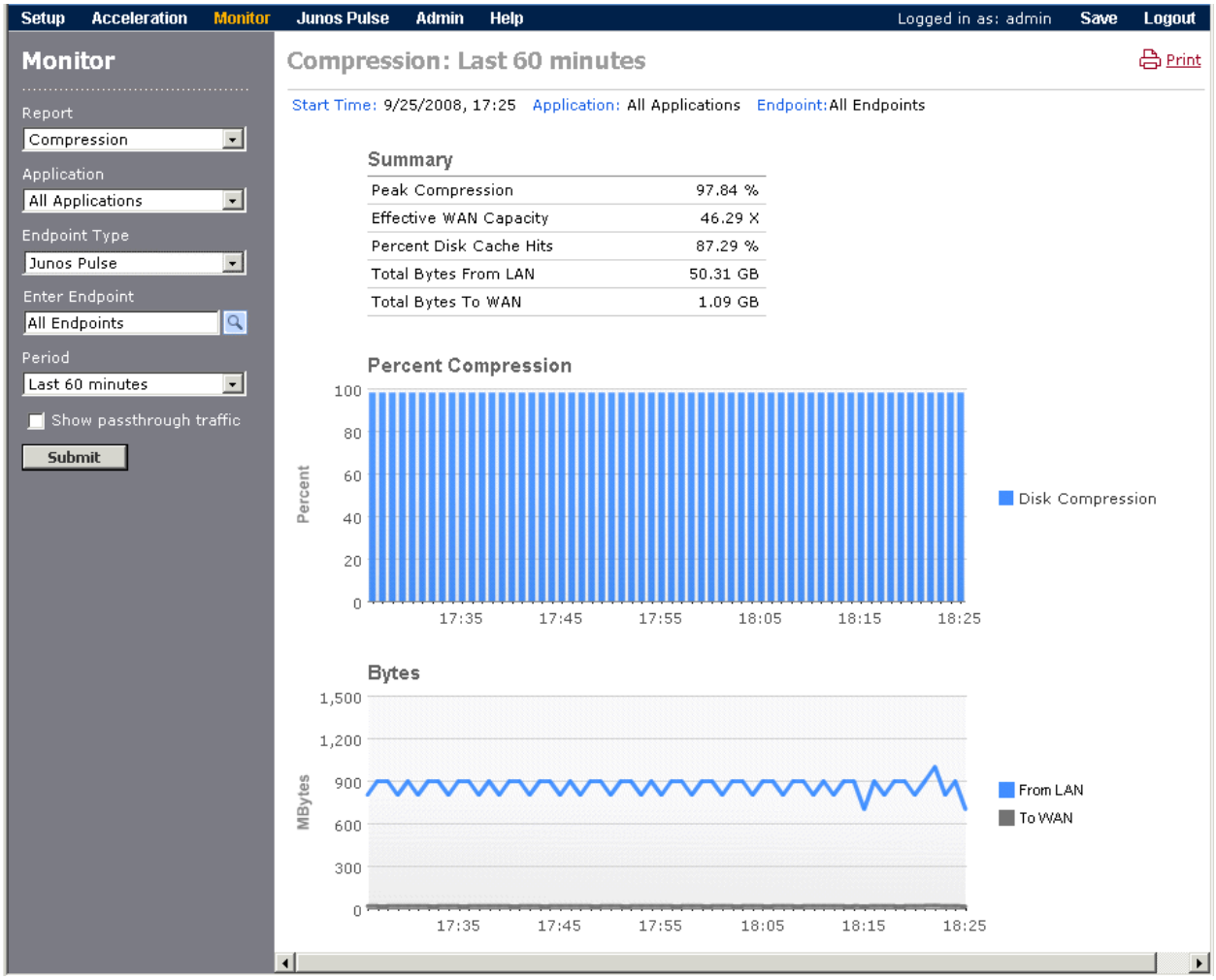
The Compression report includes a summary table, a graph of the compression percentage, and a graph of the number of bytes received from the LAN and sent to the WAN for the selected time period. Note that the compression percentage is not an average, but is based on the total number of bytes compressed:

Compression % = [(Bytes from LAN - Bytes to WAN)/Bytes from LAN] x 100

To view the Compression report:

1. Select **Monitor**, and select **Compression** from the Report list.
2. (Optional) Change the following report parameters as needed, and click **Submit**.
   - Select a monitored application from the Application list. The default is **All Applications**. To specify the monitored applications, see "Configuring Application Policies for WXC Series Gateways" on page 36.
   - Select a specific Pulse client from the Enter Endpoint list to view statistics only for traffic sent to the selected endpoint. The default is **All Endpoints**.
   - Select a time period from the Period list. You can select the current or previous hour, day, or week. The default is **Last 60 minutes**.
   - Select the **Show passthrough traffic** check box to include the traffic sent to the WAN without any processing.

Figure 15: Compression Report



3. Review the following information:

   - The Summary table shows the following information if **All Endpoints** is selected from the Enter Endpoint list.

     - **Peak Compression**. Highest percentage of data compression for the selected time period. Based on five-second intervals for hourly reports, one-minute-intervals for daily reports, and one-hour intervals for weekly and monthly reports.

     - **Effective WAN Capacity**. Factor increase in WAN capacity resulting from the total data compression. For example, this value is 2.00 if total data compression is 50%.

     - **Total Bytes From LAN**. Number of bytes received from the LAN.

  - **Total Bytes To WAN**. Number of bytes sent to the WAN.
  - **Total Bytes Passed Through**. Number of bytes sent to the WAN that are passed through without any processing. This value is shown only if the **Show passthrough traffic** check box is selected.
- The Percent Compression graph shows how the percentage of data compression varied over the selected time period.
- The Bytes graph shows the number of megabytes received from the LAN and sent to the WAN for the selected time period.

Compression by Endpoint Report on WXC Series Gateways

The Compression by Endpoint report shows the percentage of data compression achieved for the traffic sent to each remote Pulse client, and the number of bytes that the local WXC received from the LAN and sent to the WAN for each remote client. You can view the report for one or all applications.

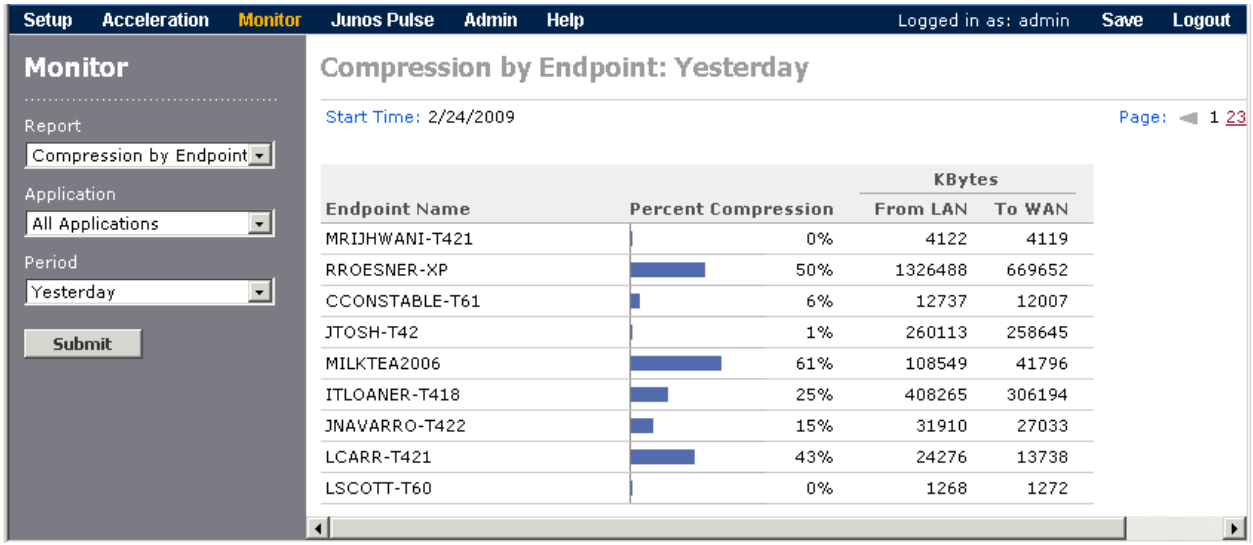
You can also select an endpoint name to view the compression by application for the selected endpoint. To view application statistics for all endpoints, see the "Compression Application Summary Report on WXC Series Gateways" on page 56.

Note that historical data is maintained for at least two months, so endpoints may be listed that have no data for the selected time period.

To view the Compression by Endpoint report:

1. Select **Monitor**, and select **Compression by Endpoint** from the Report list.
2. (Optional) Change the following report parameters as needed, and click **Submit**.
   - Select a monitored application from the Application list. The default is **All Applications**. Select **Others** to view statistics for applications that are undefined or unmonitored. To specify the monitored applications, see "Configuring Application Policies for WXC Series Gateways" on page 36.
   - Select a time period from the Period list. You can select the current or previous hour, day, or week. The default is **Last 60 minutes**.

Figure 16: Compression by Endpoint Report



3. Locate a specific endpoint by clicking the page numbers at the top of the page.
4. Review the following information for each endpoint:
   - **Percent Compression**. Percentage of data compression for the selected time period.
   - **KBytes From LAN**. Number of kilobytes received from the LAN.
   - **KBytes To WAN**. Number of kilobytes sent to the WAN.

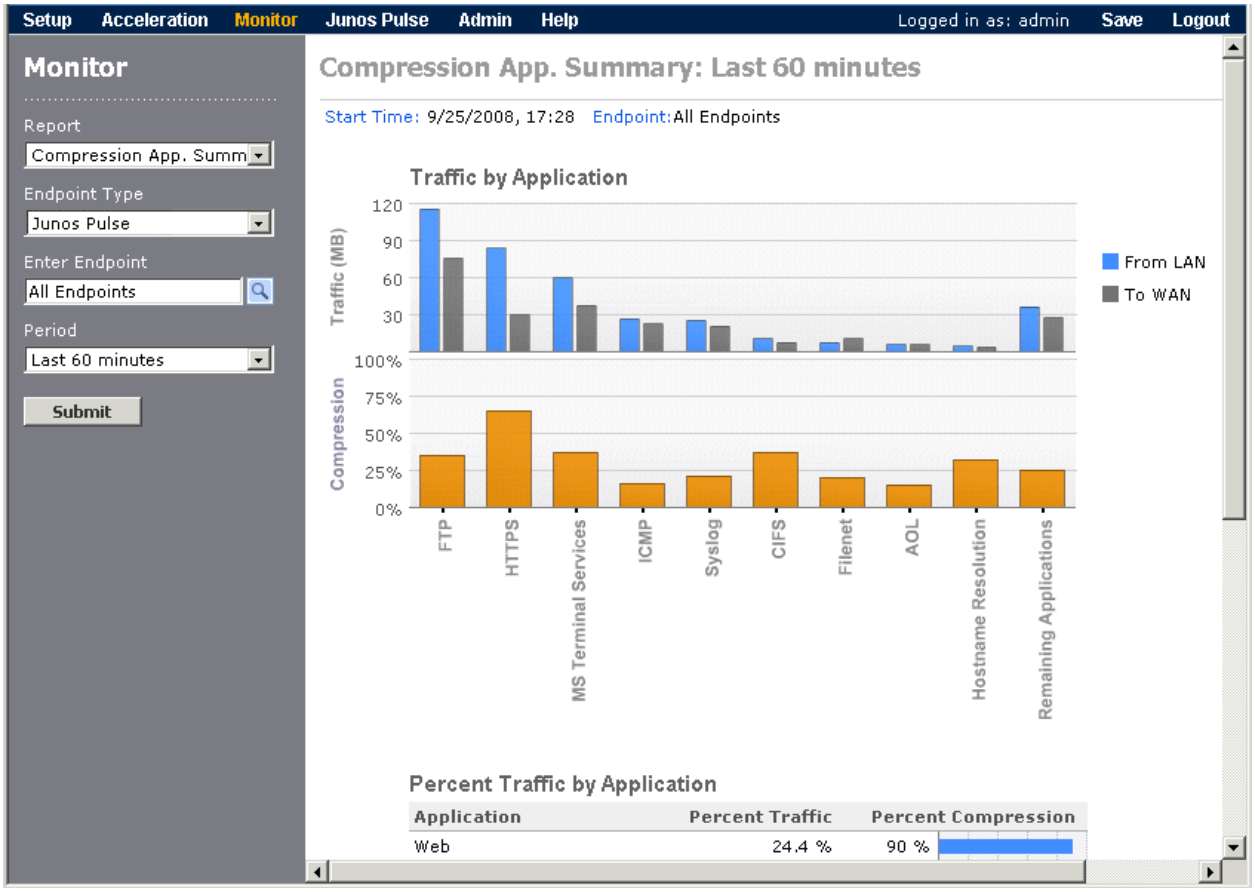
Compression Application Summary Report on WXC Series Gateways

The Compression Application Summary report shows a bar chart of the nine monitored applications that have the highest percentage of the traffic into the WXC Series gateway. A table is also included that shows the traffic statistics and percentage of data compression for each monitored application (up to 100). To specify the monitored applications, see “Configuring Application Policies for WXC Series Gateways” on page 36.

To view the Compression Application Summary:

1. Select **Monitor**, and select **Compression App. Summary** from the Report list.
2. (Optional) Change the following report parameters as needed, and click **Submit**.
   - Select a specific Pulse client from the Enter Endpoint list to view statistics only for traffic sent to the selected endpoint. The default is **All Endpoints**.
   - Select a time period from the Period list. You can select the current or previous hour, day, or week. The default is **Last 60 minutes**.

Figure 17: Compression Application Summary



3. Review the following information:

   - The bar charts show the nine monitored applications with the highest percentage of the total traffic received from the LAN for the selected endpoints. The first chart also shows the traffic sent to the WAN, which is affected by the compression percentage shown in the second chart.
   - The table has the following columns.
     - **Application**. Names of the monitored applications, sorted in descending order by the application's percentage of the total traffic.
     - **Percent Traffic**. Percentage of the total traffic received from the LAN for each application.
     - **Percent Compression**. Percentage of data compression achieved for each application. A dash is shown for applications that have no traffic or that cannot be compressed (such as encrypted applications). Data compression should be disabled for applications that consistently show little or no compression (see "Configuring Application Policies for WXC Series Gateways" on page 36).

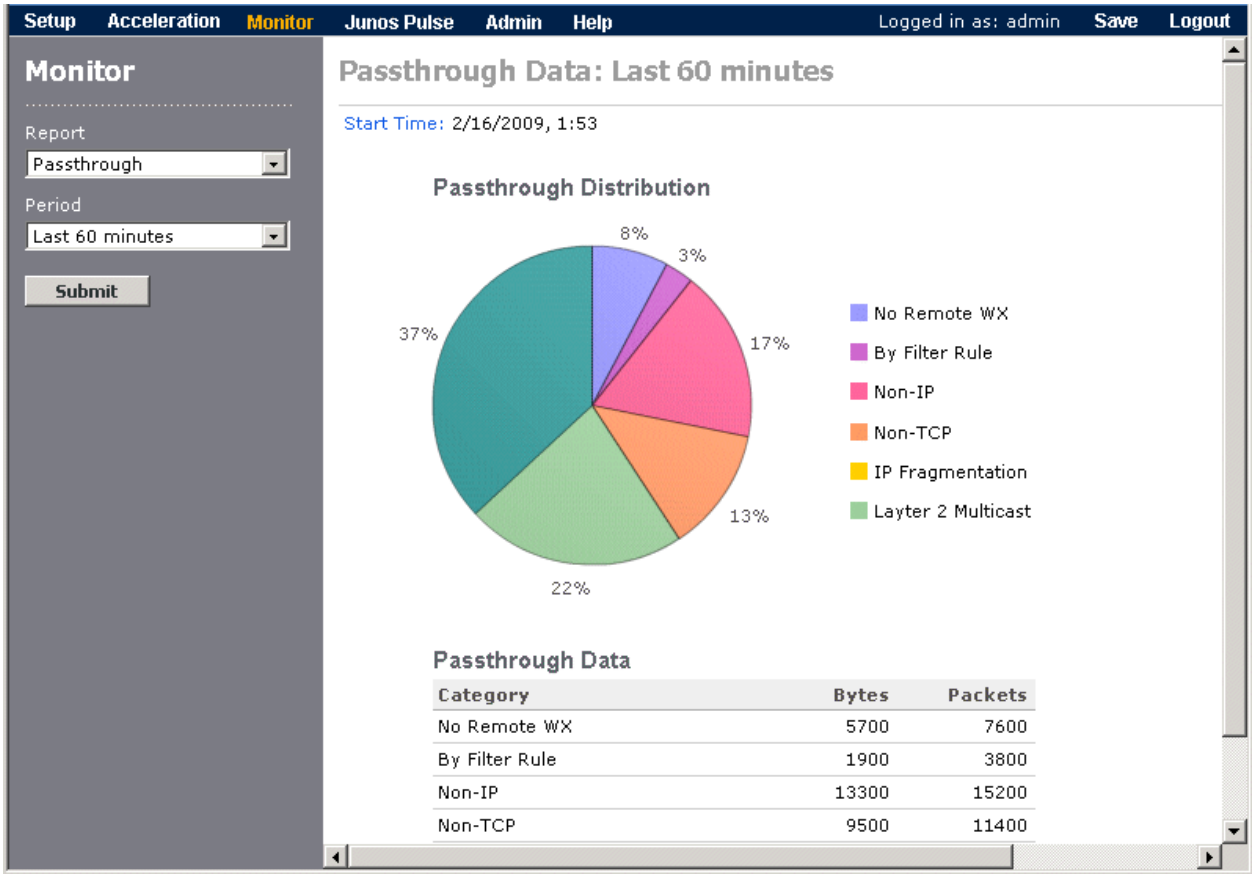
Passthrough Report on WXC Series Gateways

Traffic that falls into one of several categories is passed through the WXC Series gateway without any processing. The Passthrough report shows the percentage of passthrough traffic in each category, as well as the number of bytes and packets in each category.

To view the Passthrough report:

1. Select **Monitor**, and select **Passthrough** from the Report list.
2. Select a time period from the Period list, and click **Submit**.

Figure 18: Passthrough Report



The following table describes the passthrough categories:

Category	Description
No Remote WX	No Pulse clients are available, or TCP acceleration is disabled for one or more clients.
By Filter Rule	TCP acceleration is disabled for specific applications (see “Configuring Application Policies for WXC Series Gateways” on page 36).

Category	Description
Non-IP	Non-IP traffic is not accelerated.
Non-TCP	Non-TCP traffic is not accelerated.
IP Fragmentation	Fragmented IP packets are not accelerated.
Layer 2 Multicast	Layer 2 multicast traffic, such as for ARP, is not compressed because the intended destination is unknown.

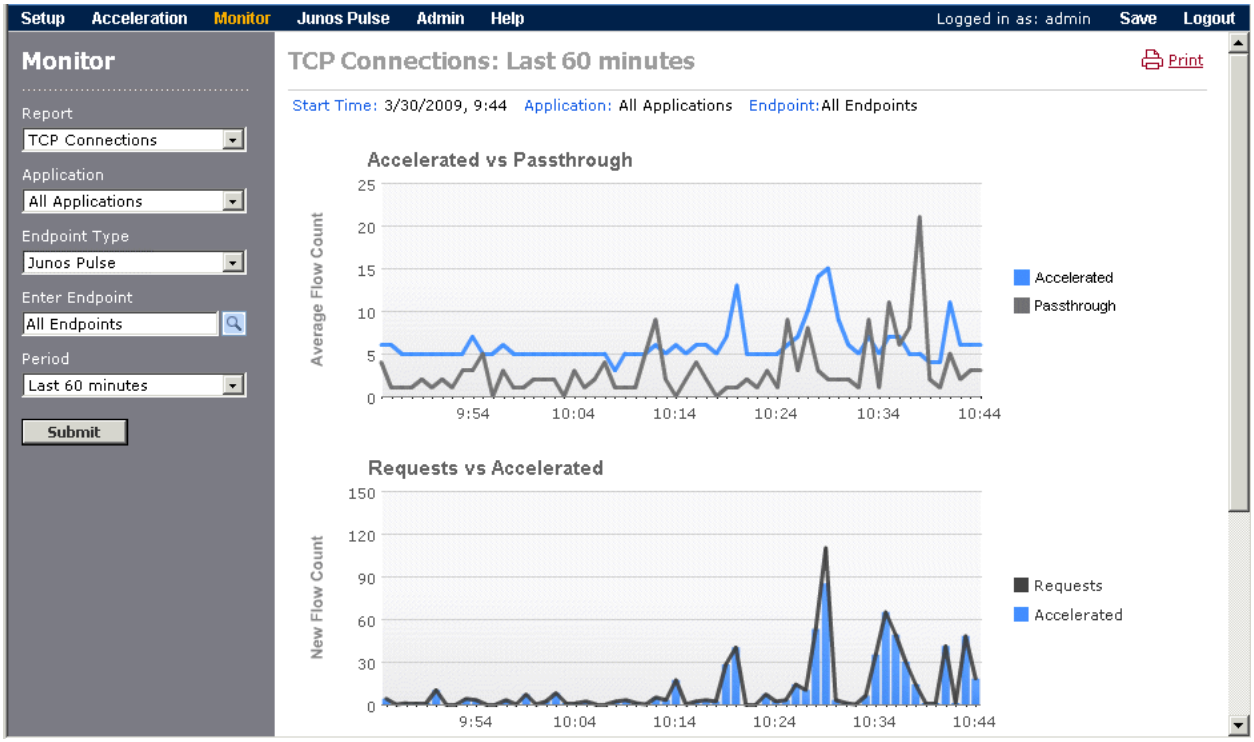
TCP Connections Report on WXC Series Gateways

The TCP Connections report compares the average number of accelerated TCP connections with the average number that are passed through, and the number of connections accelerated versus the number of acceleration requests.

To view the TCP Connections report:

1. Select **Monitor**, and select **TCP Connections** in the Report list.
2. (Optional) Change the following report parameters as needed, and click **Submit**.
   - Select a monitored application from the Application list. The default is **All Applications**. To specify the monitored applications, see "Configuring Application Policies for WXC Series Gateways" on page 36.
   - Select a specific Pulse client from the Enter Endpoint list to view connections only for the selected endpoint. The default is **All Endpoints**.
   - Select a time period from the Period list. You can select the current or previous hour, day, or week. The default is **Last 60 minutes**.

Figure 19: TCP Connections Report



3. Review the following graphs:

   - **Accelerated vs Passthrough**. Compares the average number of traffic flows receiving TCP acceleration with the total number of traffic flows being passed through without any processing. The passthrough traffic flows are shown only if you select **All Endpoints** from the Enter Endpoint list. For hourly reports, the average number of traffic flows for each minute is based on 10-second intervals.
   - **Requests vs Accelerated**. Compares the number of traffic flows that requested TCP acceleration with the number of traffic flows that were accelerated.

CHAPTER 6

Configuring Junos Pulse on WXC Series Gateways

- Junos Pulse Client Hardware and Software Requirements on page 61
- Installing the Junos Pulse Client on page 62
- Managing Junos Pulse Client Software, Configurations, and Policies on page 63

Junos Pulse Client Hardware and Software Requirements

The following table lists the hardware and software requirements of the Junos Pulse client:

Requirement	Description
Operating System	• Windows 7 Enterprise Edition (64 bit) • Windows Vista SP2 Enterprise Edition (32 bit) • Windows XP Professional SP3 (32 bit) NOTE: The above versions have been qualified (tested extensively). Windows 7 (32 bit) and Windows Vista (64 bit) are compatible in that they have received less testing, but are fully supported. For a complete list of qualified and compatible platforms, see *Junos Pulse Supported Platforms*.
CPU	500 MHz
Memory	512 MB of RAM
Available disk space	400 MB
Browser	• Internet Explorer 7.0 or 8.0 • Firefox 3.0, 3.5, or 3.6
Java	JRE-6u17-windows-i586

Installing the Junos Pulse Client

Mobile and remote Windows users can obtain the benefits of application acceleration by installing the Junos Pulse client. The Junos Pulse client accelerates traffic between the client system and a remote WXC Series gateway. The WXC Series gateways and Pulse clients discover each other automatically and begin accelerating traffic without user intervention.

NOTE: You must install the Junos Pulse client on each Windows client, not on a single Windows system that serves as a gateway for other clients.

The following sections describe how to install the Junos Pulse client:

- Downloading the Junos Pulse Client from a WXC Series Gateway on page 62
- Downloading the Junos Pulse Client from a SA Series Gateway on page 63
- Uninstalling the Junos Pulse Client on page 63

Downloading the Junos Pulse Client from a WXC Series Gateway

You can download the Junos Pulse client from any WXC Series gateway running JWOS 6.1 that has a client license. When the license is present, a **Junos Pulse** selection is shown in the taskbar of the Web interface for the WXC Series gateway.

Before users can download the Pulse client software, you must:

- Verify that Pulse client downloads are enabled (see “Enabling Pulse Client Downloads from WXC Series Gateways” on page 64).
- Specify the Pulse client configuration (see “Defining the Pulse Client Configuration on WXC Series Gateways” on page 65).

To download the Pulse client from a WXC Series gateway to a computer running Windows 7, Windows Vista, or Windows XP:

1. If the WX Client is installed, uninstall the WX Client by selecting **Start > All Programs > Juniper Networks > WX Client > Uninstall**. The WX Client supports only JWOS 6.0 and is not compatible with the Pulse client.
2. Enter the following URL in a supported Web browser:

   https://*WXC IP address/client*
3. Enter the username and password, if needed, and click **Login**.
4. Select **Install Now**, and, if necessary, click **Install** in the Security Warning dialog box. Note the following:
   - If the Windows Firewall is enabled, click **Unblock** when prompted to allow the client to accept external connections.
   - If you are prompted to stop the Network Connect client, click **OK** and restart the Network Connect client after the Junos Pulse client is installed.

When installation is complete, the Junos Pulse client starts automatically, and the Junos Pulse icon is shown in the system tray in the lower-right corner of the Windows desktop. Application acceleration starts automatically when remote WXC gateways are discovered. No additional configuration is necessary.

Downloading the Junos Pulse Client from a SA Series Gateway

The Junos Pulse client can be downloaded and installed automatically when users access a SA Series gateway. For version 6.5 or 6.3 SA Series gateways, the Junos Pulse client must first be exported from a WXC Series gateway and uploaded to the SA Series gateway (see "Distributing the Pulse Client" on page 67). Note that version 7.0 (or higher) SA Series gateways include the Junos Pulse client, so exporting the client from a WXC Series gateway is not necessary.

To download the Junos Pulse client from a SA Series gateway:

1. On a computer running Windows 7, Windows Vista, or Windows XP, enter the URL of the SA Series gateway in a supported Web browser. For example:

   https://wx-sa.juniper.net

   The Loading Components page is displayed. The Host Checker window opens for downloading the Junos Pulse client installer, followed by the Junos Pulse Client window to download and install the client. Note the following:

   - If the Windows Firewall is enabled, click **Unblock** when prompted to allow the Junos Pulse client to accept external connections.
   - If you are prompted to stop the Network Connect client, click **OK** and restart the Network Connect client after the Junos Pulse client is installed.
   - If you are prompted about improper installation of the Host Checker or Junos Pulse client, click **Try Again** to complete the installation.

   When installation is complete, the Junos Pulse client starts automatically. To start the client manually, double-click the Junos Pulse icon in the system tray. Application acceleration starts automatically when remote WXC Series gateways are discovered. No additional configuration is necessary.

Uninstalling the Junos Pulse Client

To uninstall the Junos Pulse client software, select **Start > All Programs > Juniper Networks > Junos Pulse > Uninstall**, or run the following program (if necessary, change C: to the drive where Windows is installed):

C:\Program Files\Juniper Networks\Junos Pulse\Uninstall.exe

Managing Junos Pulse Client Software, Configurations, and Policies

- Enabling Pulse Client Downloads from WXC Series Gateways on page 64
- Enabling Pulse Client Adjacencies on WXC Series Gateways on page 64
- Configuring Pulse Client Policies on WXC Series Gateways on page 64

- Viewing the Status of Pulse Clients on WXC Series Gateways on page 65
- Defining the Pulse Client Configuration on WXC Series Gateways on page 65
- Viewing the Pulse Client Configuration on WXC Series Gateways on page 66
- Uploading Pulse Client Software to WXC Series Gateways on page 66
- Distributing the Pulse Client from WXC Series Gateways on page 67

Enabling Pulse Client Downloads from WXC Series Gateways

Windows users can download and install the Junos Pulse client software from a WXC Series gateway running JWOS 6.1 or higher that has client downloads enabled. Optionally, you can require users to log in before they can download the client software.

To enable client software downloads:

1. Select **Junos Pulse > Setup > Pulse Software Download**.
2. Verify that the displayed version of the Pulse software is correct. If a later version is available, you must upload it to the WXC Series gateway (see "Uploading Pulse Client Software to WXC Series Gateways" on page 66).
3. Select **Allow Pulse software download** to allow users to download the client software.
4. Select **Require user authentication** to require users to log in, and specify the required username and password.
5. Click **Submit** to activate the changes.
6. Click **Save** in the taskbar to retain your changes after the next reboot.

Enabling Pulse Client Adjacencies on WXC Series Gateways

By default, a WXC Series gateway running JWOS 6.1 (or higher) can form an adjacency with any client that is running a supported version of the Junos Pulse client software. Traffic is accelerated after the adjacency is established. You can disable and enable client adjacencies at any time. After an adjacency is manually disabled (or disrupted for any reason), it takes about 30 seconds to reestablish the adjacency.

To enable or disable adjacencies with Junos Pulse clients:

1. Select **Junos Pulse > Setup > Pulse Adjacency**.
2. Select **Allow adjacency with Pulse clients** to enable the WXC to form adjacencies with Junos Pulse clients. If you clear the check box, all current adjacencies are disabled, and all client traffic flows are reset.
3. Click **Submit** to activate the changes.
4. Click **Save** in the taskbar to retain your changes after the next reboot.

Configuring Pulse Client Policies on WXC Series Gateways

You can configure compression and acceleration services for each client that is currently adjacent (connected) or that has been adjacent at any time since the last time the WXC

Series gateway was restarted. When an adjacency is established, the local application policies are applied to the traffic sent to that client.

To define the default configuration for a client, see "Defining the Pulse Client Configuration on WXC Series Gateways" on page 65.

To configure the Junos Pulse client policies:

1. Select **Junos Pulse > Policies**.
2. Enable a service for one or more clients by selecting the check box for the service next to the appropriate clients. To enable or disable a service for all clients, select or clear the **Select All/Clear** check box below the list.
3. Click **Submit** to activate the changes, or click **Reset** to discard them.
4. Click **Save** in the taskbar to retain your changes after the next reboot.

Viewing the Status of Pulse Clients on WXC Series Gateways

You can view the connection status of each Junos Pulse client and the status of each service between the local WXC Series gateway and each remote Pulse client. The list of clients includes the adjacent (connected) clients and all clients that are waiting for a connection or have been active at any time since the last time the WXC was restarted. Inactive adjacencies are disconnected after 15 minutes.

To view the status of Junos Pulse clients:

1. Select **Junos Pulse > Status**.
2. Review the status icons:

Icon	Description
	The Junos Pulse client is adjacent (connected).
	The Junos Pulse client is disconnected, waiting for a connection, or in the process of connecting or disconnecting.
	The service is operating normally.
	The service is not enabled on the local WXC Series gateway. To enable the service, see "Configuring Pulse Client Policies on WXC Series Gateways" on page 64.
	A problem exists, or the service is enabled on the local WXC Series gateway, but disabled on the Pulse client.

Defining the Pulse Client Configuration on WXC Series Gateways

When users download the Junos Pulse client software, a client configuration is included. You must generate a client configuration from the current WXC configuration file

(**startup.cfg**) or load a customized configuration file from a local disk, FTP server, or TFTP server.

To view the current client configuration, see "Viewing the Pulse Client Configuration on WXC Series Gateways" on page 66.

1. Select **Junos Pulse > Admin > Load Pulse Configuration**.

   The client configuration and its last update time are indicated at the top of the page. If a client configuration is not defined, **Not Available** is displayed.

2. Select one of the following:

Generate configuration file	Generates a client configuration based on the current WXC configuration saved in the **startup.cfg** file.
Local disk	Specify the path and filename on a machine in your network or click **Browse** and select the configuration file.
TFTP server	Enter a TFTP server's IP address and the path and filename on the server, such as **/juniper/client_config.cfg**.
FTP server	Enter an FTP server's IP address and the path and filename on the server, such as **/juniper/client_config.cfg**. If the FTP server does not accept anonymous user access, enter a username and password for an account that has read/write privileges on the server.

3. Click **Load** to update the client configuration.

Viewing the Pulse Client Configuration on WXC Series Gateways

The default configuration that is downloaded to Junos Pulse clients can be viewed through the Web interface. Note that when you generate the Pulse client configuration from the WXC Series gateway, the client configuration contains a subset of the CLI commands from the gateway configuration.

To view the client configuration:

1. Click **Junos Pulse > Admin > Display Pulse Configuration.**
2. View the client configuration. For more information about the CLI commands in the configuration, see the *JWOS Command Reference Guide*.

Uploading Pulse Client Software to WXC Series Gateways

When a new version of the Junos Pulse client software becomes available, you must upload it to the WXC Series gateway before it can be downloaded by users or exported for distribution. You can load the Pulse client software from a local disk or from an FTP or TFTP server.

To upload a new version of the Pulse client software:

1. Select **Junos Pulse > Admin > Load Pulse Software**.
2. Verify that you want to replace the client version displayed at the top of the page.
3. Select one of the following and specify the location of the new Pulse version:

Local disk	Specify the path and filename on a machine in your network, or click **Browse** and select the client software file.
TFTP server	Enter a TFTP server's IP address and the path and filename on the server.
FTP server	Enter an FTP server's IP address and the path and filename on the server. If the FTP server does not accept anonymous user access, enter a username and password for an account that has read/write privileges on the server.

4. Click **Load** to update the Junos Pulse client software.

Distributing the Pulse Client from WXC Series Gateways

In addition to allowing users to download the Junos Pulse client from a WXC Series gateway, you can also distribute the client using either of the following methods:

- **Juniper Networks SA Series SSL VPN Appliance**—The Junos Pulse client can be downloaded and installed automatically when users access the SA Series gateway. For version 6.5 or 6.3 SA Series gateways, you must export the Pulse client software package from a WXC Series gateway, and then upload the package to the SA Series gateway. Version 7.0 or higher SA Series gateways include the Pulse client, so exporting the client from a WXC gateway is not necessary. Junos Pulse configuration information for the SA Series gateway is included in both the *Junos Pulse Administration Guide* and the *Secure Access Administration Guide*.
- **Microsoft System Management Server (SMS)**—You can distribute the Junos Pulse client through SMS by exporting the client configuration for inclusion in the Windows installer file.

Distributing the Pulse Client Through a SA Series Gateway

Use the following procedure to distribute the Junos Pulse client through a version 6.5 or 6.3 SA Series gateway. To distribute the Pulse client through a version 7.0 or higher SA Series gateway, see the *Junos Pulse Administration Guide* or the *Secure Access Administration Guide*.

1. Load or generate a Junos Pulse client configuration (see "Defining the Pulse Client Configuration on WXC Series Gateways" on page 65).
2. Select **Junos Pulse > Admin > Export Pulse Software**.
3. Export the client software package to be installed on a SA Series gateway:
    a. Select **Create Host Checker package for use with SA** to have the Host Checker install and start the Junos Pulse client. If the client fails or is stopped manually, it is not restarted automatically.

b. Click **Export**, click **OK**, and then save the **.zip** file to a local folder or file share.

4. Upload the exported software package to an SA Series gateway:

   a. Log in as an administrator to the admin console of the SA Series gateway and select **Authentication > Endpoint Security > Host Checker**.

   b. Verify that the **Perform check every X minutes** and **Client-side process, login inactivity timeout** are set to 10 minutes or more, and that the timeout interval is not greater than the check interval.

   c. Select **New 3rd Party Policy**, specify a policy name, and select the exported Junos Pulse client software package as the Policies File.

   d. Click **Save Changes**.

   e. Select **Users > User Realms > Select Realm > Authentication Policy > Host Checker**. Select both the **Evaluate Policies** and **Require and Enforce** check boxes for the displayed Junos Pulse client policy.

   f. Click **Save Changes** to save the Host Checker policy.

Distributing the Pulse Client Through SMS

To use SMS to distribute the Junos Pulse client, you must export the client configuration from the WXC Series gateway and use it to replace the default client configuration in the Windows installer file.

To distribute the Junos Pulse client through SMS:

1. Export the client configuration from the WXC Series gateway:

   a. Select **Junos Pulse > Admin > Export Pulse Software**.

   b. Select **Download Configuration for MSI package**.

   c. Click **Export**, and then save the **Config_All.ini** file to a local folder or file share.

2. Download the Windows installer version of the Junos Pulse client software (a .msi file) to a computer that has InstallShield 2008. You can download the software from **http://www.juniper.net/customers/support**.
3. Open the downloaded file with InstallShield and select the Installation Designer tab.
4. Select **Organization > Components** in the left pane, and open the first components folder in the middle pane.
5. Select the **Files** subfolder in the middle pane, right-click on the **Config_All.ini** file displayed in the right pane, and select **Delete**.
6. Right-click on the **Files** subfolder, and select **Add**.
7. Locate the **Config_All.ini** file that you exported from the WXC, and click **Open**.
8. Select **In a new CAB file** file, select the **Stream the new CAB file into the Windows Installer package** check box, and click **OK**.
9. Click **Save** to save your changes.

CHAPTER 7

Maintaining WXC Series Gateways

- Maintaining WXC Configurations and Software on page 69
- Using Maintenance Tools on page 74
- Troubleshooting Passthrough Mode on WXC Series Gateways on page 80

Maintaining WXC Configurations and Software

- Saving the WXC Configuration on page 69
- Viewing the Configuration of WXC Series Gateways on page 70
- Loading a Configuration File on WXC Series Gateways on page 70
- Loading a Software Package on WXC Series Gateways on page 72
- Clearing Monitoring Statistics on WXC Series Gateways on page 73
- Restoring the Factory Default Configuration on WXC Series Gateways on page 73
- Rebooting the WXC Gateway on page 74

Saving the WXC Configuration

When you change a gateway's configuration, you must save the configuration file to flash memory to retain the changes after the next reboot. You can also save the configuration file to another location for backup, such as an FTP or TFTP server. If a problem occurs that requires you to restore the factory default settings, you can load a saved configuration file to restore your network settings.

NOTE: A configuration file contains hardware-specific information, such as IP network addresses. Therefore, do not load the configuration file from one WXC Series gateway to another.

1. Select **Admin > Maintenance > Save Configuration**.

2. Select one of the following:

Flash memory	Save the current configuration to the **startup.cfg** file in flash memory or click **Save to the filename** and enter another name. The name can be up to eight characters, with no file extension (for example, **myconfig**). Click **Save** to save the configuration. The **startup.cfg** file is loaded each time you reboot the gateway. Always save the standard configuration to **startup.cfg**. You can also save the configuration to a backup location.
Local disk drive	Save the current configuration to the disk of a local machine in your network. Select this option, click **Save**, and specify the filename and location.
TFTP server	Save the current configuration to a TFTP server in your network. Enter the server's IP address and a path and filename on the server (for example, **/juniper/config_save.cfg**), and then click **Save**.
FTP server	Save the current configuration to an FTP server in your network. Enter the server's IP address and a path and filename on the server (for example, **/juniper/config_save.cfg**). If the FTP server does not accept anonymous user access, enter a username and password for an account that has read/write privileges on the server, and then click **Save**.

Viewing the Configuration of WXC Series Gateways

You can view the current candidate configuration of a WXC Series gateway through the Web interface. The candidate and running configurations are the same unless a CLI user enters uncommitted changes to the candidate configuration. All uncommitted changes are applied to the running configuration when you enter a **commit** command or when you click **Submit** in the Web interface.

The running configuration might be different from the configuration saved in flash memory. To save the running configuration, see "Saving the WXC Configuration" on page 69.

To view the running configuration:

1. Select **Admin > Maintenance > Display Configuration**.
2. View the running configuration. Some configuration options can be set only through the CLI (see the *JWOS Command Reference Guide*).

Loading a Configuration File on WXC Series Gateways

You can change the configuration of a WXC Series gateway by loading a configuration file that was previously saved to flash memory, a local disk, or an FTP or TFTP server.

NOTE: A configuration file contains gateway-specific information, such as IP network addresses. Do not load the configuration file from one WXC Series gateway to another. Loading an improper configuration file can have adverse effects on the gateway.

To load a configuration file:

1. Select **Admin > Maintenance > Load Configuration**.
2. Specify the location of the configuration file, and then click **Load**.

Flash memory	Load the default configuration (startup.cfg) from flash memory or click **Load from the file** and select another configuration that is saved in flash memory.
Local disk	Specify the path and filename on a machine in your network or click **Browse** and select the configuration file.
TFTP server	Enter a TFTP server's IP address and a path and filename on the server, such as **/juniper/config_save.cfg**.
FTP server	Enter an FTP server's IP address and a path and filename on the server, such as **/juniper/config_save.cfg**. If the FTP server does not accept anonymous user access, enter a username and password for an account that has read/write privileges on the server.

3. Click **Save** in the taskbar to retain the configuration after the next reboot. This step is unnecessary if you load **startup.cfg** from flash memory.

   If the new configuration file changes the gateway's IP address, you must save the configuration to **startup.cfg** in flash memory, and then reboot the gateway (see "Rebooting the WXC Gateway" on page 74).

Loading a Software Package on WXC Series Gateways

To upgrade the JWOS operating system on a WXC Series gateway, you can load a new boot image from a local disk or an FTP or TFTP server. You can then reboot the gateway to activate the new software. Loading a boot image does not affect the configuration settings stored in the **startup.cfg** file. All configuration information is preserved.

NOTE: Always save the current configuration file before upgrading to a new release so that you can reload the configuration if you must restore the previous release (see “Saving the WXC Configuration” on page 69).

To load a software package:

1. Select **Admin > Maintenance > Load Software Package**.
2. Specify the location of the software package:

Local disk	Specify the path and filename on a machine in your network or click **Browse** and select the software image file.
TFTP server	Enter a TFTP server's IP address and the path and filename on the server.
FTP server	Enter an FTP server's IP address and the path and filename on the server. If the FTP server does not accept anonymous user access, enter a username and password for an account that has read/write privileges on the server.

3. Select **Make this the selected software package for the next reboot** to select the new software package as the default the next time you reboot the WXC Series gateway. You can change the selected software package before rebooting the gateway (see "Rebooting the WXC Gateway" on page 74).
4. If you are loading WXOS 5.6.5 or higher, select **Allow downgrade to version 5.6 or higher**. Note that you cannot downgrade from JWOS 6.x to a version prior to WXOS 5.6.5.
5. Click **Load** to update the WXC software.

Clearing Monitoring Statistics on WXC Series Gateways

At any time you can reset all the application monitoring statistics to zero.

1. Select **Admin > Maintenance > Clear Monitor Stats**.
2. Click **Clear** to clear the application monitoring statistics.

Restoring the Factory Default Configuration on WXC Series Gateways

You can erase all gateway configuration information, including compression statistics and network address information, by restoring the factory default configuration. This is useful during testing or when you want to move the gateway to another location.

NOTE: Restoring the factory default configuration removes all data, configuration information, and log files. It also disrupts the adjacencies with this gateway. Before you restore the factory default configuration, we strongly recommend that you back up the configuration file to another location (see "Saving the WXC Configuration" on page 69).

To restore the factory default configuration:

1. Select **Admin > Maintenance > Set to Factory Default**.
2. Select **Preserve IP Address** to preserve the network settings of the bridge interfaces. If you clear this check box, the gateway is powered off, and you must have physical access to the gateway to apply power and do the initial configuration.

3. Select **Wipe Disk** to erase the disks so the data cannot be restored. Enter the number of passes used to wipe the disks (up to 20). Each pass can take several hours, depending on the amount of data on the disk. We recommend five passes for maximum security. To stop the process, reboot the gateway.

   During each pass, a different value is written to each byte on the disks. The first pass uses random numbers, the second pass writes a repeated pattern, the third pass uses zeros, the fourth pass writes another repeated pattern, and the fifth pass repeats the sequence with random numbers, shifted by 1 byte.

4. Click **Set to Factory Default**. If you selected **Wipe Disk**, the current pass number and the percent completion of the pass are displayed. After the disks are wiped, the factory defaults are loaded.

5. If you cleared the **Preserve IP Address** check box, the gateway is powered off. To restart the gateway:

   a. Wait a few moments for the shutdown to complete. On the WXC3400 and WXC2600, the LCD on the front panel displays the following:

      Factory Default. Power System Off

   b. Unplug the power cable, and then plug the cable back in.

   c. Specify the IP address, subnet mask, and default gateway, and run Quick Setup (see “Running Quick Setup for a WXC Series Gateway” on page 21).

Rebooting the WXC Gateway

If you load a new boot image of the JWOS software, you must reboot the gateway to activate the new software. During a reboot, the selected boot image and the configuration file (**startup.cfg**) are loaded from flash memory into main memory.

To reboot the WXC Series gateway:

1. Select **Admin > Maintenance > Reboot**.
2. Verify that the correct version of the software is shown. To reboot the gateway using a different version, select the version from the list. Click **Submit** to save your selection as the default version.
3. Click **Reboot**.

Using Maintenance Tools

- Using the Ping Utility on WXC Series Gateways on page 75
- Using the Traceroute Utility on WXC Series Gateways on page 75
- Using the Packet Capture Utility on WXC Series Gateways on page 76
- Viewing and Saving System Logs on WXC Series Gateways on page 77
- Viewing and Saving Access Control Logs on WXC Series Gateways on page 77
- Exporting Performance Data on WXC Series Gateways on page 77

- Creating a Diagnostic File on WXC Series Gateways on page 78
- Viewing Flow Diagnostics on WXC Series Gateways on page 78

Using the Ping Utility on WXC Series Gateways

You can use the ping utility to verify connectivity with remote WXC Series gateways, or other network devices.

To use the ping utility:

1. Select **Admin > Tools > Ping**.
2. Enter the IP address of a network device.
3. (Optional) Enter the size of each ping packet (8 to 4068 bytes), and the number of packets to be sent (1 to 50).
4. Click **Submit** to ping the device. The results are shown in the Web interface, including the round-trip time of each packet (in milliseconds).

   For example:

   ```
   PING 10.87.77.20 (10.87.77.20): 32 data bytes
   40 bytes from 10.87.77.20: icmp_seq=0 ttl=63 time=0.435 ms
   40 bytes from 10.87.77.20: icmp_seq=1 ttl=63 time=0.251 ms
   40 bytes from 10.87.77.20: icmp_seq=2 ttl=63 time=0.272 ms


   --- 10.87.77.20 ping statistics ---
   3 packets transmitted, 3 packets received, 0% packet loss
   round-trip min/avg/max/stddev = 0.251/0.319/0.435/0.082 ms
   ```

Using the Traceroute Utility on WXC Series Gateways

You can use the traceroute utility to determine the number of router hops in the network path between the WXC Series gateway and another remote network device. This tool can help you determine the point in your network that is causing a connection failure.

To use the traceroute utility:

1. Select **Admin > Tools > Traceroute**.
2. Enter the IP address of the destination device, and the maximum number of router hops (1 to 30).
3. Click **Submit**. The results are displayed in the Web interface, including the IP address of each device in the path, and the round-trip time (in milliseconds) of each of the three packets sent to identify each hop. For example:

   ```
   1 192.168.53.130 2 ms 0 ms 0 ms
     2 192.168.53.70 2 ms 2 ms 4 ms
     3 192.168.53.1 0 ms 2 ms 2 ms
     4 192.168.52.15 2 ms 2 ms 2 ms
     5 192.168.0.127 2 ms 2 ms 2 ms
   ```

Using the Packet Capture Utility on WXC Series Gateways

The packet capture utility lets you capture raw network data from a Local or Remote interface on the WXC Series gateway. The packet capture information can then be exported to a file and analyzed by a protocol analyzer program or other hardware. The packet capture's file format is either **libpcap** or **snoop**. Note that the packet capture criteria can be populated from the Flow Diagnostics page (see "Viewing Flow Diagnostics on WXC Series Gateways" on page 78).

To use the packet capture utility:

1. Select **Admin > Tools > Packet Capture**.
2. Specify the following information:

Interface	Select a Local or Remote interface where you want to capture packets. The name format is **fe-** or **ge-** *slot/pair*/**0** for Local interfaces and **fe-** or **ge-** *slot/pair*/**1** for Remote interfaces.
Size	Enter the number of bytes to be captured (minimum is 4096). Execution stops when the specified number of bytes are captured.
Maximum Packets	Limit the capture to a maximum number of packets by selecting the second option and entering the number of packets.
Snap Length	Enter the maximum number of bytes captured for each packet (1 to 65535). The default is 1514. Select **All** to capture the entire packet.
Filter	(Optional) Select **On** to limit the packet capture to any combination of the following options: • Enter a source and/or destination IP address and port number. • Select **TCP** or **UDP** from the IP Protocol list, or select **Enter** and enter a protocol number (0 to 255). • Select one or more TCP flags (applied only to TCP traffic). To populate the filter settings from a current traffic flow, see "Viewing Flow Diagnostics on WXC Series Gateways" on page 78.
Storage Format	Select the format of the captured data (**libpcap** or **snoop**). The default filename is **pkgdump.dmp**.
Delete After	Enter the number of hours that the packet capture file is retained (1 to 168).

3. Click **Start** to start the packet capture. The status is displayed on the left side of the page. Click **Stop** at any time to stop the capture.
4. Click **Save** to save the packet capture, and specify a filename and location.
5. Click **Delete** to manually delete the packet capture file. You cannot run another packet capture until the previous one is deleted.

Viewing and Saving System Logs on WXC Series Gateways

The system log files can be displayed in the Web interface or downloaded to a local machine for use by third-party applications. If your network has dedicated syslog servers, you can configure the WXC Series gateway to send log messages to up to five syslog servers (see "Configuring Syslog Reporting for WXC Series Gateways" on page 32).

To view or download system log files:

1. Select **Admin > Tools > Display System Log** to view the system log file. The current system log is displayed in the Web interface. The most recent entries are displayed last.
2. Click **Save System Log** in the navigation pane to download a system log file for a specific time period.

   The **wxoutput** file contains the most recent data. Each time **wxoutput** reaches 1 MB in size, it is saved as **wxoutput1**, and the existing log files are renumbered up to **wxoutput10** (older log files are discarded). The First entry time column shows the oldest entry in each log file.
3. Click the name of the log file you want to save, click **Save**, and specify a filename and location.

Viewing and Saving Access Control Logs on WXC Series Gateways

The access control log shows the username, date, and time of each user who accessed the WXC in the last five days. The access method is shown as SSH (CLI access), HTTPS (Web access), or CONSOLE (direct access). The workstation IP address is included for SSH and HTTPS.

NOTE: The access log has six files. Viewing or saving the access log concatenates the data from all the files.

To view or download an access control log file:

1. Select **Admin > Tools > Display Access Control Log** to display the access control log. The most recent entries are displayed last.
2. Click **Save Access Control Log** in the navigation pane to download the access control log. Click the name of the log file you want to save, click **Save**, and specify a filename and location.

Exporting Performance Data on WXC Series Gateways

You can export the performance data for all time periods to a file in comma-separated values (CSV) format. You can then import the CSV file into a spreadsheet program (such as Microsoft Excel) or other data evaluation program. The performance data is similar to the data displayed in the Monitor page of the Web interface (see "Performance Statistics Exported from WXC Series Gateways" on page 95).

To export performance data to CSV format:

1. Select **Admin > Tools > Export Data**.
2. Select **All (ZIP format)** to export the data for all time periods as a **.zip** file. If you cannot open a **.zip** file (some browser versions cannot), select **All (CSV format)**.

   For a description of the CSV data file, see "Performance Statistics Exported from WXC Series Gateways" on page 95.
3. Click **Submit**, and then click **Save** and specify a filename and location.

Creating a Diagnostic File on WXC Series Gateways

If you experience problems with a WXC Series gateway, you can generate a diagnostic file to send to Technical Support. The diagnostic file contains current configuration, filter settings, system information, and the most recent log files. After you generate and save the diagnostic file, e-mail it to support@juniper.net.

To create and send a diagnostic file to Technical Support:

1. Select **Admin > Tools > Diagnostic File**.
2. Click **Submit** to generate the diagnostic file, and then click **Save** and specify a filename and location.
3. E-mail the diagnostic file as an attachment to support@juniper.net. A support representative will contact you.

Viewing Flow Diagnostics on WXC Series Gateways

You can view diagnostic details for up to 50 of the most recently started active traffic flows. You can also initiate a packet capture for a specific flow, and download the top 50 most recent flows to a file in CSV format. For a description of the exported diagnostics, see "Flow Diagnostics Exported from WXC Series Gateways" on page 99).

NOTE: A flow constitutes data that is sent or received from a single source IP address and port number, to a single destination IP address and port number over the same protocol.

To view the flow diagnostics:

1. Select **Admin > Tools > Flow Diagnostics**.
2. Click **Download** to export the diagnostics for the 50 most recent traffic flows to a file in CSV format, and then click **Save** and specify a filename and location.
3. Click **Go** to view the top 50 most recent traffic flows.

4. To view specific traffic flows, specify any of the following options, and then click **Go**.

Source Subnet	Enter a subnet in the following format to view only the traffic flows from that subnet: ***IP address/subnet mask*** The subnet mask indicates the number of bits used for the network portion of the address (for example, 10.10.20.0/24).
Source Port	Enter the source port number of the flows you want to view. An asterisk (*) indicates any port. For a list of common application ports, see: **http://www.iana.org/assignments/port-numbers**
Destination Subnet	Enter a subnet in the following format to view only the traffic flows sent to that subnet: ***IP address/subnet mask*** The subnet mask indicates the number of bits used for the network portion of the address (for example, 10.10.20.0/24).
Destination Port	Enter the destination port number of the flows you want to view. An asterisk (*) indicates any port.
Application	Select an application to view just the traffic flows for the selected application (the default is **All**).
Protocol	Select an application protocol or select **Any** to indicate TCP or UDP. You can also type in a protocol number (0 to 134).
Show reg. port names	Click the check box to view the registered names for all ports. Clear the check box to view the names only for port numbers up to 1024.
Show domain names	Click the check box to view the domain names for each IP address. To specify the DNS servers to be queried, see “Configuring the Domain Name for WXC Series Gateways” on page 28. The IP address is displayed if its domain name cannot be resolved. The DNS queries might take a few seconds.

5. Click the arrow icon next to a flow to open the Packet Capture page with the filtering criteria for the traffic flow.
6. Click the magnifier icon next to a flow to view a summary of the diagnostic details for the traffic flow. The summary details are grouped into the following sections:
   - General Flow
   - TCP Acceleration
   - Application Acceleration
   - CIFS
   - LZ

7. Click the **Auto Refresh** check box to update the summary every 5 seconds.
8. Click **Show details** next to a section name to view more details related to the section. For a description of the flow details provided, see "Flow Diagnostics Exported from WXC Series Gateways" on page 99.

Troubleshooting Passthrough Mode on WXC Series Gateways

The following topics describe how to correct a condition where all traffic is passed through the WXC Series gateway without any processing:

- Detecting Passthrough Mode on page 80
- Using the WXC Web Interface to Recover from Passthrough Mode on page 81
- Using the WXC Console to Recover from Passthrough Mode on page 81

Detecting Passthrough Mode

During normal operation, some traffic (such as non-TCP traffic) is passed through the WXC Series gateway without any processing. However, some hardware and software errors can cause a WXC Series gateway to enter passthrough mode where all traffic is passed through.

To determine whether the WXC is in passthrough mode:

1. Try to log in to the WXC Web interface by entering the IP address of the bridge interface in the browser. You can also use the IP address of the management interface, if configured.

   https://*IP address*

2. If you can log in, and one of the messages in Table 7 on page 80 is displayed in the banner, see "Using the WXC Web Interface to Recover from Passthrough Mode" on page 81. If the login fails, see "Using the WXC Console to Recover from Passthrough Mode" on page 81.

Table 7: Passthrough Error Messages

Error Message	Description
HW-Passthru: Mgmtd	The management process is down. You cannot log in to the Web interface, so this message is displayed only on the WXC console.
HW-Passthru: Netd	The network manager is down.
HW-Passthru: IfMgrd	The interface manager is down.
HW-Passthru: DiskMgrd	The disk drive manager is down.
SW-Passthru: SvcP	The services processor is down.

Table 7: Passthrough Error Messages *(continued)*

Error Message	Description
SW-Passthru: MonAgtProcess	The monitoring agent is down. Monitoring reports and some SNMP data are not available while the gateway is in passthrough mode.
SW-Passthru: WxTimer	The WXC timer process is down.
SW-Passthru: br-0/0 is down	The bridge interface is down. This can occur if the interface is disabled manually, configured incorrectly, or missing any required static routes.

Using the WXC Web Interface to Recover from Passthrough Mode

1. If the message displayed is **SW-Passthru: br-0/0 is down**, do the following:
   a. Select **Setup > Bridge Interfaces > br-0/0** and verify that the IP address, subnet mask, and default gateway address are correct. Make any necessary changes, and click **Submit**.
   b. If the status of the Local or Remote interface is down, verify the physical connections to the network. Note that in off-path deployments, only the Local interface is connected.
   c. Select **Local Routes** and verify that the appropriate static routes are defined. Add any necessary static routes, and click **Submit**.

   If the problem persists, contact Technical Support.
2. For all other passthrough messages, use the following procedure to collect the diagnostic information for Technical Support.
   a. Select **Admin > Tools > Diagnostic file**, click **Download**, and save the file.
   b. If you cannot download the diagnostic file, select **Admin > Tools > Display System Log** and copy the displayed log entries to a file. Also, select **Admin > Display Configuration** and copy the gateway configuration to a file.
3. After you collect the diagnostic information, try rebooting the gateway:
   a. Select **Admin > Reboot**, select the alternate JWOS software image (if you have one), click **Submit**, and then click **Reboot**.
   b. If the problem persists, determine whether a JWOS upgrade is available, and upgrade the gateway to the new version.
   c. If the preceding steps fail, try rebooting from the JWOS Safe OS as described in “Using the WXC Console to Recover from Passthrough Mode” on page 81.

Using the WXC Console to Recover from Passthrough Mode

For more information about the CLI commands used in the following procedure, see the *JWOS Command Reference Guide*.

1. Log in as the **admin** user on a terminal connected to the WXC console port. If the gateway is in passthrough mode, one of the messages in Table 7 on page 80 is displayed. If the login fails, contact Technical Support.
2. Run the following commands and collect the output for Technical Support:
   - **show system**
   - **show interfaces br-0/0 extensive**
   - **show log**
   - **show boot**
   - **show disks**
   - **show flow-stats**
3. After you collect the diagnostic information, try rebooting the gateway. If you have an alternate JWOS software image, specify the alternate partition (**A** or **B**):

   config set boot *partition*
   request system reboot
4. If the problem persists, determine whether a JWOS upgrade is available, and upgrade the gateway to the new version:
   a. Before loading the JWOS upgrade, reboot the gateway using the JWOS Safe OS:

      config set boot safe
      request system reboot
   b. When the **(none)safe>** prompt is displayed, load the JWOS upgrade and reboot the gateway:

      request system install *path*
      request system reboot

PART 2

Specifications

- Specifications for WXC Series Gateways on page 85
- SNMP Traps and Syslog Messages on WXC Series Gateways on page 91
- Data Exported from WXC Series Gateways on page 95
- Certifications for WXC Series Gateway on page 105
- Copyrights on page 109

APPENDIX A

Specifications for WXC Series Gateways

The following topics describe the technical specifications for the WXC Series gateways, and the pinouts for the DB-9 console port.

- WXC Platform Specifications on page 85
- DB9 Console Port Pinouts on WXC Series Gateways on page 88

WXC Platform Specifications

- General Specifications for All WXC Series Gateways on page 85
- Specifications for WXC590, WXC2600, and WXC3400 on page 87

General Specifications for All WXC Series Gateways

Table 8 on page 85 describes the specifications that apply to all WXC gateways.

Table 8: General Specifications for All WXC Platforms

Product Features	Description
Traffic services	Compression, acceleration, application identification and monitoring
Protocols supported	Any IP-based traffic (such as TCP, UDP, GRE, ICMP, and L2TP)
Applications supported	All TCP-based applications, such as Microsoft Office applications, Oracle E-Business Suite, Sharepoint, Microsoft Exchange, Citrix, SAP, and web-based applications
Network Integration	
Installation	In line between an aggregation switch and edge router, or off the WAN router using policy-based routing
Transparency	Transparent bridge-mode operation, configurable DSCP, and IP port transparency
Topology support	Point to point, hub and spoke, full mesh
Adjacency creation	Automatic or manual

Table 8: General Specifications for All WXC Platforms *(continued)*

Product Features	Description
Fault tolerant nonstop operation	10/100/1000BASE-T auto switch-to-wire on any power, hardware, or software failure condition
High availability	Automatically fail-to-wire
Quality of Service (QoS)	
Honor, preserve and/or set ToS/DSCP	Retain settings on received traffic and set ToS/DSCP values for WXC control traffic
Application identification	Automatic, based on source/destination IP address/port, ToS/DSCP, IP protocol; follows port hopping applications (FTP, Exchange)
Application Acceleration	TCP acceleration, Microsoft CIFS acceleration
Device Management	
SNMP, syslog	SNMPv2c, MIB II, WXC Enterprise MIB, and local syslog
Secure remote access	SSHv1, SSHv2, and HTTPS (SSL)
Reports	Device-level reports available through Web interface
Authentication, Authorization, and Accounting	Local user-account database
Network upgradable	Through FTP, HTTP and TFTP; dual software images and configurations
Monitoring	
Compression statistics	Per application and destination; both real-time and historical
WAN Performance statistics	Network latency, loss, and availability for SLA monitoring and enforcement
Acceleration	TCP session time and throughput; both real-time and historical
Data export	CSV format
Application reporting	Detail by IP address, port number, IP protocol, DSCP/ToS value, and application type
Event monitoring	Generate automatic alerts (SNMP traps, console) for system events
Operating Environment	
Temperature	41º to 104º F (5º to 40º C)
Relative humidity	10% to 85%, noncondensing at 95º F (35º C)

Table 8: General Specifications for All WXC Platforms *(continued)*

Product Features	Description
Maximum altitude	10,000 ft (3048 m)
Nonoperating Environment	
Temperature	-40° to 158° F (-40° to 70° C)
Relative humidity	10% to 85%, noncondensing at 95° F (35° C)
Maximum altitude	40,000 ft (12,192 m)
Regulations	
Emissions	FCC Class A, EN 55022 Class A, EN 55024 Immunity, EN 61000-3-2, VCCI Class A
Safety	CAN/CSA-C22.2 No. 60950-1-03- UL 60950-1 and EN 60950-1
Acoustic noise	Maximum noise level less than 70 dB

Specifications for WXC590, WXC2600, and WXC3400

Table 9 on page 87 lists the specifications for the disk-based WXC platforms supported by JWOS 6.0.

Table 9: WXC Family Specifications

	WXC590	WXC2600	WXC3400
Performance			
Total compression throughput speed	Up to 10 Mbps	128 Kbps to 8 Mbps	2 Mbps to 45 Mbps
Adjacencies supported (all features enabled)	100	250	1000
Concurrent accelerated traffic flows	2000	1000	4000
Disk capacity	500 GB (two redundant, replaceable 250 GB drives)	250 GB (replaceable)	1 TB (two redundant, replaceable 500 GB drives)
Application definitions	Up to 256	Up to 256	Up to 256
Connections			

Table 9: WXC Family Specifications *(continued)*

	WXC590	WXC2600	WXC3400
Network interfaces	Two copper fail-to-wire 10/100/1000 Ethernet ports	• Two copper fail-to-wire 10/100/1000 Ethernet ports • Console port • High-availability port • Management port • USB port • Slot for pluggable bypass interface module (PBIM)	• Two copper fail-to-wire 10/100/1000 Ethernet ports • Console port • High-availability port • Management port • USB port • Two PBIM slots
Power			
Power	Dual 100 to 240 VAC, 50 to 60 Hz, 300 W max or 1025 BTU/hr. Designed to work with IT power systems.	100 to 240 VAC, 50 to 60 Hz, 300 W max or 1025 BTU/hr	Dual 100 to 240 VAC, 50 to 60 Hz, 400 W max or 1370 BTU/hr. DC option available. Designed to work with IT power systems.
Dimensions and Weight			
(W x H x D)	17.1 x 3.4 x 16.7 in (43.4 x 8.7 x 42.4 cm) 2 U	17.5 x 1.8 x 14.5 in (44.5 x 4.6 x 36.8 cm) 1 U	17.5 x 3.4 x 18 in (44.5 x 8.6 x 45.7 cm) 2 U
Weight	25 lbs (11.3 kg)	17 lbs (7.7 kg)	30 lbs (13.6 kg)

DB9 Console Port Pinouts on WXC Series Gateways

Table 10 on page 88 and Table 11 on page 89 list the pinouts for a null-modem cable used to connect the DB9 console port to a DB9 or DB25 terminal port. These specifications apply to all WXC Series gateways.

Table 10: Pinouts for DB9-to-DB9 Cable

Console Port	DB9	DB9	Terminal Port
Receive Data	2	3	Transmit Data
Transmit Data	3	2	Receive Data
Data Terminal Ready	4	6+1	Data Set Ready + Carrier Detect

Table 10: Pinouts for DB9-to-DB9 Cable *(continued)*

Console Port	DB9	DB9	Terminal Port
System Ground	5	5	System Ground
Data Set Ready + Carrier Detect	6+1	4	Data Terminal Ready
Request to Send	7	8	Clear to Send
Clear to Send	8	7	Request to Send

Table 11: Pinouts for DB9-to-DB25 Cable

Console Port	DB9	DB25	Terminal Port
Receive Data	2	2	Transmit Data
Transmit Data	3	3	Receive Data
Data Terminal Ready	4	6+8	Data Set Ready + Carrier Detect
System Ground	5	7	System Ground
Data Set Ready + Carrier Detect	6+1	20	Data Terminal Ready
Request to Send	7	5	Clear to Send
Clear to Send	8	4	Request to Send

APPENDIX B

SNMP Traps and Syslog Messages on WXC Series Gateways

This appendix describes the SNMP traps and syslog messages for the system events generated by WXC Series gateways.

- System Events and SNMP Traps for WXC Series Gateways on page 91
- Syslog Message Format for WXC Series Gateways on page 93

System Events and SNMP Traps for WXC Series Gateways

Table 12 on page 91 describes each system event, and provides the associated SNMP trap name, object ID (OID), and syslog ID.

Table 12: System Events and SNMP Traps

Metric Name	Severity	Message	SNMP Trap/OID	Syslog ID
Client Limit Exceeded	Error	**Client Limit Exceeded** The licensed concurrent connections for Junos Pulse clients has been exceeded. Contact Juniper Networks to obtain a new license with a higher number of concurrent connections.	jnxWxCommonEventClientLimitExceeded 1.3.6.1.4.1.2636.3.41.1.1.3.0.6	204
Cold Start	Notice	**WX Device is initialized** The gateway restarted.	Cold Start 1.3.6.1.6.3.1.1.5.1	302
Fail Safe Mode Active	Critical	**Put the system in SW bypass** The gateway restarted in safe mode. Power is on, but all traffic is passed through without any processing.	jnxWxGrpEventInFailSafeMode 1.3.6.1.4.1.2636.3.41.1.1.3.0.7	301

Table 12: System Events and SNMP Traps *(continued)*

Metric Name	Severity	Message	SNMP Trap/OID	Syslog ID
Interface Duplex Mismatch	Error	**Interface duplex mismatch** A possible duplex mismatch exists between the Local or Remote interface and the device attached to that interface. The interface is identified in SNMP by jnxWxCommonEventDescr.	jnxWxGrpEventInterfaceDuplexMismatch 1.3.6.1.4.1.2636.3.41.1.1.3.0.10	403
Interface Speed Mode Mismatch	Error	**Speed-duplex mismatch between local and remote interface** A speed or duplex mismatch exists between the Local and Remote interface on the WXC Series gateway.	jnxWxGrpEventInterfaceSpeedMismatch 1.3.6.1.4.1.2636.3.41.1.1.3.0.8	401
Interface Speed Mode Ok	Notice	**Speed matches between local and remote interface** A previously detected mismatch between the Local and Remote interface is now resolved.	jnxWxGrpEventInterfaceSpeedOk 1.3.6.1.4.1.2636.3.41.1.1.3.0.9	402
LAN Link Down	Information	**LAN Link down** The Local interface link failed. Verify that the link state change was not due to a network error.	LAN Link Down 1.3.6.1.6.3.1.1.5.4	502
LAN Link Up	Notice	**Lan Link up** The Local interface link is established.	LAN Link Up 1.3.6.1.6.3.1.1.5.3	501
License Expired	Error	**Evaluation License expired** The temporary license expired. Contact Juniper Networks for a permanent license.	jnxWxGrpEventLicenseExpired 1.3.6.1.4.1.2636.3.41.1.1.3.0.5	203
License Will Expire	Information	**License will expire soon** The temporary license will expire soon. Contact Juniper Networks to obtain a permanent license.	jnxWxGrpEventLicenseWillExpire 1.3.6.1.4.1.2636.3.41.1.1.3.0.3	201
Login Failure	Error	**Login failed: access=*method* user=*name*** A login attempt failed. The access method is **Web**, **SSH**, or **Console**.	jnxWxGrpEventLoginFailure 1.3.6.1.4.1.2636.3.41.1.1.3.0.11	601
Management Config Save Failure	Error	**Management Config save failure** An attempt to save the configuration failed.	None	702

Table 12: System Events and SNMP Traps *(continued)*

Metric Name	Severity	Message	SNMP Trap/OID	Syslog ID
Management Startup Config Saved	Notice	**Management startup config saved** The startup configuration was saved successfully.	None	701
Power Supply Failure	Error	**Power supply failure** One or more power sources failed. A redundant power supply has taken over.	jnxWxGrpEventPowerSupplyFailure 1.3.6.1.4.1.2636.3.41.1.1.3.0.1	101
Power Supply Ok	Notice	**Power supply Ok** One or more previously failed power sources are now working normally. The system returned to normal without being restarted.	jnxWxGrpEventPowerSupplyOk 1.3.6.1.4.1.2636.3.41.1.1.3.0.2	102
Security Login Success	Notice	**Login ok: access=*method* user=*name*** A user logged in successfully. The access method is **Web**, **SSH**, or **Console**.	None	602
WAN Link Down	Information	**WAN Link down** The Remote interface link failed. Verify that the link state change was not due to a network error.	WAN Link Down 1.3.6.1.6.3.1.1.5.4	504
WAN Link Up	Notice	**WAN Link up** The Remote interface link is established.	WAN Link Up 1.3.6.1.6.3.1.1.5.3	503

Syslog Message Format for WXC Series Gateways

The syslog message format is based on the syslog-19 standard. For more information about syslog-19, go to **http://tools.ietf.org/html/draft-ietf-syslog-protocol-19**. Each message consists of a header, structured data enclosed in brackets, and the text of the message. The header contains the date, time, and IP address of the WXC Series gateway that sent the message, followed by "1 - - Juniper-WX", a module name, and the event ID.

In the following example, the module name is **authentication**:

```
Feb 13 17:34:48 10.88.16.34 1 - - Juniper-WX authentication 0601 [wx-event@juniper.net
eventtime="1234730471" metric="Login Failure" sev="error" type="sys"
   devid="164584745349120"]
Login failed: access=Web user=admin
```

The structured data starts with **wx-event@juniper.net**, followed by the event time, metric name, and severity level. All messages are for events of type **sys**. The **devid=** value is not

used. The syslog messages, event IDs, metric names, and severity levels are listed in “System Events and SNMP Traps for WXC Series Gateways” on page 91

APPENDIX C

Data Exported from WXC Series Gateways

- Performance Statistics Exported from WXC Series Gateways on page 95
- Flow Diagnostics Exported from WXC Series Gateways on page 99

Performance Statistics Exported from WXC Series Gateways

The following topics describe the performance data that can be exported from a WXC Series gateway in CSV format (see "Exporting Performance Data on WXC Series Gateways" on page 77):

- General Device Information on page 95
- Data Section Information on page 96
- System Session Statistics on page 96
- Compression Statistics on page 97
- WAN Performance Statistics on page 98
- TCP Flow Statistics on page 98

General Device Information

Table 13 on page 95 describes the exported information that identifies the gateway.

Table 13: General Device Information

Parameter	Description
Device IP	IP address of the WXC Series gateway.
Software version	Version of JWOS software that was running when the statistics were exported.
Serial number	Serial number of the WXC Series gateway that exported the statistics.
License speed	Licensed speed of the WXC Series gateway.
Operation mode	Indicates whether the gateway is active (Inline).
Monitored applications	Names of the applications being monitored for reports.

Data Section Information

Table 14 on page 96 describes the data section information that precedes the statistic tables for each exported time range.

Table 14: Data Section Information

Parameter	Description
time data section	Indicates one of the following time ranges for the statistics tables that follow: • This hour • Last hour • Today • Yesterday • This week • Last week
device local time=	Local date and time of the export.
gmt_time=	Date and time of the export in Greenwich Mean Time (GMT).

System Session Statistics

Table 15 on page 96 describes the exported session statistics.

Table 15: System Session Statistics

Parameter	Description
startTime	Start of the time interval for the generated statistics (in GMT). The length of each time interval depends on the data section. For example, in the **This hour** data section the intervals are 1 minute.
ptAppDefMatchBytes	Number of bytes passed through due to application policy.
ptAppDefMatchPkts	Number of packets passed through due to application policy.
ptNoRemoteWxBytes	Number of bytes passed through due to no remote Pulse client.
ptNoRemoteWxPkts	Number of packets passed through due to no remote Pulse client.
ptNonTcpProtoBytes	Number of non-TCP bytes passed through.
ptNonTcpProtoPkts	Number of non-TCP packets passed through.
ptNonIpBytes	Number of non-IP bytes (such as IPX) passed through.
ptNonIpPkts	Number of non-IP packets passed through.
ptFragIpBytes	Number of bytes of IP fragments passed through.
ptFragIpPkts	Number of packets of IP fragments passed through.

Table 15: System Session Statistics *(continued)*

Parameter	Description
ptVlanBytes	Number of bytes of VLAN traffic passed through.
ptVlanPkts	Number of packets of VLAN traffic passed through.
ptMcastBytes	Number of Layer 2 multicast bytes passed through.
ptMcastPkts	Number of Layer 2 multicast packets passed through.
compFailAppDefDisableBytes	Number of bytes not compressed because of application policy.
compFailAppDefDisablePkts	Number of packets not compressed because of application policy.
compFailTcpAcclToRemoteBytes	Number of bytes not compressed because TCP acceleration to remote is disabled.
compFailTcpAcclToRemotePkts	Number of packets not compressed because TCP acceleration to remote is disabled.
compFailResCrunchBytes	Number of bytes not compressed because of buffer overflow.
compFailAlgoLimitBytes	Number of bytes not compressed because of buffer overflow algorithmic limitation.
compTcpAccFailedBytes	Number of bytes not compressed because local TCP acceleration is disabled.
compTcpAccFailedPkts	Number of packets not compressed because local TCP acceleration is disabled.
cifsFailAppDefBytes	Number of CIFS bytes not accelerated due to application policy.
cifsFailAppDefPkts	Number of CIFS packets not accelerated due to application policy.
cifsFailTcpAcclToRemoteBytes	Number of CIFS bytes not accelerated because TCP acceleration to remote is disabled.
cifsFailTcpAcclToRemotePkts	Number of CIFS packets not accelerated because TCP acceleration to remote is disabled.
cifsFailTcpAcclFailedBytes	Number of CIFS bytes not accelerated because TCP acceleration to remote failed.
cifsFailTcpAcclFailedPkts	Number of CIFS packets not accelerated because TCP acceleration to remote failed.

Compression Statistics

Table 16 on page 97 describes the exported compression statistics for each session.

Table 16: Compression Session Statistics

Parameter	Description
startTime	Start of the time interval for the generated statistics (in GMT).
appName	Name of the application.

Table 16: Compression Session Statistics *(continued)*

Parameter	Description
hostName	Name of the remote Pulse client.
remoteWXId	Internal ID of the remote Pulse client.
remoteWX Mac Address	Hardware address of the remote Pulse client.
bytesIn	Number of bytes received by the compression engine.
bytesOut	Number of compressed bytes sent to the remote Pulse client.
cachesHit	Number of lookups in the compression dictionary that were successful.
cachesMiss	Number of lookups in the compression dictionary that were unsuccessful.

WAN Performance Statistics

Table 17 on page 98 describes the exported WAN performance statistics.

Table 17: WAN Performance Statistics

Parameter	Description
startTime	Start of the time interval for the generated statistics (in GMT).
appName	Name of the application.
hostName	Name of the remote Pulse client.
remoteWXId	Internal ID of the remote Pulse client.
remoteWX Mac Address	Hardware address of the remote Pulse client.
bytesToWan	Number of bytes sent to the WAN for the remote Pulse client and application.
bytesFromWan	Number of bytes received from the WAN for the remote Pulse client and application.
proxyBytesToWan	Number of bytes sent to the WAN using TCP acceleration.

TCP Flow Statistics

Table 17 on page 98 describes the exported TCP traffic flow statistics.

Table 18: TCP Flow Statistics

Parameter	Description
startTime	Start of the time interval for the generated statistics (in GMT).

Table 18: TCP Flow Statistics *(continued)*

Parameter	Description
appName	Name of the application.
hostName	Name of the remote Pulse client.
remoteWXId	Internal ID of the remote Pulse client.
remoteWX Mac Address	Hardware address of the remote Pulse client.
ptFlowCountAvg	Average number of flows that are passed through without being proxied (no TCP acceleration).
proxyFlowCountAvg	Average number of flows that are currently being proxied.
ptFlowCountDiff	Number of flows that were passed through in the last 10 seconds.
proxyRequestCountDiff	Number of proxy flow requests received in the last 10 seconds.
proxyFlowCountDiff	Number of flows proxied in the last 10 seconds.
failedToProxyCountDiff	Number of flows that were not proxied for any reason in the last 10 seconds.

Flow Diagnostics Exported from WXC Series Gateways

Table 19 on page 99 describes the flow diagnostics data exported to the **flowdiag.csv** file.

Table 19: Flow Diagnostics

Parameter	Description
SrcIp	IP address of the flow source.
SrcPort	Source port number.
DstIp	IP address of the flow destination.
DstPort	Destination port number.
Application	Traffic flow application name.
Proto	Traffic flow protocol (TCP, UDP, or protocol number).
Start Time	Date and time the flow started.
Last Active	Date and time of the last flow activity.
General Flow	

Table 19: Flow Diagnostics *(continued)*

Parameter	Description
Proxy Mode On Box	TCP acceleration mode (Opaque).
Proxy Mode Mismatch	TCP acceleration mode configured differently on remote client (True or False).
Configured CIFS	CIFS acceleration is enabled locally (True or False).
Configured LZ	LZ compression is enabled locally (True or False).
Actual CIFS	CIFS acceleration is applied (True or False).
Actual LZ	LZ compression is applied (True or False).
Proxied	TCP acceleration is applied (True or False).
Total Packets Rcvd	Number of packets received for proxied flows.
Total Bytes Received from WAN	Number of bytes received from the WAN for proxied flows.
Total Bytes Sent to WAN	Number of bytes sent to the WAN for proxied flows.
Total Packets	Number of packets sent or received for all traffic flows.
Total Bytes	Number of bytes sent or received for all traffic flows.
Flow Start Time	Date and time the flow started.
Last Time Packet Sent or Received	Date and time of last packet sent or received for the flow (proxied or passthrough).
TCP Acceleration	
Number of Reads At PSI Layer	Number of read operations for peer socket information (PSI).
Number of Writes At PSI Layer	Number of write operations of peer socket information.
Generic PSI Layer State	State of peer socket.
PSI Socket Eagain Counter	Number of timeouts that occurred while waiting to receive data.
Last PSI Socket Error Number	Last PSI socket error.
Socket fd	Socket file descriptor (negative value indicates an error).
Initial sequence number	First sequence number in the traffic flow.

Table 19: Flow Diagnostics *(continued)*

Parameter	Description
Initial syn-ack number	Sequence number of the SYN-ACK packet.
Number of SYNs seen	Number of SYN packets seen.
Number of SYN-ACKs seen	Number of SYN-ACK packets seen.
Options In SYN	Options specified in the SYN packet.
Options Supported	Options supported by the local WXC Series gateway.
SACK supported	Options supported in the SYN-ACK packet.
MSS	Maximum segment size (in bytes).
Read window size	Size of the TCP read window (in bytes).
Write window size	Size of the TCP write window (in bytes).
TCP bytes recvd	Number of bytes received.
TCP bytes sent	Number of bytes sent.
TCP connection state	Status of TCP connection.
FIN received	The FIN packet was received.
Which side received FIN	The WXC Series gateway or Pulse client received the FIN packet (local or remote).
Has bidirectional FIN received	The FIN packet was received by both local and remote endpoints.
Was RST received	The RST packet was received.
Last socket error	Last socket error.
Last RTT	Last round-trip time (in milliseconds).
Best RTT	Lowest round-trip time (in milliseconds).
Largest send window	Largest TCP send window (in bytes).
LAN packets transmitted	Number of packets sent to the LAN.
LAN duplicates acks received	Number of duplicate acknowledgments received from the LAN.
WAN packets transmitted	Number of packets sent to the WAN.

Table 19: Flow Diagnostics *(continued)*

Parameter	Description
WAN duplicates acks received	Number of duplicate acknowledgments received from the WAN.
Application Acceleration	
Protocol accelerated	Name of the accelerated application (CIFS).
AAP sync version	The version of protocol acceleration.
Flow initialized	The flow was initialized.
Hard quits	Number of flows ended by the application.
Soft quits	Number of flows for which the application disabled acceleration.
Unknown quits	Number of flows for which an unknown agent disabled acceleration.
Bytes to server	Number of bytes sent to the application server.
Bytes from server	Number of bytes received from the application server.
PDUs to server	Number of protocol data units (PDUs) sent to the application server.
PDUs from server	Number of PDUs received from the application server.
Bytes to client	Number of bytes sent to the client.
Bytes from client	Number of bytes received from the client.
PDUs to client	Number of PDUs sent to the client.
PDUs from client	Number of PDUs received from the client.
AAP state	The current state of the flow acceleration.
Present AAP PDU size	Number of bytes per PDU.
CIFS	
Signed	Indicates whether SMB signing is used.
Client OS	Windows version running on the client.
Server OS	Windows version running on the server.
Accl Reads	Number of accelerated read requests.

Table 19: Flow Diagnostics *(continued)*

Parameter	Description
Total Reads	Total number of read requests.
Accl Writes	Number of accelerated write requests.
Total Writes	Total number of write requests.
Accl Trans2 Count	Number of accelerated Trans2 packets.
Total Trans2 Count	Total number of Trans2 packets.
Free Disk Space Positive	Number of times the server had enough disk space to satisfy a write request or a Trans2/SetEndOfFile request. These requests are accelerated.
Free Disk Space Negative	Number of times the server did not have enough disk space to satisfy a write request or a Trans2/SetEndOfFile request. These requests are not accelerated.
Free Disk Space Stale	Number of times write or Trans2/SetEndOfFile requests were not accelerated because the server's disk space information on the WXC was out of date.
Free Disk Space Unavailable	Number of times write or Trans2/SetEndOfFile requests were not accelerated because the server's disk space information was unavailable.
Prefetch Reuse OK	When a file is closed, the read prefetch data for the file is kept for reuse. This counter is the number of times the prefetch data was found to be eligible for reuse.
Prefetch Reuse Not OK	Number of times the prefetch data was not eligible for reuse.
Whole File Prefetches	Number of times an entire file was prefetched for read acceleration.
Whole File Prefetch Alloc Failed	A file prefetch failed (TRUE or FALSE).
MID Table Full	The table of multiplex IDs used to track CIFS requests became full at least once (TRUE or FALSE).
Write Update Error (Prefetch Buffer)	Indicates whether an update error occurred when an accelerated write overlaps with a read prefetch, and the write data is used to update the read prefetch data (TRUE or FALSE).
Close Accl Failure	Indicates whether an accelerated Close failed on the server (TRUE or FALSE).
Write Through on File Open	Indicates whether a file open operation writes the file directly to disk, rather than to a cache in memory (TRUE or FALSE).
Write Through On Write	Indicates whether file open operations were written directly to disk, rather than cached in memory (TRUE or FALSE). These write operations are not accelerated.
Send Buffer Alloc Failed	Indicates whether the allocation of a send buffer failed (TRUE or FALSE).
LZ	

Table 19: Flow Diagnostics *(continued)*

Parameter	Description
Bytes to WAN	Number of compressed bytes sent to the WAN.
Bytes from WAN	Number of compressed bytes received from the WAN.
Bytes to LAN	Number of uncompressed bytes sent to the LAN.
Bytes from LAN	Number of uncompressed bytes received from the LAN.
Flow ID	ID number of the traffic flow.
Elapsed Time	Number of seconds elapsed since the traffic flow started.

APPENDIX D

Certifications for WXC Series Gateway

This appendix describes the safety, electrical, and environmental certifications for the supported WXC Series gateways.

- Certifications for WXC Series Gateways on page 105
- Product Reclamation and Recycling Program on page 106

Certifications for WXC Series Gateways

Table 20 on page 105 lists the certifications for the supported WXC Series gateways.

Table 20: Certifications for WXC Series Gateways

Description	WXC590	WXC2600 WXC3400
Safety Standards		
CSA 60950-1 (2003)	X	X
UL 60950-1 (2003)	X	X
EN 60950-1 (2001)	X	X
IEC 60950-1 (2001)		X
EN 60825-1 +A1+A2 (1994)		X
EN 60825-2 (2000)		X
Conformity for EMC and EMI		
EN 300 386 V1.3.3 (2005)		X
FCC Part 15 Class A	X	X
EN 55022 Class A	X	X
VCCI Class A (2007)		X

Table 20: Certifications for WXC Series Gateways *(continued)*

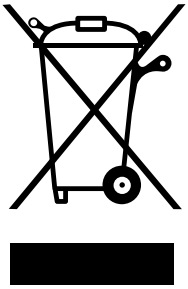
Description	WXC590	WXC2600 WXC3400
Immunity		
EN 55024 +A1+A2	X	X
EN 61000-3-2	X	X
EN 61000-3-3 +A1+A2+A3	X	X
EN-61000-4-2 +A1 +A2		X
EN-61000-4-3 +A1 +A2		X
EN-61000-4-4 (2004)		X
EN-61000-4-5 (2006)		X
EN-61000-4-6 (2007)		X
EN-61000-4-11 (2004)		X
Gost	X	

Product Reclamation and Recycling Program

Juniper Networks is committed to environmentally responsible behavior. As part of this commitment, we continually work to comply with environmental standards such as the European Union's *Waste Electrical and Electronic Equipment* (WEEE) Directive and *Restriction of Hazardous Substances* (RoHS) Directive.

These directives and other similar regulations from countries outside the European Union regulate electronic waste management and the reduction or elimination of specific hazardous materials in electronic products. The WEEE Directive requires electrical and electronics manufacturers to provide mechanisms for the recycling and reuse of their products. The RoHS Directive restricts the use of certain substances that are commonly found in electronic products today. Restricted substances include heavy metals, including lead, and polybrominated materials. The RoHS Directive, with some exemptions, applies to all electrical and electronic equipment.

In accordance with Article 11(2) of Directive 2002/96/EC (WEEE), products put on the market after 13 August 2005 are marked with the following symbol or include it in their documentation: a crossed-out wheeled waste bin with a bar beneath.



Juniper Networks provides recycling support for our equipment worldwide to comply with the WEEE Directive. For recycling information, go to http://www.juniper.net/environmental, and indicate the type of Juniper Networks equipment that you wish to dispose of and the country where it is currently located, or contact your Juniper Networks account representative.

Products returned through our reclamation process are recycled, recovered, or disposed of in a responsible manner. Our packaging is designed to be recycled and should be handled in accordance with your local recycling policies.

APPENDIX E

Copyrights

- Traceroute Copyright License on page 109
- OpenSSL Copyright License on page 110
- GNU GENERAL PUBLIC LICENSE on page 112

Traceroute Copyright License

This code is derived from software contributed to Berkeley by Van Jacobson. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER

IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenSSL Copyright License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (**http://www.openssl.org/**)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (**http://www.openssl.org/**)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Original SSLeay License

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses,

in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program” , below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification” .) Each licensee is addressed as “you” .

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent

and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this

License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version” , you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA. Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

PART 3

Index

- Index on page 121

Index

A

AAA settings 30
acceleration
  application policies 36
  CIFS, SMB signing 44
  client policies 64
  client status 65
  protocol....36
  TCP....35
access control log file....77
active FTP 40
application policies, configuring 36
applications
  defining 37
  summary statistics
    all traffic....56
    WAN traffic....50
ARP, configuring 31
autonegotiate
  bridge interfaces 26
  management interface 27

B

baud rate, default 13
boot images
  activating....74
  loading 72
bridge interfaces, configuring....26
browser support 21
bypass disable command....14, 17, 21

C

certifications 105
CIFS acceleration
  about 36
  application policies....37
  client policies 64
  client status 65
  SMB signing 44
clients, Junos Pulse
  configuring adjacencies....64
  configuring policies 64
  defining the client configuration 65
  distributing through SMS or SA....67
  download from a SA Series gateway....63
  download from a WXC gateway....62
  enable downloads 64
  hardware and software requirements....61
  loading a client image 66
  uninstall....63
  viewing status 65
communities, defining 30
community strings, SNMP....32
compliance
  certifications....105
  product reclamation and recycling....106
compression
  application policies....37
  client policies 64
  client status 65
compression statistics
  peak compression 49, 54
  viewing 53, 55
configuration, Junos Pulse client
  defining....65
  displaying 66
configuration, WXC
  displaying 70
  loading 70
  saving 69
  setting to the factory default 73
console port
  DB9 cable pinouts....88
  default settings....13
contact information....25
CSV, interpreting exports 95
customer support....xvii
  contacting JTAC....xvii

D

default gateway
- bridge interfaces 25
- configuring in front panel 16, 19
- management interface 27

deployment examples....5
device names 25
diagnostic files, generating 78
diagnostics, traffic flow
- description of exported data 99
- viewing and exporting....78

disk drives, replacing 10
display settings....21
distributing Junos Pulse clients through SMS or SA....67
DNS servers, configuring 28
domain names
- configuring 28
- in flow diagnostics....79

downgrading to a previous release 72
download a Junos Pulse client 62, 63
DSCP values
- in application definitions 41
- in WXC control traffic *See* JWOS Command Reference Guide

E

electronic equipment, recycling....106
EMC and EMI certifications 105
erasing the disks....74
Executive report 47
exporting
- Junos Pulse client software or configuration....67
- packet capture data....76
- performance statistics 77, 95

external policy-based router commands for packet interception....33

F

facility, syslog....32
factory default WXC configuration....73
failure propagation, link....27
fans, replacing....10
firewall requirements 9
flow diagnostics
- description of exported data 99
- viewing and exporting 78

front panel
- securing 31
- using the buttons 16, 19

FRU components 10
FTP application type....40
FTP servers, using
- to load a client configuration file....65
- to load a WXC software package....72
- to load the Pulse client software....66
- to load WXC configuration files....70
- to save WXC configuration files....69

G

gateway names 25
gateways
- bridge interfaces....25
- configuring default in front panel....16, 19
- management interface 27

general specifications....85

H

hardware
- installation overview....9
- passthrough....14, 17, 21
- reclamation and recycling....106

hazardous materials, reclamation and recycling....106
high-availability support....27

I

idle user timeout....31
immunity certifications....105
inline deployment 11
installation
- inline and off-path....11
- Junos Pulse clients....62
- postinstall tasks....22
- pre-install tasks....9
- procedure....11
- WXC2600 15
- WXC3400 18
- WXC590 11

interfaces
- bridge 26
- configuring in front panel 16, 19
- management....27

IP address
- bridge interfaces 25
- configuring in front panel 16, 19

management interface 27
NTP servers....28

J
Junos Pulse clients
configuring adjacencies 64
configuring policies 64
defining the client configuration 65
distributing through SMS or SA....67
download from a SA Series gateway....63
download from a WXC gateway....62
enable downloads....64
hardware and software requirements....61
loading a client image 66
uninstall....63
viewing status 65

L
Layer 2 multicast traffic....59
lead in equipment, reclamation and recycling....106
LEDs, checking
WXC2600....16, 19
WXC590....13
license keys, entering 29
link failure propagation 27
loading software
for Junos Pulse clients 66
for WXC 72
local domain name....28
local users, defining 30
log files
WXC access control 77
WXC system 77
logging in
to access the WXC 23
to download Junos Pulse client software 64
LZ compression
client policies 64
client status 65

M
MAC addresses
in ARP entries....31
of Local and Remote interfaces....26
message severity, syslog....32
monitoring applications....37
monitoring statistics, clearing 73

N
naming gateways and other objects....23
network settings, configuring
in front panel....16, 19
in Web interface 25, 27
NTP, configuring....28

O
off-path deployment
configuring....33
installing 11

P
packaging, recycling....107
packet capture
enabling user privilege 31
using 76, 79
packet interception 33
passthrough statistics....58
passwords
to access the WXC 30
to download Junos Pulse client software....64
peak compression....49
performance data, exporting 77, 95
permanent license keys....29
ping utility 75
port numbers
in application definitions....40
in flow diagnostics....79
required for TCP and UDP 9
postinstallation tasks 22
power supplies, replacing 10
preinstallation tasks....9
privilege level, user 31
protocol acceleration, about 36
protocols
in application definitions....40
in flow diagnostics....79

R
rebooting the gateway 74
reclamation and recycling....106
recycling Juniper Networks equipment....106
reports
Application Summary
all traffic 56
WAN traffic 50
Compression....53, 55
Executive 47

Passthrough Data 58
TCP Connections 59
throughput
all traffic 52
WAN traffic 49
Restriction of Hazardous Substances (RoHS) Directive, recycling equipment....106
RoHS (Restriction of Hazardous Substances) Directive, recycling equipment....106
rolling back to a previous release 72
routes, static....26
RTT
reported by ping utility....75
reported by traceroute utility....75

S

SA Series gateway, download a Junos Pulse client from....63
safety certifications 105
sample topologies 5
secure wipe 74
security features....30
defining local users....30
securing front panel access....31
serial port
DB9 cable pinouts....88
default settings 13
servers
DNS....28
NTP 28
syslog 32
severity levels, syslog 32
SMB signing....44
SNMP
configuring 32
list of traps 91
SNTP, configuring 28
software upgrades
for Junos Pulse clients 66
for WXC 72
special characters 24
specifications, gateway 85
speed
bridge interfaces....26
management interface....27
static routes, adding 26
statistics
application
all traffic 56
WAN traffic 50
clearing....73
compression 53, 55
executive summary 47
exporting....77, 95
interpreting CSV exports....95
passthrough traffic 58
TCP connections 59
throughput
all traffic 52
WAN traffic 49
subnet mask
bridge interfaces 25
configuring in front panel 16, 19
management interface 27
subnets, filtering flow diagnostics....79
support
browser 21
generating diagnostic files....78
support, technical *See* technical support
syslog
configuring 32
list of messages....91
message format....93
system log file....77

T

TCP acceleration
about 35
application policies....37
client policies 64
client status 65
TCP Connections report....59
TCP ports used by WXC 9
technical support
contacting JTAC....xvii
generating diagnostic files....78
terminal emulation program....13
throughput statistics
all traffic....52
WAN traffic....49
time settings
manual 28
NTP server 28
timeout, idle user 31
topology examples 5

ToS/DSCP values
in application definitions 41
in WXC control traffic *See* JWOS Command Reference Guide
traceroute utility 75
traps, SNMP
configuring 32
list of.....91
types of applications 40

U

UDP ports used by WXC 9
undefined applications, defining.....37
uninstall the Junos Pulse client.....63
upgrading
client software 66
the WXC software 72
user class.....31
usernames and passwords
to access the WXC 30
to download Junos Pulse client software 64

V

VPN configuration.....6

W

WAN statistics.....49
Waste Electrical and Electronic Equipment (WEEE) Directive. *See* WEEE Directive
Web interface
about.....23
browser support 21
display settings 21
logging in.....23
WEEE (Waste Electrical and Electronic Equipment) Directive, recycling equipment.....106
wiping the disks 74
WXC2600 installation.....15
WXC3400 installation 18
WXC590 installation.....11